CRITICAL ANALYSES OF SOME PUBLIC-KEY CRYPTOSYSTEMS FOR HIGH-SPEED SATELLITE TRANSMISSION APPLICATIONS

by

MOSES HSINGWEN MA

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE
DEGREES OF

BACHELOR OF SCIENCE
and
MASTER OF SCIENCE

in

ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June, 1980

(i.e. February '81)

Signature of Author _____

Department of Electrical Engineering and Computer Science, May 14, 1980

Certified by _____

Ronald L. Rivest
Thesis Supervisor (MIT)

Accepted by _____

Arthur C. Smith
Chairman, Department Graduate Committee

CRITICAL ANALYSES OF SOME PUBLIC-KEY CRYPTOSYSTEMS FOR HIGH-SPEED SATELLITE TRANSMISSION APPLICATIONS

by

MOSES HSINGWEN MA

Submitted to the Department of Electrical Engineering and
Computer Science on May 14, 1980 in
partial fulfillment of the requirements for the Degrees of
Bachelor of Science and Master of Science in
Computer Science

ABSTRACT

Communication privacy and user authentication have become important issues in data communications, especially for high speed (e.g., 64 Kbits/sec to 120 Mbits/sec) digital satellite communications. The recently proposed Data Encryption Standard (DES) might not be desirable for many applications in high-speed data transmission via satellites, because of the potential problems of key distribution and key management associated with the conventional cryptosystems. Public-key cryptosystems have been proposed to alleviate the problems of key distribution and key management. This dissertation incorporates mathematical analysis and computer techniques to perform cryptanalysis on the Rabin and Williams schemes, thereby determining some of the properties which would help in assessing its suitability for high speed satellite communication applications.

Academic Thesis Supervisor: Dr. Ronald L. Rivest

Title: Professor of Computer Science and Electrical Engineering

ACKNOWLEDGEMENTS

I wish to acknowledge the guidance and advice from my advisor Prof. Ronald Rivest in my efforts on this project. Also, I would like to thank Prof. Vaughan Pratt for the funds from NSF grant no. MCS78-04338 that made completion of my thesis possible.

The work reported here was done at M.I.T.'s Laboratory of Computer Science and at Comsat laboratories at Clarksburg, Maryland under the VI-A co-operative program with M.I.T..

I also wish to express my gratitude to my mother and father for their encouragement during the course of my education and during this work.

I am extremely thankful for the proofreading assistance I received from Jay Dunnington and Mark Williams.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

1 PRELIMINARIES

1.1 INTRODUCTION

With the arising need for data communications and data processing, cryptography has been considered as an important means to provide communication privacy and message authenticity. The application of cryptography is no longer limited to military or diplomatic communities.

Some previously known schemes for privacy of communications include the one-time cipher, running key cipher, Hagelin Machine, rotor machines, linear feedback shift registers, etc.. These schemes are called "conventional" because they use the identical key for both enciphering and deciphering. The message must be encoded by an encipherer using this particular key before it is sent. The receiver would then use the same key in the decipherer to perform the inverse operation of the encipherer, and thereby decode the message. Thus, security of the system is dependent upon the key and therefore, it must be kept secret.

Key management has been an important aspect of communication security. It is required for any key-controlled cryptographic algorithm. Key management requires a protocol for safely handling and controlling its cryptographic keys. This protocol involves issues such as: who should have access to which part of the key, who should generate and maintain the keys, how the keys should be protected, and how the keys should be changed.

Another major aspect of communication security of key distribution. Key distribution is the transporting or routing of cryptographic keys through the cryptographic system for subsequent installation into the designated cryptographic devices. Key distribution involves issues such as: how the keys should be distributed securely to authorized users, who should distribute the keys, and how to assure that the keys are properly distributed.

To alleviate these problems of key distribution and key management, Hellman invented the concept of public-key, which uses a one-way trap-door function. In this concept, two separate keys are employed for encryption and decryption. The decryption key is kept secret by the receiver while the encryption key is made public. The encryption and decryption algorithms are known to every user. Knowing the encryption key without knowing the decryption key makes it practically impossible for one to decrypt the message. The simplicity is made possible by the design of the trap-door one-way functions which are built into every public-key scheme. The sender must obtain the recipient's encryption key from the public file to encrypt the message before sending it to the recipient. Since the recipient is the only one who has the trap-door information which is the decryption key, he is the only one who can decrypt the message.

In a conventional scheme, communication between n nodes requires as many as n^2 secret keys. On the other hand with the public-key schemes communication between n nodes requires only n

secret keys. There is a difference of a factor of n in key distribution and key management between public-key and conventional systems. Public-key schemes alleviate the need to manage n(n-1) keys that would have to be used in the conventional scheme to only n keys.

Cryptography uses tranformations of the actual data to make the resulting data useless to one's opponents. These transformations help solve the two major data security problems of privacy and authentication. The privacy problem involves preventing opponents from extracting information from the communication channel. The authentication problem involves preventing the opponents from altering transmissions by adding incorrect data into the communication channel and thus changing the messages.

For some public-key systems the encryption and decryption operations are interchangeable and can be used for authentication. Let two users be user A and user B. In public-key systems there are two keys for each user. The encryption keys are E^A and E^B and the decryption keys are D^A and D^B. Define $D^A(E^A(M))=M$ and $D^B(E^B(M))=M$. The decryption keys are secret, whereas the encryption keys are public. The sender, user A, can encrypt or sign his message, M, first with D^A to produce $D^A(M)$. Then he encrypts the result with E^B to produce $E^B(D^A(M))$. Then the cryptogram is transmitted to the receiver, user B. User B then decrypts the cryptogram first with D^B to produce $D^B(E^B(D^A(M)))$, which is $D^A(M)$. User B decrypts the result with E^A to produce $E^A(D^A(M))$, which yields the desired message M. This process permits user B to authenticate the message sent by user A, since only user A could have encrypted the message with D^A. The message must be time dependent, otherwise anyone could record $E^B(D^A(M))$ and use it later as a signature for A.

The candidate cryptosystem for high-data rate (64 Kbits/sec-120 Mbits/sec) satellite communications must be: 1) secure, and 2) relatively simple to implement. In addition the cryptosystem must allow for relatively easy distribution and management of the keys. The desired speed of cryptosystems for satellite communications is in the 1 to 10 Mbit/sec range. Public-key cryptosystems will be the primary candidates for high-speed satellite communication applications because of the relative ease of key distribution and key management for these cryptosystems. In the past, many different public-key schemes have been developed. This dissertation discusses several schemes of Rivest-Shamir-Adleman, Merkle and Hellman, Rabin, and Williams individually and comes to a conclusion as to which of the schemes are compatible with the criteria set for high-speed secure satellite communication. The possibility of using conventional schemes such as the recently proposed Data Encryption Standard (DES) for satellite communications will also be discussed.

1.2 SCOPE OF THE DISSERTATION

To aid in understanding of the dissertation organization, a brief summary of each chapter is given here.

Chapter 1 introduces the problem area and gives the motivation for the studies undertaken.

Chapter 2 summarizes the previous conventional schemes. The following five schemes will be discussed: 1) the running key cipher; 2) the Hagelin machine; 3) rotor machines; 4) linear feedback shift registers; and 5) IBM's Data Encryption Standard (DES). These conventional schemes will be of interest when one studies public-key schemes. Also described is the main downfall of all conventional schemes requiring that only one secret key be securely given to both users trying to communicate. This leads to a study of public-key cryptosystems which alleviate this problem.

Chapter 3 discusses several of the existing public-key schemes including the public-key schemes of: 1) Rivest-Shamir-Adleman (RSA) scheme; and the 2) Merkle and Hellman (knapsack scheme). These two public-key schemes will be of interest when the Rabin scheme and Williams scheme are analyzed and shown to have some advantages and disadvantages when compared to other public-key schemes.

Chapter 4 describes the main public-key schemes to be discussed in depth in this dissertation. It discusses: 1) the Rabin scheme; 2) how the decryption of the Rabin scheme is equivalent to factoring r; 3) the Williams scheme and how it solves the ambiguity problem; and 4) how the decryption of the Williams scheme is equivalent to factoring r.

The next three chapters will discuss inportant properties of the Rabin scheme which must first be found in order to find its weaknesses. The properties lead to some very interesting cryptanalysis attacks on the Rabin scheme. Some of the properties are counterintuitive, while other properties are very intuitive.

Chapter 5 discusses how many decryptions each possible cryptogram may have in the Rabin scheme. The cases are: 1) one-decryption; 2) two-decryptions; and 3) four-decryption.

Chapter 6 describes the effects of choosing different b's on the Rabin scheme. The parameter b has no real effect on the cryptograms except for a shift of the relative positions of the cryptograms with respect to the messages. The number of four-solutions, two-solutions, and one-solution cryptograms remains the same for different b's as do the relative positions of the four-solutions, two-solutions, and one-solution cryptograms with respect to each other. Some of the subproperties are counterintuitive, while other subproperties are very intuitive. The four major sub-properties are as follows: 1) for $b=1, 2, 3, \ldots (r-1)/2$ the scheme has the same cryptograms as for $b=-1, -2, -3, \ldots (1-r)/2$, respectively, except the values of the cryptograms are shifted with respect to the values of the messages; 2) as b varies the number of four-solutions, two-solutions, and one-solution cryptograms remain the same. For any b not equal to 0 (mod p) or 0 (mod q) the number of cryptograms of the form $z=0 \pmod p$ or $0 \pmod q$ remain the same. Also, the pattern which relates cryptograms to their respective numbers of solutions shifts with respect to the values of the messages; and 3) for $b=-k \pmod p$ or $-j \pmod q$ or $+k \pmod p$ or $+j \pmod q$ there is a method to find a cryptogram that equals 0 (mod p) or 0 (mod q). Therefore, the choice of b has no effect, and that the breaking of the Rabin scheme for one b breaks the Rabin scheme for all b's.

In the Rabin scheme, seven additional properties are of particular interest are discussed in Chapter 7. These are: 1) cryptograms and messages of the form 0 (mod p) or 0 (mod q); 2) the encryption function which maps r possible messages into only about r/4 possible cryptograms; 3) $m=z$; 4) $m=-b$; 5) $z_1-z_2=0$ (mod p) or 0 (mod q); 6) repeated encryption; and 7) the relative speeds of the Rabin and the Rivest-Shamir-Adleman schemes.

Chapter 8 describes the ambiguity problem of the Rabin scheme. The ambiguity problem is to decide which of the four-solution messages found in decryption is the original message. There are several possible approaches to solve the problem by: 1) the simple parity check; 2) the choice of largest solution; 3) the choice of a set of possible messages ; 4) coding; and 5) the usage of the Williams scheme.

General attacks on the Rabin scheme are introduced in chapter 9 including how: 1) a repeated encryption attack can always be launched; 2) the Pollard algorithm can be used for a repeated encryption attack; 3) the equivalence of decryption to factoring enables a chosen ciphertext attack; 4) the equivalence of decryption to factoring does not contribute to other attacks; 5) the equivalence of decryption to factoring contributes to possible signature attacks; and 6) Rabin added patches to protect his scheme from signature attacks. These potential attacks are all byproducts from an investigation of Rabin scheme properties.

Chapter 10 describes general attacks on the Williams scheme, including how: 1) the equivalence of decryption to factoring enables a chosen ciphertext attack; 2) the equivalence of decryption to factoring does not contribute to possible signature attacks; 3) the equivalence of decryption to factoring does not contribute to other attacks; 4) Williams added patches to protect his scheme from chosen ciphertext and signature attacks; and 5) there is no repeated encryption attack or Pollard's algorithm attack on the Williams scheme.

Chapter 11 describes conclusions and areas for future research.

Chapter 12 is the bibliography.

2 PREVIOUS CONVENTIONAL SCHEMES

2.1 INTRODUCTION

This chapter discusses previous conventional schemes. Focusing on following five schemes: 1) the running key cipher; 2) the Hagelin machine; 3) rotor machines; 4) linear feedback shift registers; and 5) IBM's Data Encryption Standard (DES).

These conventional schemes are of interest when one studies public-key schemes. Public-key schemes were invented to alleviate some of the problems in existing conventional schemes. For a more detailed description of conventional schemes consult either "Privacy and Authentication: An Introduction to Cryptography" by Diffie and Hellman or "The Codebreakers" by Kahn.

2.2 OLD CONVENTIONAL SCHEMES

The old conventional schemes include: 1) the running key cipher; 2) the Hagelin machine; 3) rotor machines; and 4) linear feedback shift registers. These schemes contain weaknesses which enabled the cryptanalysts to break them. The main problem with conventional schemes is that they require one private key between each pair of users. However, only one private key needs to be used.

2.2.1 THE RUNNING KEY CIPHER

To encipher, the plaintext is added modulo 26 to the key which is a readily available book or magazine. Spaces are deleted from the ciphertext to make the cryptanalysis harder. To decipher the key is subtracted from the ciphertext.

The method for breaking this scheme makes use of probable words which occur in the plaintext such as: of the, tion, who, what, etc.. The probable words are subtracted from the ciphertext to find part of the key.

2.2.2 THE HAGELIN MACHINE

Used during World War II as a field cipher, the Hagelin machine is similar to the running key cipher in that a key of letters are added together with the message to encipher. The key stream is the set of letters in the alphabet. The plaintext, P, is subtracted from the keystream, K (mod 26), so the ciphertext C is its own inverse.

$C = K-P \pmod{26} \rightarrow P = K-C \pmod{26}$

Therefore the keystream generation is very important. The keystream is generated by a set of key wheels generating a pseudorandom sequence of six bit groups, which are then translated into characters by the cage. Prior to enciphering, the machine is keyed by adjusting the pin settings on the wheel to produce the correct enciphering and deciphering. There are six keywheels with teeth having the following number of teeth respectively: 26, 25, 23, 21, 19, and 17. Each tooth of every wheel has a pin that can be extended or retracted and each bit of key determines the setting of each pin. The wheels are set to inital positions before turning. The wheels are labeled with as many letters of the alphabet possible for the number of teeth starting with a and ending with z with the initial position of the wheels starting at aaaaaa. The six pins that are on the six teeth of the a's on each wheel correspond to the first letter of the wheel. The wheels are rotated one position each until bbbbbb is reached and from here the next set of pins are read to retrieve the next letter. This continues until the first seventeen letters are read off the six wheels at qqqqqq. The next turn of the wheel produces rrrrra and the pins are read again for the next letter. Since the numbers 26, 25, 23, 21, 19, and 17 are relatively prime, the number of possible characters is $(26x25x23x21x19x17) = 101,000,000$.

The cage functions as a PROM containing $2^6 = 64$ letters, which are represented by the numbers 0 to 25. The six bits read from the wheel serve as a memory address to the PROM, so when the address is read to the PROM, the corresponding character is retrieved. The deciphering is done by subtracting the ciphertext from the key stream, which is the reverse of enciphering.

2.2.3 ROTOR MACHINES

Another device used in World War II was the rotor machine. Around the rotor there were electrical contacts each of which represents some letter. Each rotor has a front face and a back face. Each electrical contact on the front face is wired to one electrical contact on the back face, thereby creating a permutation. An electrical signal for a character is permuted as it travels from the front to the back of the rotor. If the rotor is rotated the permutation produced on an incoming signal will change. Rotor operation can be shown by representing the rotor function as R, the permutation as P, and the shift as C; so the permutation that is represented by the rotor is

$P = C^N R C^{-N}$

The shift of C^N is a cyclic shift through N positions of the rotor. Therefore, if $R(F) = M$, then $C^4R(F) = Q$ and $C^4RC^{-4}(F) = C^4R(B) = C^4(I) = M$.

Rotors can be interconnected so that after a character leaves one rotor it enters another rotor at a different location. The additional permutations in a set of rotors make the system more complex. This is shown in the following:

$$P= C^{N_1}R_1C^{-N_1}C^{N_2}R_2C^{-N_2}...C^{N_m}R_mC^{-N_m}=C^{N_1}R_1C^{N_2-N_1}R_2...R_{(m-1)}C^{N_m-N_{(m-1)}}R_mC^{-N_m}$$

This arrangement of rotors can implement a very large variety of permutations since each rotor can be rotated to different positions. The rotation of the rotors is used to change the permutations instead of a change of the connector positions, because it is much harder to change electical connections than to rotate the rotors. As each character is enciphered it is necessary to rotate the rotor to ensure a strong cryptographic system, consequently the motion of the rotor is important and must be carefully chosen. The simplest method of rotation is a odometer motion. The rightmost wheel rotates after each encipherment, until the wheel has completed one rotation. Then the wheel to the left advances once while the rightmost wheel continues to rotate. Desirable characteristics for motion of the rotors include: 1) the period must be long enough so that the key cannot be remembered; 2) each state change should be large, so that as many of the rotors rotate as much as possible relative to each other. Therefore, very few of the exponents $C^{N_1-N_2}$ are zero. These characteristics are not easy to accomplish.

The longest possible motion is that of the odometer consisting of $26^6 \simeq 309$ million different states; however, each state change does not effect most of the rotors. Therefore, something similar to the Hagelin machine rotation may be desirable. For this method each wheel does not rotate to all of its possible positions; it skips a few selected positions so that it can simulate the Hagelin machine's rotation. The first wheel rotates to all of the 26 contacts, the second wheel to 25 contacts, the third wheel to 23 contacts, the fourth wheel to 21 contacts, the fifth wheel to 19 contacts and the last wheel to 17 contacts. Then all of the wheels can rotate at once like the Hagelin machine. This rotation satisfies objective 2) while still giving a reasonable number of possible states, 101 million, which can satisfy characteristic 1).

The rotor machine is keyed by changing positions of the rotors, the order of the rotors, the number of stopping places per wheel (the number of stops must not have common factors with each other to maintain a maximum number of states), the pattern of motion, or by choosing different rotors out of a basket.

2.2.4 LINEAR FEEDBACK SHIFT REGISTERS

Since the one-time cipher has been shown to be completely secure, one may try to simulate it using large linear feedback shift registers to produce pseudorandom key strings to XOR with the message. The initial settings of the shift register can be thought of as the key. Figure 2.2.4 shows a possible implementation of a shift register.

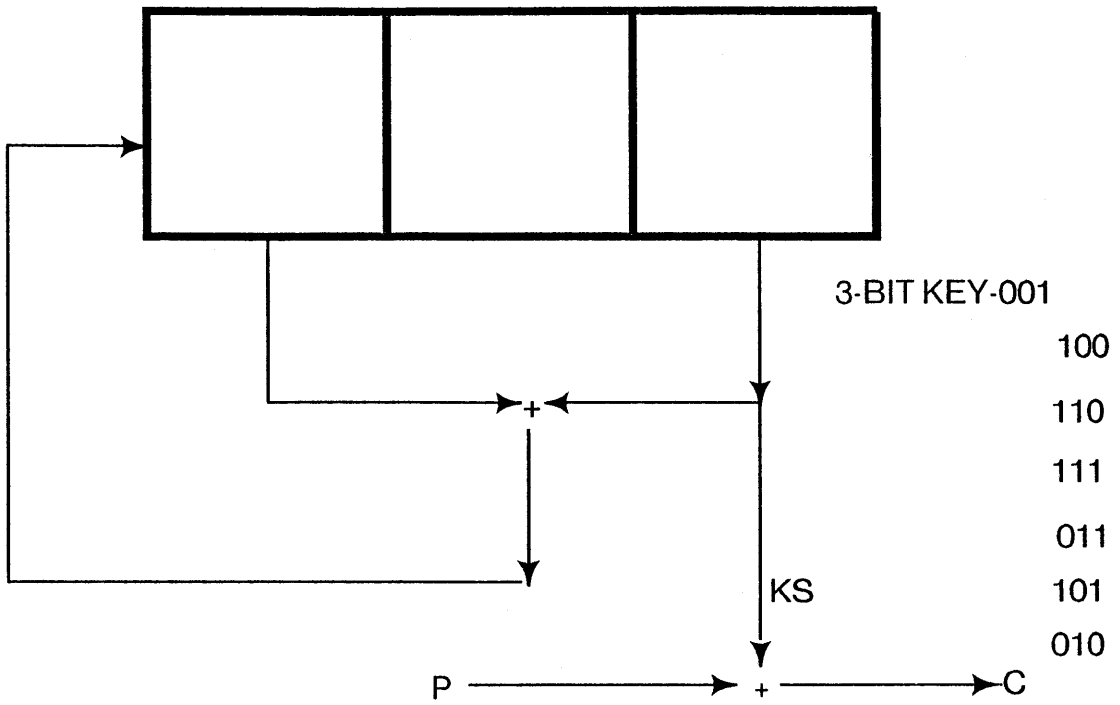


FIGURE 2.2.4

The figure above illustrates a three stage shift register. The first and second stages are added (mod 2) to form the next input to the shift register. The key is the initial inputs stored in the shift register. If the key is chosen to be 001 and the shift register is started, then the sequence of states after the initial key state are shown in figure 2.2.4. The shift register goes through seven non-zero states before returning to the key state, where the eighth possible state is never reached because it loops around itself. The period of seven is the largest possible number of states for a three stage shift register. In general, if there are x stages then there are 2^x-1 number of possible states in a loop.

In the figure, the plaintext is added (mod 2) to the third stage bits of the shift register to produce the ciphertext. Since the modulo two addition is self-inverse, the decryption is done in the same manner. The length of the loop or the period is dependent on the shift register taps. If taps were on all the stages instead of just the first and third stages, the maximum length of the loop would be four instead of seven. This system is not secure although it is meant to imitate a secure system.

2.3 COMMENTS ON OLD CONVENTIONAL SCHEMES

The above four schemes have been broken, either probabilistically or by other means. The main problem is the distribution of the keys, especially with conventional cryptographic schemes. This includes the recently proposed Data Encryption Standard. For the receiver and the sender to securely communicate the key, they must use a secure channel such as registered mail and set a time

to have cryptographic communications. The registered mail will take time and therefore key distribution has been a major problem in the use of cryptography. This key distribution problem is more pronounced in large scale networks, where the number of possible connections and keys grows on the order of n(n-1)/2 for n users. A system with a million users has almost 500 billion possible connections and the cost of key distribution can become too large to be done effectively.

2.4 DATA ENCRYPTION STANDARD (DES)

The DES is shown in figure 2.4.1. Based on S boxes, the 64 bit plaintext is first put through an initial permutation, and then the plaintext block is split into two sub-blocks. These 32 bit long sub-blocks are R0 and L0. The algorithm then switches the sub-blocks from left to right with the addition of a function on the right block, R, and the key block, K, for a total of 16 rounds.

$L(i) = R(i-1)$ and

$R(i) = L(i-1) \oplus F(R(i-1), K(i)) \pmod 2$

The $\oplus$ operation is a modulo two addition, K(i) is a 48 bit section of key that is used in the i-th round, and F is a function with a 32 bit output.

The function F need not be invertible to decrypt since L(i-1), and R(i-1) can be computed from L(i) and R(i) as follows:

$R(i-1) = L(i)$ and

$L(i-1) = R(i) \oplus F(L(i), K(i)) \pmod 2$

This works even if the function F(R,K) is an n-to-one mapping.

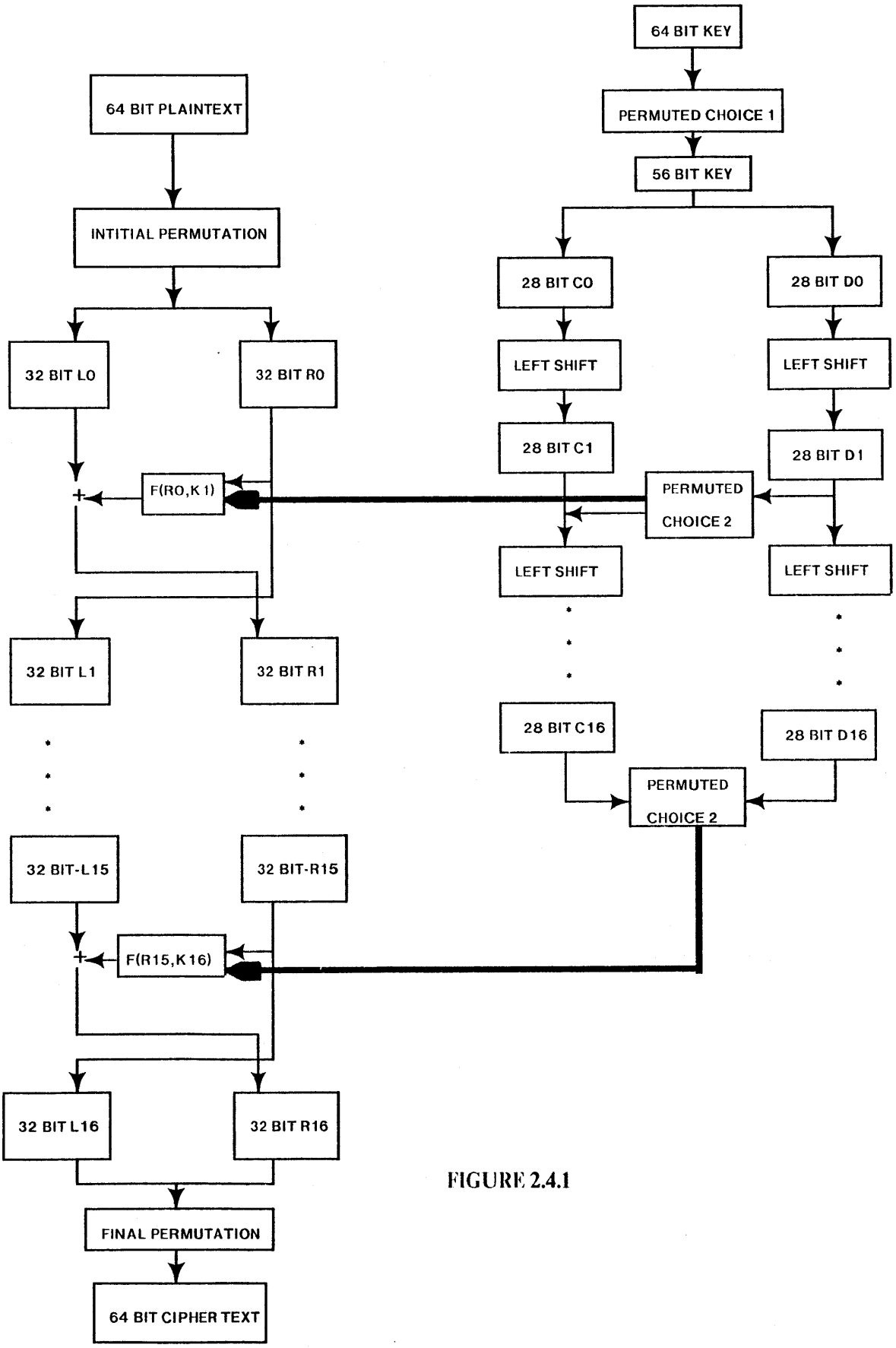

64 BIT KEY
PERMUTED CHOICE 1
56 BIT KEY
64 BIT PLAINTEXT
INTITIAL PERMUTATION
28 BIT C0
28 BIT D0
32 BIT L0
32 BIT R0
LEFT SHIFT
LEFT SHIFT
28 BIT C1
28 BIT D1
F(R0,K 1)
PERMUTED CHOICE 2
LEFT SHIFT
LEFT SHIFT
32 BIT L1
32 BIT R1
28 BIT C16
28 BIT D16
PERMUTED CHOICE 2
32 BIT-L15
32 BIT-R15
F(R15,K16)
32 BIT L16
32 BIT R16
FINAL PERMUTATION
64 BIT CIPHER TEXT

FIGURE 2.4.1

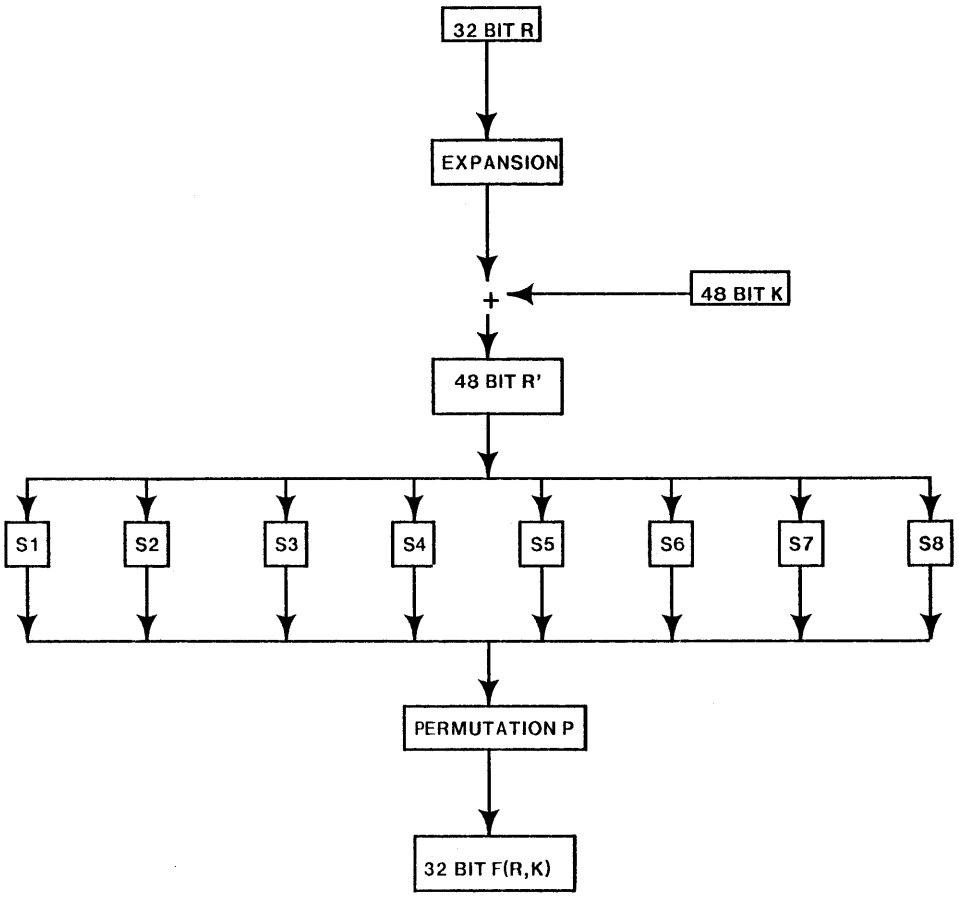


FIGURE 2.4.2

The algorithm for the function F is shown in figure 2.4.2. The S boxes are non-linear and will be the source of the security for DES. All the other operations are linear and can be cryptanalyzed. In function F, the 32 bit R is first expanded to 48 bits in R'. The extra sixteen bits are duplicated bits of the first 32 bits of R, (1, 4, 5, 8, 9, 12, ... , 24, 27, 28, and 32). These are the bits on the outside of each of the six bits that go into each of the S boxes. In other words, the first four bits of R go into the first S box along with bit 32 and bit 5. This process continues for all the S boxes. The repeated bits are added on cyclically to each four bit byte to make a six bit byte. If R is represented by r1, r2, r3, ... r32, then R' is represented by r32, r1, r2, r3, r4, r5, r4, r5, r6, r7, r8, r9, r8, r9, r10, r11, r12, r13, ... , r28, r29, r30, r31, r32, r1. After this is done, the 48 bit R' and part of the key, K, are added modulo two. They are then separated into six bit bytes input to each of the eight S boxes. The S boxes are non-linear because they input six bits but output four bits. Thus, there are 32 bits of output from the S boxes.

Since eight bits of the key are used for parity, the key has essentially 56 bits. From these, there must be 16 sets of 48 bit key for the sixteen rounds or sixteen sets of keys, k1 through k16 containing a total of 768 key bits. The key scheduling can be accomplished by using two 28 bit shift

registers with 24 taps each. These 48 taps provide the 48 bits of key used for each of the 16 rounds. After each round is encrypted, the shift register is shifted left to produce the next set of 48 bits of key. Since all of the operations in DES are linear except for the S boxes, there is still the criterion that the operation of encryption not be affine. If the S boxes are affine, then the whole operation of encryption is affine and would be of the following form:

$$C=AP\oplus BK\oplus D \pmod 2$$

where A, B, and D would be fixed, K is the 56 bit key, and C is the ciphertext. The knowledge of only one plaintext ciphertext pair would then allow the cryptanalyst to compute the key as follows:

$$K=(C-AP-D)1/B \pmod 2$$

The decryption algorithm for the ciphertext is the same algorithm used for the encryption of the plaintext, except the key scheduling algorithm is run in reverse.

2.5 COMMENTS ON THE DATA ENCRYPTION STANDARD (DES)

Diffie, Hellman, Merkle, Schroeppel, Washington, Pohlig, and Schweitzer made an attempt to cryptanalyze DES in August 1976. They found that the DES S boxes were not affine and discovered other structures, present in the DES algorithm, some of which strengthened, while others weakened the DES algorithm.

The positive structure found was this: each one bit change in input to the S boxes resulted in two bits of change in the output. This structure creates a large set of changes, even if only one bit of plaintext or key is changed. Therefore, the error propagation is large. This is good because it will hurt the cryptanalyst who tries a cluster analysis attack. In addition the permutation P and expansion E make the four outputs from any S box seemingly look like outputs from six different S boxes. This enhances error propagation and hinders the chances of cluster analysis.

The negative structure found was a deep symmetry in DES under complementation which halved the search effort under a chosen plaintext attack. If Sk denotes the enciphering using DES, k denotes the key, and P denotes the plaintext, and P denotes the plaintext, then:

$$C=Sk(P)\rightarrow Sk'(P')$$

where C', k', and P' are the complements of C, k, and P respectively. This symmetry, and the fact that

$$F(F,k)=F(ER\oplus k) \pmod 2\rightarrow F(R,k)=F(R',k')$$

brings the conclusion that F is invariant under complementation of R and k, where ER is the

expanded version of R.

This structure makes cryptanalysis quicker than a trial and error search for the key. Let P encipher to C and P' encipher to C'. If P, P' and C, C' are known (or can be found using a chosen plaintext attack), then enciphering P to C" under all possible keys with the least significant bit zero, one knows that if C" is not equal to C, then k is not the correct key. If C" is not equal to C', then k' is not the correct key as well. Since two keys can be tried for each encryption instead of only one the speed of attack is doubled.

DES is fast enough for high speed satellite communications, but the key distribution and key management problems may be too great for large scale communication networks. Therefore, the choice of DES does not have the desirable properties that a public-key cryptosystem has. Public-key cryptosystems alleviate some of the problems in the key distribution and key management. The combined use of public-key schemes for key distribution and DES for encryption/decryption alleviates the problem of key distribution.

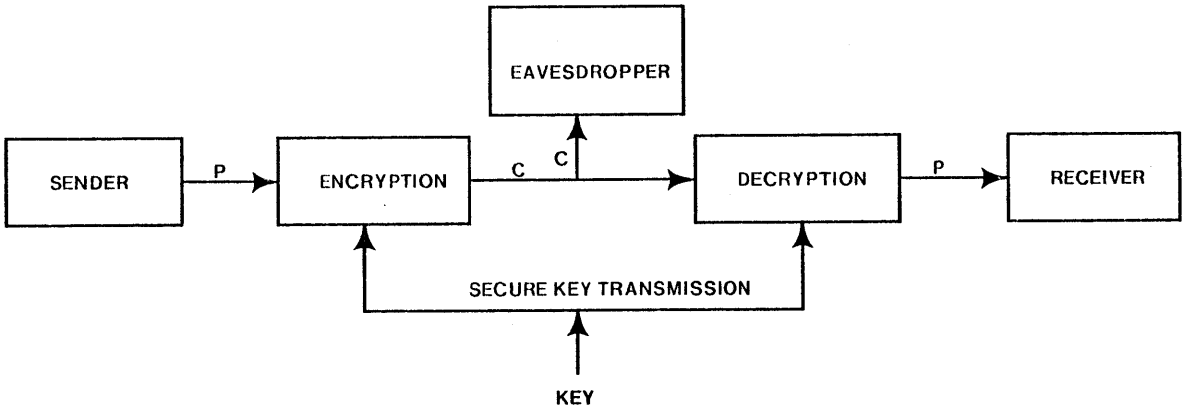
3 PUBLIC-KEY SCHEMES

3.1 INTRODUCTION

This chapter discusses several of the existing public-key schemes including the public-key schemes of: 1) Rivest-Shamir-Adleman (RSA); and 2) Merkle and Hellman (knapsack scheme). These two public-key schemes will be of interest when the Rabin scheme and Williams scheme are analyzed and shown to have some advantages and disadvantages when compared to other public-key schemes.

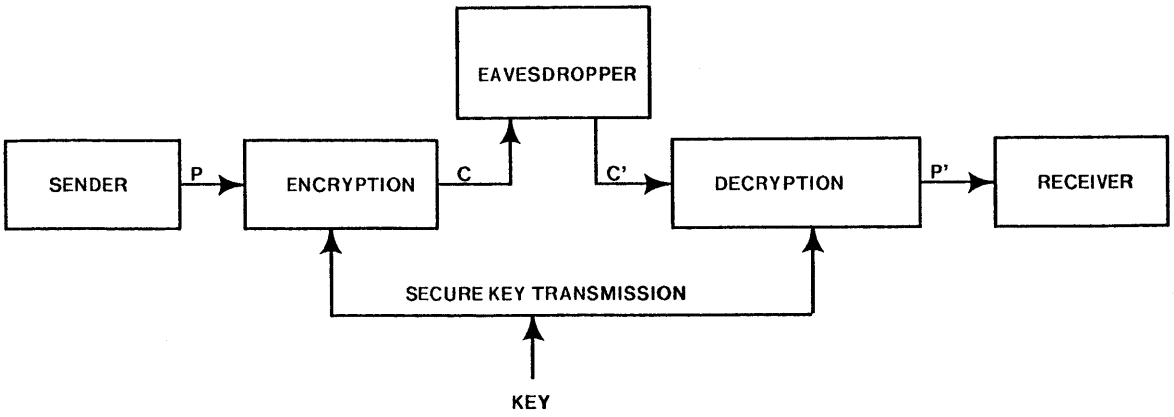
3.2 PUBLIC-KEY

Diffie and Hellman and, independently Merkle suggested a method to communicate securely without a secure key distribution channel. This method is called public-key and was invented to alleviate some of the problems in key distribution and key management discussed in chapter two. A normal conventional scheme for privacy and authentication, along with a public-key scheme, are represented in figures 3.2.1 to 3.2.3.



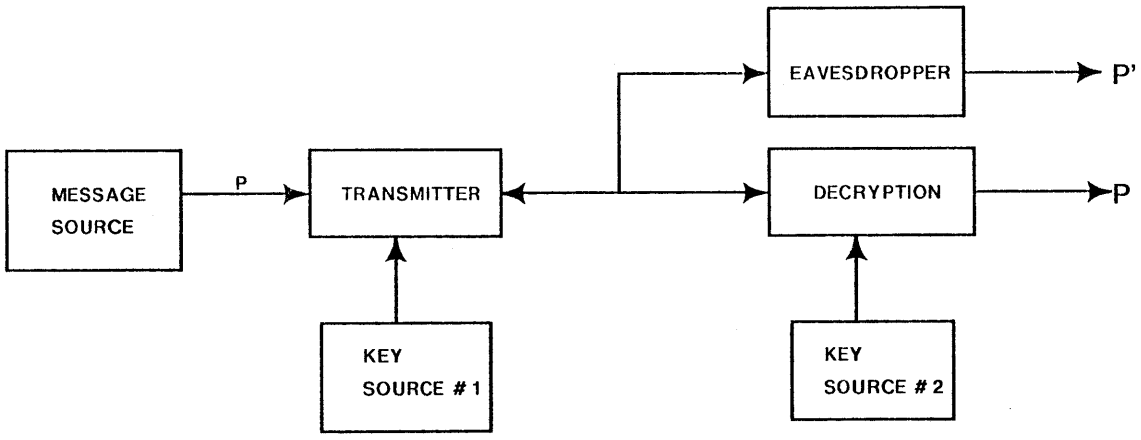
THE FLOW OF INFORMATION IN A CRYPTOGRAPHIC PRIVACY SYSTEM

FIGURE 3.2.1



THE FLOW OF INFORMATION IN A CRYPTOGRAPHIC AUTHENTICATION SYSTEM

FIGURE 3.2.2



THE FLOW OF INFORMATION IN A PUBLIC-KEY SYSTEM

FIGURE 3.2.3

Two problems with conventional schemes are privacy and authentication, as shown in figure 3.2.1 and figure 3.2.2. The privacy problem is to prevent an opponent from extracting information from a communication channel whereas the authentication problem is to prevent an opponent from injecting false data into the channel or altering the messages. Therefore, there is a need to securely transfer the key to the sender and the receiver. In the public-key scheme the secure key transfer link can be eliminated and only n secret keys need be used instead of as many as n^2. This alleviates the key management and key distribution problems.

In figure 3.2.3 the public-key system shows that communication between the transmitter and receiver can be accomplished while allowing an eavesdropper to listen to the communications. Since the keys are never transmitted, the eavesdropper cannot steal the key by listening. In public-key

cryptosystems there are separate keys for encryption and decryption. Keys must be protected in conventional schemes, because enciphering and deciphering require the same key, and the two functions are separated. Public-key systems separate the encryption and decryption functions and use two keys one for encryption and the other for decryption. Therefore, the encryption key does not have to be secret.

Public-key cryptosystems consist of separate encryption and decryption functions that are invertible and dependent on the key. The functions encrypt a message, m, to a cryptogram, c, and decrypt a cryptogram, c, to a message, m. The following properties exist in public-key systems: 1) for every key the decryption function, D, has an inverse, E, such that for any key, k, and any message, m, one has $D(E(m))=m$; 2) for every key and message the values of E(m) and D(c) are easy to compute; 3) for almost any key, any easily computed algorithm that is equivalent to D is computationally unfeasible to derive from E; and 4) for every key, it is feasible to generate the inverse pair, E and D, from the key.

The first property insures that the encryption algorithm has an inverse. The second property insures that the encryption and decryption algorithms are easy to apply. The third property insures that E can be made public without a loss of security on D, while the fourth property insures that once the key is known, there must be a method to compute E or D in a reasonable amount of time. The system alleviates the key distribution problem, since each user can generate E and D, and then make E public. Anyone can encrypt messages to the user, but no one else can decrypt the messages sent to him.

The authentication problem in conventional schemes is illustrated in figure 3.2.2. The figure shows how a conventional scheme can provide a method to prevent an eavesdropper from inserting false undetected messages into the system, although it does not provide a method to determine if messages are ever sent. The problem exists between the sender and the receiver, when the receiver says that a certain message was sent, but the sender denies this. The problem arises because the sender and receiver have the same keys.

Digital signatures can be used to alleviate the authentication problem. In extended public-key systems the authentication problem can be solved by the use of digital signatures. Extended public-key systems have the following property added: 5) for every key, E is the inverse of D so that for any k and any m, $E(D(m))=m$. The following method of digital signatures is described below. If user A sends a signed message to user B, he first calculates $S=D^{A}(m)$ which he uses as a signature, then user B calculates $E^{A}(S)=m$ to retrieve the message. User B can save S as proof that user A sent the particular message to him, since only A could have produced S. (Only A has $D^{A)}$. User A can be held responsible for producing signature S. This method of digital signatures provides an unforgeable message-dependent signature.

To include privacy into the extended public-key system, user A can calculate $E^{B}(S)=c$ and send this cryptogram to B. Since only B has D^{B}, he is the only one that can decrypt c with D^{B} to

retrieve $D^B(c)=S$ and can save S as proof that user A sent the message, m, to him. To prevent B from saying A sent the message more than once, user A can make the message time-dependent.

Public-key cryptosystems can alleviate some of the problems in key distribution and key management. In addition if property five is included in the public-key cryptosystems, it can provide digital signatures for solving the authentication problem.

3.3 RIVEST-SHAMIR-ADLEMAN SCHEME (RSA)

This scheme makes use of discrete exponentiations for its encryption and decryption with the assumption that factoring a number, the product of two large primes, is computationally unfeasible. Given two users, A and B, who wish to communicate with each other, A chooses two very large primes, p and q, and multiplies them together to get r. A then calculates $\Phi(r)=(p-1)(q-1)$ using p and q, and chooses another number, E^A, such that $(\Phi(r),E^A)=1$ and $1<E^A<\Phi(r)-1$, where (X, Y) is the g.c.d of X and Y. User A calls E^A his encryption function and puts E^A and r into a public file to be used by other users to encrypt messages to him. Typically encryption is done in blocks of 400-500 bits. Each block is encrypted by raising the message block, M, to the E^A power modulo r as follows:

$$C=M^{E^A} \pmod{r}$$

where C is the cryptogram block that represents the encrypted message block, M. In modular arithmetic calculations in the exponents is done modulo $\Phi(r)$. User A can calculate D^A by simply calculating the inverse of E^A modulo $\Phi(r)$. (Since E^A is relatively prime to $\Phi(r)$, this inverse can be found). Once this is accomplished, A can decrypt his message using D^A as follows:

$$M=C^{D^A}=(M^{E^A})^{D^A}=M \pmod{r}$$

Where E^A is the inverse of D^A modulo $\Phi(r)$.

3.4 COMMENTS ON THE RSA SCHEME

The RSA scheme is a very ingenious, but because of the exponentiation it is slow in comparison to conventional schemes such as DES. Presently the highest-speed implementation of the RSA scheme is only in the Kbit/sec range, whereas satellite communications require rates in the 1 to 10 Mbit/sec range. If the speed of the Rivest scheme could be increased in encryption or decryption, it would be a very viable scheme for satellite communications. With present limitations the RSA scheme can be used for public-key distribution.

Studies by Simmons and Norris have developed an attack on the RSA scheme by repeated

encryption of the cryptogram. This method has been rendered ineffectual by Rivest, choosing primes such that $\Phi(p)$ and $\Phi(q)$ have very large prime factors themselves.

Other studies, by Tore Herlestam, have developed an attack on the RSA scheme by taking the cryptogram to some power that is a polynomial in E. If $p=2p'+1$ and $q=2q'+1$, a choice Rivest stated to be secure against the Simmons and Norris attack, then the Herlestam method is supposedly able to attack the RSA scheme. Herlestam has relied heavily on fixed points to attack the RSA scheme. His method is as follows:

For $a=1, 2, \ldots m$ and for $n=1, 2, \ldots$, calculate:

$(c^{E^{(n+a)}})(c^{E^n}) \pmod r$ (1)

and

$(c^{E^n})(c^{E^a}) \pmod r$ (2)

If (1) or (2) is c for any a then

$m=(c^{E^{(n+a-1)}})(c^{E^{(n-1)}}) \pmod r$ if (1) is true or

$m=(c^{E^{(n-1)}})(c^{E^{(a-1)}}) \pmod r$ if (2) is true.

It relies heavily on the following:

$(E^{(n+a)})(E^n)=1 \pmod{p'}$ and $(E^n)(E^a)=1 \pmod{q'}$

This method appears to be very similar to the Simmons and Norris attack and is just a generalization of that attack. If n and a are always small, then the attack may be viable, although Herlestam gives no analytic proof of this. If a and n are large, then this attack is not feasible.

3.5 MERKLE AND HELLMAN SCHEME (KNAPSACK SCHEME)

The Knapsack scheme is based on the well known np-complete knapsack problem. The knapsack problem deals with a vector $B=(b_1, b_2, \ldots, b_n)$ of integers and some large integer Q. The problem is to find the vector $C=(c_1, c_2, \ldots, c_n)$ such that the dot product $B \cdot C$ is Q, which has been shown to be np-complete. The knapsack problem can be used in a public-key cryptosystem by simply dividing up the message M into n bit blocks and forming the bit vector $M=(m_1, m_2, \ldots, m_n)$. The dot product of M and B equals Q, and the knapsack problem is to recover the message M from Q. This is computationally unfeasible if B and M are randomly chosen. However, if B is chosen so that each element is larger than the sum of the preceeding elements, solving the knapsack problem is simple. Let B' be such a vector in which each element is larger than the sum of the preceeding

elements. Choose an integer, V, such that V is greater than the sum of all the elements in B', and choose U so that (U, V)=1. Given two users, A and B, user A forms the vector:

$$B=UB' \pmod V$$

With vector B in the public file, user B can communicate with A, by forming the dot product:

$$Q=B^{\bullet}M$$

User B then sends this, and user A can decrypt it by finding the inverse of U (mod V), i.e., U' such that

$$UU'=1 \pmod V$$

User A can decrypt the message by multiplying Q by U'. This leads to the solvable knapsack problem in which all the elements of B' are greater than the sum of the preceeding elements. The following demonstates the scheme analytically:

$$Q'=U'Q=U'\sum b_i m_i=U'(\sum Ub'_i \pmod V)m_i=(\sum U'Ub'_i \pmod V)m_i$$

$$=(\sum b'_i \pmod V)m_i=B'^{\bullet}M \pmod V$$

where V is greater than the sum of all the b's. Thenceforth, it is easy to compute the values for the vector M, since all the elements of B' are greater than the sum of the preceding elements.

3.6 COMMENTS ON THE KNAPSACK SCHEME

The knapsack scheme has a large bandwidth expansion caused by division of the message into bit vectors multiplied by the B' vector. Since some of the integers in B' are very large, the dot product of B' and M is also large. Therefore, even small messages require a very large number Q' in order to be sent, and although this scheme is faster than the RSA scheme, it is hindered by the bandwidth expansion.

Tore Herlestam has proposed a method to break the knapsack scheme, which involves the choice of a prime p, greater than the integers of the vector B, and an index i so that $1 \leq i \leq n$. He then computes a W such that $Wb_i=1 \pmod p$ and lets $B'=WB \pmod p$ and $Q'=WQ \pmod p$. If $b'_n > b'_1 + b'_2 + \ldots b'_{(n-1)}$ and $Q' + p > b'_1 + b'_2 + \ldots b'_n$, then m_n can easily be determined. The value of m_n will be one, if Q' is greater than b'_n, or zero, if Q' is less than b'_n. Then the knapsack problem can be reduced to the remaining elements of the B' and M vectors and whatever is left of A' after $b'_n m_n$ is subtracted from it. Therefore, the reduced knapsack problem is as follows:

$$Q' - b'_n m_n = b'_1 m_1 + b'_2 m_2 + \ldots + b'_{(n-1)} m_{(n-1)}.$$

This reduced knapsack problem can be solved by successively choosing new p's until one is found which follows the criteria. However, for large vectors this method is computationally infeasible.

4 THE RABIN SCHEME AND WILLIAMS SCHEME

4.1 INTRODUCTION

This chapter discusses: 1) the Rabin scheme; 2) how the decryption of the Rabin scheme is equivalent to factoring r; 3) the Williams scheme and how it solves the ambiguity problem; and 4) how the decryption of the Williams scheme is equivalent to factoring r. The structure of the proofs for the theorems and lemmas are due to Rabin and Williams.

4.2 THE RABIN SCHEME

This newly proposed scheme is similar to the Rivest scheme and deals with two very large primes, p and q, where p and q must be of the form 4k+1 or 4k-1. The primes p and q are multiplied together to get r. A user, A, chooses the primes p and q and a constant b and places b and r into a public file. The message, m encrypts to the cryptogram, z. The encryption is as follows:

$$z = m(m+b) \pmod{r}$$

The decryption is a bit more difficult, since the receiver must solve the following equation for m:

$$z = m^2 + b*m \pmod{r}.$$

Let

$$x_1 = z \pmod{p} \text{ and}$$

$$x_2 = z \pmod{q},$$

then user A must solve the following:

$$m^2 + m*b - x_1 = 0 \pmod{p} \text{ and}$$

$$m^2 + m*b - x_2 = 0 \pmod{q}.$$

These equations can be solved using the quadratic formula so that:

$$m_1 = \frac{(-b + \sqrt{(b^2 - 4*x_1)}}{2} \pmod{p}$$

$$m_2=\frac{(-b-\sqrt{(b^2-4*x_1)}}{2} \pmod p$$

$$m_3=\frac{(-b+\sqrt{(b^2-4*x_2)}}{2} \pmod q$$

$$m_4=\frac{(-b-\sqrt{(b^2-4*x_2)}}{2} \pmod q.$$

Once the square root is calculated, user A finds four solutions, m_1, m_2, m_3, and m_4 and using the Chinese remainder theorem the four solutions to the cryptogram z can be found. The four solutions cause an ambigtuity problem, since the receiver can not easily determine the original message from the four solutions. To take square roots user A must solve

$$y^2-m=0 \pmod p \qquad (1).$$

Assume first that $p=4k-1$ so that $4|p+1$. Since m is a quadratic residue, then

$$m^{((p-1)/2)}=1 \pmod p.$$

One of the square roots can be written as

$$j=\sqrt{m}=m^{((p+1)/4)} \pmod p.$$

Then,

$$j^2=m^{(p+1/2)}=m(m^{((p-1)/2)})=m \pmod p.$$

If $p=4k+1$, user A can solve equation (1) directly using a probabilistic algorithm.

4.3 HOW THE DECRYPTION OF THE RABIN SCHEME IS EQUIVALENT TO FACTORING THE MODULUS

The structure of the following proof is due to Rabin and can be found in "Digitalized Signatures and Public-Key Functions as Intractable as Factorization". The Rabin scheme encryption algorithm is

$$z=m(m+b) \pmod r \qquad (*).$$

By a substitution of variables this can be reduced to $y^2 = n \pmod r$, where $n=z+d^2$ and $b=2*d \pmod r$. Substituting into (*), one gets the following:

$$m^2+2*d*m+d^2 = (m+d)^2 = n \pmod r.$$

where, clearly $y=(m+d) \pmod r$. Now to prove the equivalence of decryption to factorization, one proves the following theorem.

THEOREM: Let AL be an algorithm for finding one of the solutions of

$$y^2 = n \pmod r \qquad (***)$$

whenever a solution exists. Suppose F(r) steps are required. Then there is an algorithm for factoring r requiring $2F(r)+2*\log_2 r$ steps.

PROOF: Assume that $r=p*q$ is a product of two large primes. Then for any k in the range $0<k<r$ and $(k,r)=1$, there are exactly four-solutions to the equation:

$$y^2 = k^2 \pmod r \qquad (**)$$

Letting $t=k \pmod p$ and $s=k \pmod q$, the four-solutions by the Chinese remainder theorem are $\pm t \pmod p$ and $\pm s \pmod q$. Each of the four numbers mod r is a solution. Now for any u and v such that $0 \leq u, v \leq r$ and $u^2=v^2 \pmod r$, solutions to (**) can be divided into classes containing four-solutions for $(y,r)=1$; two-solutions for $(y,r)=p$ or q; and one-solution for $(y,r)=r$.

Since AL just performs a square root function, let $n^{1/2}$ be the solution of the equation (***) for any n with $(n,r)=1$.

Now choose a random number k such that $0<k<r$. If $(k,r)\neq 1$, then one can immediately get a factor because $(k,r)=p$ or q. On the other hand if $(k,r)=1$, which is normally the case, one can still factor r.

Using AL to find one-solution, $k_1=n^{1/2}$. The solutions occur in classes, so by choosing a random number k, all the solutions in that class have an equal probability of being chosen. Now for $(y,r)=1$ there are four-solutions per class, so there is equal probability of ¼ for each of the following:

$k=k_1 \pmod p$, and $k=k_1 \pmod q$ or
$k=-k_1 \pmod p$, and $k=k_1 \pmod q$ or
$k=k_1 \pmod p$, and $k=-k_1 \pmod q$ or
$k=-k_1 \pmod p$, and $k=-k_1 \pmod q$.

So that with probability of ½ one has:

$k=k_1 \pmod p$, and $k=-k_1 \pmod q$ or

$k=-k_1 \pmod p$, and $k=k_1 \pmod q$.

Thus one has with probability ½ that

$(k-k_1, n) = p$ or q.

The computation of $n^{1/2}$ requires F(r) steps, while the computation of the g.c.d requires at most $\log_2 r$ subtractions and divisions by 2, of numbers smaller than n. Thus the expected number of steps to factor r, given AL, is $2*F(r)+2*\log_2 r$. ***QED.***

This proof can easily be extended to the general case.

4.4 THE WILLIAMS SCHEME AND HOW IT SOLVES THE AMBIGUITY OF THE RABIN SCHEME

The Williams scheme solves the ambiguity problem of the Rabin scheme. The encryption and decryption functions are different from those of the Rabin scheme and consists of two encryption functions E^1 and E^2 along with two decryption functions D^1 and D^2.

In the Williams scheme there are two large prime numbers, p and q, whose product is the modulus $r=p*q$ and for reasons to be seen later the preimes have a special form. Prime p is congruent to 3 (mod 8) and q is congruent to 7 (mod 8). The first encryption function is as follows:

Let m be a message in *M* subject to the following restrictions:

$(2(2*m+1)) < r$ if $(2*m+1 \mid r) = -1$ or
$(4(2*m+1)) < r$ if $(2*m+1 \mid r) = 1$.

The first part of the encryption process is as follows:

$$n=E^1(m)=\begin{cases}(2(2*m+1)) & \text{if } (2*m+1 \mid r) = -1\\ (4(2*m+1)) & \text{if } (2*m+1 \mid r) = 1.\end{cases}$$

The second encryption function, E^2 depends on an exponent e having the property that $(e, \lambda(r))=1$, where $\lambda(r)=$ lcm(p-1,q-1). Since we want the smallest quantity x such that $m^x=1 \pmod r$, $\lambda(r)$ can be used instead of $\Phi(r)$. One then calculates d such that $e*d=(((p-1)*(q-1)/4-1)/2) \pmod{\lambda(r)}$ and uses the encryption:

$g=E^2(n)=n^e \pmod r$.

The encrypted message is sent, whereupon the receiver takes the cryptogram g and decrypts it using the two decryption functions. The first is as follows:

$h = D^2(g) = g^{2d} \pmod{r}$.

Now the receiver can decode the reduced cryptogram h with the following rule to make h even:

$$h = \begin{cases} h & \text{if } h \text{ is even} \\ r-h & \text{if } h \text{ is odd.} \end{cases}$$

Then use the following rule to compute m:

$$m = \begin{cases} ((h/4 - 1)/2) & \text{if } h = 0 \pmod 4 \\ ((h/2 - 1)/2) & \text{if } h = 2 \pmod 4. \end{cases}$$

To show that this is a valid encryption and decryption scheme, one must show that $D^1(D^2(E^2(E^1(m)))) = m \pmod r$. Since $n = E^1(m)$, n must be even, $0<n<r$, and $(n|r) = 1$.

$$h = D^2(E^2(n)) = n^{2ed} = n^{((p-1)(q-1)/4+1)} = \pm n.$$

This last equality is true because of the lemma: If $r = p*q$, and p, q are such that $p = q = -1 \pmod 4$, and $(m|r) = 1$, then,

$$m^{(p-1)(q-1)/4} = \pm 1 \pmod r.$$

Since $(m|p*q)$, $(m|p) = (m|q)$, so there are two cases:

If $(m|p) = (m|q) = 1$ implies that

$$m^{(p-1)/2} = 1 \pmod p \rightarrow m^{(p-1)(q-1)/4} = 1 \pmod p, \text{ and}$$
$$m^{(q-1)/2} = 1 \pmod q \rightarrow m^{(p-1)(q-1)/4} = 1 \pmod q$$
$$\text{then } m^{(p-1)(q-1)/4} = 1 \pmod r.$$

Conversely if $(m|p) = (m|q) = -1$ implies that

$$m^{(p-1)/2} = -1 \pmod p \rightarrow m^{(p-1)(q-1)/4} = -1 \pmod p, \text{ and}$$
$$m^{(q-1)/2} = -1 \pmod q \rightarrow m^{(q-1)(p-1)/4} = -1 \pmod q$$
$$\text{then } m^{(p-1)(q-1)/4} = -1 \pmod r.$$

The first two implications are true because (p-1)/2 and (q-1)/2 are odd, so that -1 to an odd power is still -1.

Therefore, if h is even, then $h = n$; if h is odd, then $h = -n$ or $h = r-n$. If $h = 0 \pmod 4$, then the encryption was of the form $4(2m+1)$, and the decryption will be $m = (h/4-1)/2$. Conversely, if $h = 2 \pmod r$, then the encryption was of the form $2(2m+1)$, and the decryption will be $m = (h/2-1)/2$. The cases where $h = 1 \pmod 4$ are the same as $h = 0 \pmod 4$, once h is replaced by r-h. The

cases where $h=3 \pmod 4$ are the same as $h=2 \pmod 4$, once h is replaced by r-h.

4.5 HOW THE DECRYPTION OF THE WILLIAMS SCHEME IS EQUIVALENT TO FACTORING THE MODULUS

This section will discuss the equivalence of the decryption in the Williams scheme to the factoring of r. The structure of the proof is due to Williams and can be found in "A Modification of the RSA Public-Key Encryption Procedure". This proof follows from a set of lemmas which depend on the fact that $r=p*q$.

LEMMA 1: If one selects any integer x such that $(x|r) = -1$, then there exists some integer γ such that $0 \leq \gamma \leq (\log_2 r)/2$ and some message $m \in M$ such that $E(m) = k$, where $k=2^{-4\gamma e} x^2 \pmod r$.

LEMMA 2: $r=p*q$ and $p=q=-1 \pmod 4$, so for any given integer x there exists an integer y such that $y^2 = x^2 \pmod r$ and $(y|r)=-(x|r)$. (This is essentially the four-decryption case with the solutions $\pm x \pmod p$ and $\pm x \pmod q$ to be detailed later).

PROOF OF LEMMA 2: Let $y=-x \pmod p$ and $y=x \pmod q$. Then $y^2=x^2 \pmod{p*q}$ and therefore

$(y|r)=(y|p)(y|q)=(-x|p)(x|q)=-(x|r)$. ***QED.***

PROOF OF LEMMA 1: Now from lemma 2 there exists some y such that $x^2=y^2 \pmod r$ such that $(y|r)=-(x|r)=1$. Let n^* be the solution of

$z^e=y \pmod r$ (note this implies $z^{2e}=y^2=x^2 \pmod r$)

such that $0<n^*<r$. Then to make n^* even, define n' to be

$$n' = \begin{cases} n^* & \text{if } n^* \text{ is even} \\ r-n^* & \text{if } n^* \text{ is odd.} \end{cases}$$

Next factor all the 4's out of n' so that $n'=2^{2\gamma}$, where 2|n and 8 does not divide n. Taking the logs of both sides one obtains

$2\gamma \log_2 n = \log_2 r$
$0<2\gamma<\log_2 r$
$0<\gamma<\log_2 r/2$.

We have $(n'|r)=(y|r)=1$, because $n'^e=y \pmod r$, so $(n'|r)^e=(y|r)$. Since $(e,\text{lcm}[p-1,q-1])=1$ and $\text{lcm}[p-1,q-1]=2$, e must not be even . If e is odd the only way to have $(n'|r)^e=(y|r)=1$ is to have

$(n'|r)=1$.

The value of $(2|r)$ is always -1, because $(2|p)=1$ and $(2|q)=-1$. The equality $n'=2^{2\gamma}n$ implies that $(n'|r)=(2|r)^{2\gamma}(n|r)$. The value of $(2|r)^{2\gamma}$ must be 1 because -1 raised to an even power is 1. This implies that $(2|r)^{2\gamma}(n|r)=(n|r)=(n'|r)=1$ and finally $(n|r)=(n'|r)=(y|r)=1$.

If this is the case, there must exist some $m \in M$ such that $E^1(m)=n$. Since $(n|r)=1$ and $2|n$ or even $4|n$, one can use $D^1(n)$ to find an m that satisfies the values of n. Also, one has

$$E^2(n)=n^{2e}=(2^{-2\gamma}n')^{2e}=2^{-4\gamma e}\ x^2 \pmod{r}.$$

Letting $k=2^{-4\gamma e}\ x^2 \pmod{r}$ $(0<k<r)$, it is easily seen that $E(m)=k$. ***QED.***

LEMMA 3: If $p=7 \pmod 8$ and $q=3 \pmod 8$, with $r=p*q$ and $(x|r)=-1$, then there exists an integer z such that $x=\pm 2z^2 \pmod{r}$.

PROOF OF LEMMA 3:

Once again there are two cases in the proof.

CASE 1: If $(x|p)=1$ and $(x|q)=-1$, then there must exist an integer z_1 such that $x=2z_1^2 \pmod{p}$. This is true because 2 is a quadratic residue for $p=8k+7$ and $x/2$ is also a quadratic residue; thus, z_1 is the square root of $x/2$. This square root is guaranteed to exist since $x/2$ is a quadratic residue. The value of $x/2$ must be a quadratic residue since x and 2 are both quadratic residues. In addition there must exist an integer z_2 such that $x=2z_2^2 \pmod{q}$. This is true because 2 is a non-quadratic residue for $q=8k+3$ and $x/2$ is a quadratic residue; thus, z_2 is the square root of $x/2$. This square root is guaranteed, since $x/2$ is a quadratic residue. The value of $x/2$ must be a quadratic residue, since x and 2 are both quadratic non-residues. ***QED.***

CASE 2: If $(x|p)=-1$ and $(x|q)=1$, then there must exist an integer z_1 such that $x=-2z_1^2 \pmod{p}$. This is true because -2 is a quadratic non-residue for $p=8k+7$ and $-x/2$ is a quadratic residue; thus, z_1 is the square root of $x/2$. This square root is guaranteed to exist since $-x/2$ is a quadratic residue. The value of $-x/2$ must be a quadratic residue since x and -2 are both quadratic non-residues. In addition, there must exist an integer z_2 such that $x=-2z_2^2 \pmod{q}$. This is true because -2 is a quadratic residue for $q=8k+3$ and $-x/2$ is a quadratic residue; thus, z_2 is the square root of $-x/2$. This square root is guaranteed, since $-x/2$ is a quadratic residue. The value of $-x/2$ must be a quadratic residue, since x and -2 are both quadratic residues. ***QED.***

LEMMA 4: If $(y|r)=1$ and $(x|r)=-1$ and $r=p*q$, then $(y-x,r)=p$ or q.

PROOF OF LEMMA 4:

In this lemma there are again different cases in the proof.

CASE 1; If $(y|p)=(y|q)=1$ and $(x|p)=1$ and $(x|q)=-1$, then

$(x|p)=(y|p)\rightarrow$
$x=y \pmod{p}\rightarrow$
$x=y+np$
$x-y=np$ or more simply $p|(x-y)$.

In order to show $(x-y,r)=p$ or q and not r, it must be ascertained that $q|(x-y)$ is not true. Assume that it is true. We have,

$x-y=nq$,
then $x=y \pmod{q}$
and $(x|q)=(y|q)$

which is a contradiction. Therefore $q|(x-y)$ is not true and only $p|(x-y)$, which means $(x-y,r)=p$. ***QED.***

CASE 2; If $(y|p)=(y|q)=1$ and $(x|p)=-1$ and $(x|q)=1$, reverse the roles of p and q. This reverts back to case 1. ***QED.***

CASE 3; If $(y|p)=(y|q)=-1$ and $(x|q)=1$ and $(x|p)=-1$, then this is the same as case 1. ***QED.***

CASE 4; If $(y|p)=(y|q)=-1$ and $(x|q)=-1$ and $(x|p)=1$, then this is the same as case 2. ***QED.***

Now by letting $K=\{K|K=E(m),\ m \in M\}$., this leads to the equivalence theorem.

THEOREM OF EQUIVALENCE; If for any $K=E(m) \in K$ there exists an algorithm F such that F can be applied to find m, then F can also be used to factor r.

PROOF OF EQUIVALENCE; Choose any x such that $(x|r)=-1$. Then all such values of x are characterized by lemma 3. By lemma 1 there must exist some γ such that $0 \leq \gamma < \log_2 r/2$ and some $m \in M$ such that,

$E(m)=K$,

where $K=(2^{-2\gamma e}x)^2 \pmod{r}$. Since $K \in K$, one can use F to find m. By letting $y=E^1(m)^e \pmod{r}$, one then has

$y^2=K=(2^{-2\gamma e}x)^2 \pmod{r}$.

Then since $(y|r)=1$, one has $(2^{-2\gamma e}x|r)=-1$. By lemma 4

$$(y\text{-}2^{-2\gamma e}x,r)=p \text{ or } q,$$

but, since $(2^{-2\gamma e},r)=1$, one can state that

$$(2^{2\gamma e}y\text{-}x,r)=p \text{ or } q. \quad \textbf{\textit{QED.}}$$

5 CRYPTOGRAMS WITH MULTIPLE SOLUTIONS IN THE RABIN SCHEME

5.1 INTRODUCTION

This chapter discusses how many decryptions each possible cryptogram may have in the Rabin scheme. The cases are: 1) one-decryption; 2) two-decryptions; and 3) four-decryptions. Additional properties will be discussed in the next two chapters. The properties lead to several very interesting cryptanalytic attacks on the Rabin scheme, some of which are counterintuitive, while other properties are very intuitive.

5.2 NUMBER OF DECRYPTIONS

Rabin stated that decryption under the Rabin scheme yields four solutions. In fact a cryptogram has either four solutions, two solutions, one solution, or no solution. This leads to many algorithms for potential attacks on the Rabin scheme. However, these attacks have a low probability of success. The existence of multiple solutions makes the decrypting difficult. In this section we discuss the number of solutions for any particular cryptogram and the reasons for the different possibilities.

Rabin's decryption algorithm begins by evaluating the cryptogram, z, modulo p and q, obtaining:

$x_1 = z \pmod{p}$ and
$x_2 = z \pmod{q}$.

The quadratic formula for solving quadratic equations can be used on each of the x's to find m s.t. $m(m+b) = z \pmod{p}$. There are two solutions from the quadratic formulas for each of the x_1 and x_2. Four-solutions messages can be found by combining the two solutions for x_1 and the two solutions for x_2 using the Chinese remainder theorem. This is only true if the discriminant of each of the quadratic formulas is non-zero. If the discriminant of the quadratic formula is zero for only one of the x's, then there will be only one solution for that particular x and two solutions for the other x. Two-solutions messages can be found by combining the one solution for one of the x's with the two solutions for the other x using the Chinese remainder theorem. Finally, if the discriminant is zero for both x_1 and x_2, then the quadratic formula will yield only one solution for x_1 and one solution for x_2. One-solution message can be found by combining the one solution for x_1 and the one solution for x_2 using the Chinese remainder theorem. This one-solution message is the original message. Unfortunately, there is no apparent method to determine how many solutions a cryptogram has a priori. The analytic discussion is as follows:

Encoding:

Let $z=m(m+b) \pmod r$, $r=p*q$ (*).

Decoding:

Let $x_1=m(m+b) \pmod p$ (1).

Let $x_2=m(m+b) \pmod q$ (2).

Then let:

$$m_{11}=\frac{-b+\sqrt{(b^2-4*x_1)}}{2} \pmod p \quad (3).$$

$$m_{12}=\frac{-b-\sqrt{(b^2-4*x_1)}}{2} \pmod p \quad (4).$$

$$m_{21}=\frac{-b+\sqrt{(b^2-4*x_2)}}{2} \pmod q \quad (5).$$

$$m_{22}=\frac{-b-\sqrt{(b^2-4*x_2)}}{2} \pmod q \quad (6).$$

Using the quadratic formulas, m_{11} and m_{12}, are the solutions of equation (1), and using m_{21} and m_{22}, are the solutions of equation (2). Since m_{11} and m_{12} are the solutions to (1), and m_{21} and m_{22} are the solutions to (2), four possible solutions can be found to (*) using the Chinese remainder theorem. The four-solutions messages are as follows:

$m_1=c_1*m_{11} + c_2*m_{21} \pmod{p*q}$,

$m_2=c_1*m_{11} + c_2*m_{22} \pmod{p*q}$,

$m_3=c_1*m_{12} + c_2*m_{21} \pmod{p*q}$, and

$m_4=c_1*m_{12} + c_2*m_{22} \pmod{p*q}$,

where $c_1=q*q^{-1}=1 \pmod p$ and $c_2=p*p^{-1}=1 \pmod q$.

Another way to view this property is to observe the cross-product of primes resulting in the four-solutions, two-solutions, and one-solution messages. Applying a change of variable as in chapter four, the Rabin scheme reduces to:

$n=y^2 \pmod r$

For this case the four-solutions messages will be $\pm y \pmod p$ and $\pm y \pmod q$. The four solutions to the quadratic formulas, m_{11}, m_{12}, m_{21}, and m_{22} can be combined using the Chinese remainder theorem to get the above four-solutions messages. This is best illustrated in the cross-product table below:

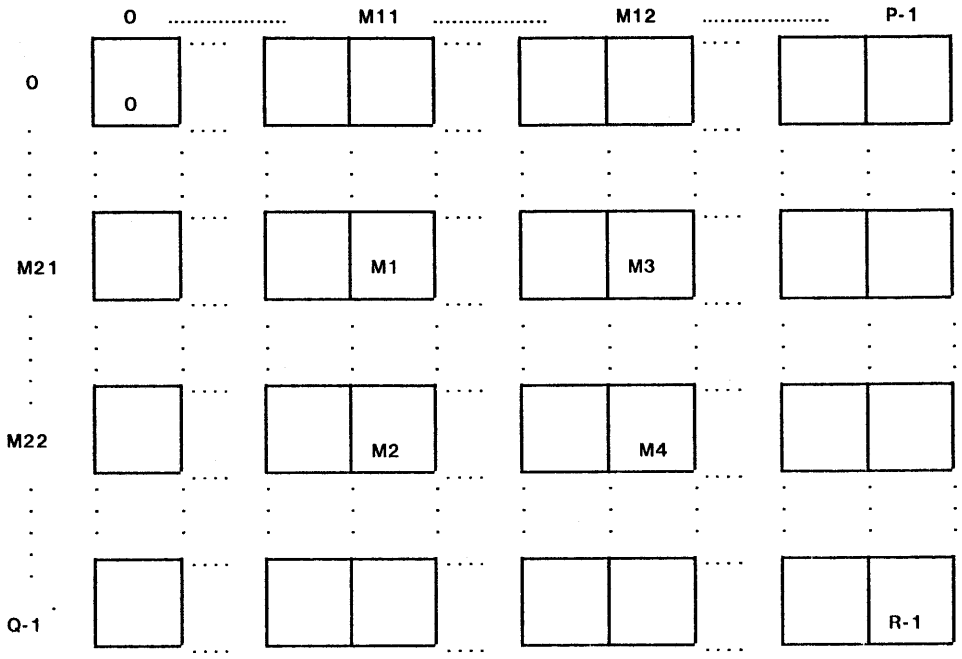


Figure 5.2

In the figure the columns represent the residues modulo q and the rows represent the residues modulo p. The entries in the table are the residues modulo r which are found by combining the residues modulo q and p using the Chinese remainder theorem. From the figure, it is evident that the four solutions to the quadratic equations can be combined to form four-solutions messages. Using the cross-product table the four four-solutions messages lie directly below m_{11} and m_{12}, and directly across from m_{21} and m_{22}. If the discriminant of only one of the quadratic equations is zero, then $m_{11}=m_{12}$ or $m_{21}=m_{22}$. Using the cross-product table again, the two-solutions messages lie directly below m_{11} and/or m_{12}, and directly across from m_{21} and/or m_{22}. As before if both discriminants are zero, then $m_{11}=m_{12}$ and $m_{21}=m_{22}$. Using the cross-product table again, the one-solution message lies directly below m_{11} and directly accross from m_{22}.

5.3 ONE DECRYPTION

This section discusses the various properties of the one-solution message and cryptogram. Usually, there will be four-solutions as was stated in the previous section, but if the discriminant is zero for both quadratic equations, then there will be only one solution (mod p) and only one solution (mod q). These two solutions can then be combined using the Chinese remainder theorem to retrieve the original message sent. This is the only case in which the decryption function is a one-to-one and onto mapping from the cryptogram to the message. Other cases result in multiple solutions and a degree of ambiguity.

If the discriminant, $\sqrt{(b^2-4*x)}$, is zero for both quadratic equations, there is only one solution. The equations (3-6) reduce to the following:

$m_{11}=-b/2 \pmod{p}$,

$m_{12}=-b/2 \pmod{p}$,

$m_{21}=-b/2 \pmod{q}$, and

$m_{22}=-b/2 \pmod{q}$.

This is the degenerate case where $m_{11}=m_{12}$ and $m_{21}=m_{22}$. Combining these two equations with the Chinese remainder theorem, one obtains the true message:

$m=c_1*m_{11} + c_2*m_{21} \pmod{p*q}$.

For any b, the output remains the same in terms of solutions and the distance between the four-solutions, two-solutions and one-solution cryptograms remains the same (this fact will be discussed later). In other words, the number of solutions for each cryptogram relative to the number of solutions for other cryptograms in the cryptogram spectrum remains the same. The cryptogram spectrum is all of the possible cryptograms. An interesting case is $b=0$, where the message equal to zero causes the single one-solution cryptogram.

If $b=0$ and $m=0$, then

$z=m^2=0 \pmod{r}$,

and z has only one solution, and it is unique.

When $b\neq 0$, the message corresponding to the one-solution cryptogram can still be found easily by applying the Chinese remainder theorem to $-b/2 \pmod{p}$ and $-b/2 \pmod{q}$. It can be shown that for b odd the one-solution message is $(r-b)/2 \pmod{r}$, and for b even the one-solution message is $(r-1-b)/2 + (r-1)/2 \pmod{r}$.

If the cryptogram was simply $z=m^2 \pmod p$, it would be evident from the theory of quadratic residues that one half of the cryptograms would be the same as the other half. In the Rabin scheme if one considers $b=0$, then $z=m^2 \pmod{p*q}$, and there must be a duplication of cryptograms. This interesting phenomenon is called the duplication property in which the cryptograms are duplicated around the one-solution cryptogram. In the modulo p case all messages that are between 1 and (p-1)/2 encrypt to the same cryptograms as messages that are between (p-1)/2+1 and (p-1) respectively. So all of the cryptograms are duplicated except the one at zero. However, all the messages that are between 1 and (p-1)/2 encrypt to different cryptograms. For modulo $r=p*q$ case, all the messages between 1 and (r-1)/2 also encrypt to the same cryptograms as messages between (r-1)/2+1 and (r-1). Thus, all of the cryptograms are duplicated except the one at zero. However, not all the messages between 1 and (r-1)/2 encrypt to different cryptograms. In fact, there may be at most two messages within half of the message spectrum that encrypt to the same cryptogram. From the discussion it is clear that all of the cryptograms that are caused by messages between 0 and (r-1)/2 are the same as cryptograms caused by messages between (r-1)/2+1 and (r-1). Therefore, each cryptogram has a mirror image about the one-solution cryptogram, and the $r=p*q$ case is a mere extension of the quadratic residue property.

There is only a single one-solution message and one-solution cryptogram. An attack on the Rabin scheme cannot be made just by knowing the one-solution message and/or the one-solution cryptogram. Both the one-solution message and the one-solution cryptogram can always be found, (since it is the encrypted version of the one-solution message) but, they do not provide a means to break the Rabin scheme.

5.4 TWO DECRYPTIONS

5.4.1 PROPERTIES OF TWO DECRYPTIONS

This section discusses the various properties of the two-solutions messages and cryptograms. Usually, there will be four-solutions as was stated in one of the previous sections. If the discriminant is zero for only one of the quadratic equations, then there will be either only one solution (mod p) and two solutions (mod q), or two solutions (mod p) and only one solution (mod q). These three solutions can then be combined using the Chinese remainder theorem to retrieve two possible messages that are encrypted to the same cryptogram.

If the discriminant-$\sqrt{(b^2-4*x)}$ is zero for one of the quadratic equations, then there are only two-solutions. The equations (3-6) reduce to the following:

$$m_{11}=\frac{-b+\sqrt{(b^2-4*x_1)}}{2} \pmod{p},$$

$$m_{12}=\frac{-b-\sqrt{(b^2-4*x_1)}}{2} \pmod{p},$$

$m_{21}=-b/2 \pmod{q}$, and

$m_{22}=-b/2 \pmod{q}$;

or

$m_{11}=-b/2 \pmod{p}$,

$m_{12}=-b/2 \pmod{p}$,

$$m_{21}=\frac{-b+\sqrt{(b^2-4*x_2)}}{2} \pmod{q}, \text{ and}$$

$$m_{22}=\frac{-b-\sqrt{(b^2-4*x_2)}}{2} \pmod{q}.$$

This is the degenerate case where $m_{21}=m_{22}$ or $m_{11}=m_{12}$. Depending upon which of the above cases is true, one can combine three equations using the Chinese remainder theorem to retrieve either

$m_1=c_1*m_{11} + c_2*m_{21} \pmod{p*q}$, and

$m_3=c_1**m_{12} + c_2*m_{21} \pmod{p*q}$;

or

$m_1=c_1*m_{11} + c_2*m_{21} \pmod{p*q}$, and

$m_2=c_1*m_{11} + c_2*m_{22} \pmod{p*q}$.

Once again we use the fact that no matter what b is chosen, the output remains the the same in terms of solutions. For $b=0$ the two-solutions cryptograms are only caused by messages that are of the form cp or cq, except for the case when $c=0$, where c is some constant. Thus,

If $b=0$ and $m=cp$ or cq, then $z=m^2 \pmod{r}$,
and z has only two solutions for $c\neq 0$.

For $b=0$ the two-solutions messages are of the form cp or cq where $c\neq 0$, since the choice of b does not change the number of two-solutions messages, and their relative position with respect to the one-solution message is the same. Therefore, the one-solution cryptogram is the base point relative to which the other cryptograms shift. If m' is the one-solution message, then the two-solutions messages will be m'+cp, m'-cp, m'+cq, or m'-cq, where $c\neq 0$. The shift caused by the choice of b is equivalent to the shift of the one-solution message from zero. The shift of the two-solutions messages is (r-b)/2 (mod r) for b odd, and (r+1-b) + (r-1)/2 (mod r) for b even. Thus the two-solutions messages for any b will be of the following form:

For odd b:

(r-b)/2 + cp (mod r),

(r-b)/2 - cp (mod r),

(r-b)/2 + cq (mod r), and

(r-b)/2 - cq (mod r).

For even b:

(r+1-b) + (r-1)/2 + cp (mod r),

(r+1-b) + (r-1)/2 - cp (mod r),

(r+1-b) + (r-1)/2 + cq (mod r), and

(r+1-b) + (r-1)/2 - cq (mod r).

Therefore, knowing p or q is equivalent to knowing the values of the two-solutions messages and cryptograms. Conversely, knowing the values of the two-solutions messages is equivalent to knowing p or q.

Once one finds a two-solutions cryptogram, z, with two-solutions messages, m_1 and m_2, one knows that the difference between m_1 and m_2 is either cp or cq depending on whether the discriminant for x_1 or x_2 is zero. One can then define m_3 and m_4 to be functions of m_1 such that z_3 and z_4 will differ by cp or cq depending on the difference between m_1 and m_2. Once a two-solutions message or cryptogram is found, one can find both m's and z's that differ by cp or cq. If z is a two-solutions cryptogram with two-solutions messages m_1 and m_2 that differ by cp*, and m_1 is known, then one can define m_3 and m_4 such that z_3 and z_4 differ by dp*. If one lets

$m_3=m_1+1$ and $m_4=m_1-1$, then

$z_3=m_3(m_3+b)$ (mod r), and

$z_4 = m_4(m_4+b) \pmod r \rightarrow$

$z_4 - z_3 = dp^* \pmod r$,

where p^* is p or q.

5.4.2 HAPPENINGS AROUND TWO DECRYPTIONS

This section discusses what happpens around the two-solutions messages and cryptograms. If z is a two-solutions cryptogram with two-solutions messages, m and m', then let m_1 be m^*-1 and m_2 be m^*+1, where m^* is m or m'. The encryption of m_1 and m_2 gives z_1 and z_2 respectively. If the two-solutions messages, m and m', are the shifted versions of the two-solutions messages for cp^* when $b=0$, then $z_1 - z_2 = dp^*$, where p^* is p or q. Since different choices of b's do not matter, we can consider the case for $b=0$. One then has the following:

If z has two solutions m and m' and $m = cp^*$ $(c \neq 0)$,
then let $m_1 = m^*-1$ and $m_2 = m^*+1$ with

$z_1 = m_1^2 \pmod r$ and

$z_2 = m_2^2 \pmod r$ then

$z_1 - z_2 = dp^* \pmod r$.

The constraint that $c \neq 0$ is very important. If $c=0$ was also a message for a two-solutions cryptogram, then a two-solutions message, and $z_1 - z_2$ could always be found. Then by using the Euclidean algorithm, one could find p^* and break the system. Unfortunately, if $c=0$, then the message is a one-solution message.

The two-solutions messages lie at opposite ends of the (modulo r) field, because of the duplication property. Each of the two-solutions messages lie the same distance (distance is the difference between the messages) from the one-solution message. Therefore, the two-solutions messages will be kp^*+1 apart, where k is an even number.

As with duplication, other properties affect the locations of the two-solutions messages. In the four-decryption section, the four-solutions messages are shown to be interrelated by the duplication property or by the multiplication property. The latter property states that the distance between the four-solutions messages is cp^*. Two-solutions messages are related by the duplication property and by the multiplication property. Thus, once again the two-decryption case is just a degenerate case of the four-decryption case and the multiplication property arises because if the discriminant for x_1 is zero, then the difference between the two-solutions messages will be cp. On the other hand, if the discriminant for x_2 is zero, then the difference between the two-solutions messages will be cq. Thus

one has the following:

Define $z_1=m_1(m_1+b) \pmod r$ and $z_2=m_2(m_2+b) \pmod r$.

If $z_1=z_2$ and $\sqrt{(b^2-4x^*)}=0 \pmod r$ (meaning a two-solutions cryptogram, where x^* is either x_1 or x_2 but not both), then

$(m_1+m_2+b)=(cp)(q) \pmod r$, and

$(m_1-m_2)=cp^*$,

where p^* is p, if x^* is x_1, or p^* is q, if x^* is x_2.

From the value of b, the parity of constant, c, can be determined, i.e.: if b is even, then c is even, and if b is odd, then c is also odd. A zero discriminant in the quadratic formula for either x_1 or x_2, resulted in a two-solution cryptogram, and the difference between the two-solutions messages was either cp or cq. Thus one has the following:

Let $z_1=m_1(m_1+b) \pmod r$ and $z_2=m_2(m_2+b) \pmod r$.

If $z_1=z_2$ and $(m_1+m_2+b)=(cp)(q)$ (duplication property), and $\sqrt{(b^2-4x^*)}=0$, and b=even (odd), then

$(m_1-m_2)=cp^*$

where c is even (odd), and p^* is p, if x^* is x_1, and p^* is q, if x^* is x_2.

5.4.3 SLIM CHANCE OF ATTACK WITH TWO DECRYPTIONS

With a two-solutions message known, cp or cq may be determined. If m_1 is the two-solutions message, then let m_2 be m_1 plus one, and let m_3 be m_1 minus one. Then the difference between z_2 and z_3 is cp or cq, depending on whether the message is shifted from cp or cq when b equals zero. If the message is shifted from cp^* when b equals zero, then the difference between z_2 and z_3 is cp^*. Therefore, once cp^* is found, the prime can be found by using the Euclidean algorithm for GCD's on cp^* and r. Once p^* is known, the other prime is easily found, and the Rabin scheme is easily broken.

Very few of the cryptograms are two-solutions cryptograms. An attack on the Rabin scheme can be made, if either one of the two-solutions messages or either one of the two-solutions cryptograms can be found. If a two-solutions message, m, is found, it can be encrypted to find a two-solutions cryptogram. If $m_1=m-1$ and $m_2=m+1$, then $z_1-z_2=cp$ or cq. If both of the two-solutions messages are found, then their difference is cp or cq. There are $(p+q-2)/2$ possible number of two-

solutions cryptograms, and the probability of finding a two-solutions message or cryptogram can be quite large for p and q small. However, the limit of (p+q-2)/2*p*q is just 1/p or 1/q as p and q become large and it would be very difficult to find two-solutions messages or cryptograms for large p and q. Therefore, an attack which uses the above method is usually not possible, whether it uses the ciphertext only attack, plaintext-ciphertext pair attack or the chosen plaintext attack. It is shown later that a chosen ciphertext attack will work under the above method.

5.5 FOUR DECRYPTIONS

This section discusses the various properties of the four-solutions messages and cryptograms. This is the typical case and in practice all messages and cryptograms will be four-solutions messages and four-solutions cryptograms respectively. If the two discriminants are nonzero, then there will be four solutions to the quadratic formulas. These four solutions can be combined using the Chinese remainder theorem to retrieve four possible messages that are encrypted to the same cryptogram. From the previous discussion on two-decryptions and one-decryption, one can ascertain that all the rest of the messages and cryptograms that are not in the two-decryptions or one-decryption case are four-solutions messages and cryptograms.

The interrelation between the four-solutions messages for a particular four-solutions cryptogram is stated by the duplication and multiplication properties. The duplication property divides the four-solutions messages into two equal groups and the correspondence between the two groups is governed by the multiplication property. Suppose that the four-solutions messages to the four-solutions cryptogram, z are m_1, m_2, m_3, and m_4 and that the first group contains m_1 and m_3 and the second group contains m_2 and m_4. Then m_1 minus m_2, or m_1 minus m_4 is a multiple of p*, and m_3 minus m_2, or m_3 minus m_4 is also a multiple of p*, regardless of the b chosen. Thus one has the following:

Define $z_1=m_1(m_1+b) \pmod r$, and $z_2=m_2(m_2+b) \pmod r$ with

and $z_1=z_2$.

Then

$m_1-m_2=cp^*$ or

$(m_1+m_2+b)=(cp)(q)=0 \pmod r$.

Therefore, the above shows that if three of the four four-solutions messages were found, the scheme could be broken with probability 1. This is because two of the three solutions will exhibit the property that m_1 minus m_2 will be cp*. Now, the Euclidean algorithm for g.c.d. can be used to find p or q, and the other prime falls out trivially. If two of the four four-solutions messages were found, the scheme could be broken with probability of ½. This is one reason why the chosen ciphertext

attack works, and is similar to the two-decryptions case, in which the knowledge of a two-solutions message will break the scheme. In this case three of the four-solutions messages are needed in order to ensure a break the scheme.

For the two-decryptions or four-decryptions case in which two messages m_1 and m_2 differ by cp* there is a property concerned with messages that are exactly in the middle of the two messages m_1 and m_2. Messages that are exactly in the middle, m_1' and m_2', will only differ by one and have cryptograms z_1' and z_2' that differ by cp*. The difference between z_1' and z_2' is cp or cq depending on whether m_1-m_2 is cp or cq. Therefore,

define $z_1 = m_1(m_1+b) \pmod r$, and $z_2 = m_2(m_2+b) \pmod r$.

If $z_1 = z_2$ and $m_1 - m_2 = cp^*$, and c is odd then define:

$m_1' = \lfloor (m_2 - m_1 + 1)/2 \rfloor + m_1 - 1 \pmod r$ and

$m_2' = \lfloor (m_2 - m_1 + 1)/2 \rfloor + m_1 \pmod r \rightarrow$

$z_2' - z_1' = dp^* \pmod r$.

Four-solutions cryptograms around the two-solutions cryptograms exhibit a strange behavior. Let a two-solutions cryptogram, z, have two-solutions messages, m and m' and let m_1 be m*+k and m_2 be m*-k, where m* is either m or m'. If z_1 is the cryptogram for m_1, and z_2 is the cryptogram for m_2, then z_1 and z_2 differ by dp or dq depending on whether m* is a shifted version of m*=cp or m*=cq when b=0. Therefore,

Let $m_1 = m^* + k$ and $m_2 = m + k$

$m = cp^*$ and

$z_1 = m_1^2 \pmod r$ and

$z_2 = m_2^2 \pmod r \rightarrow$

$z_1 - z_2 = dp^* \pmod r$.

The four-solutions messages are duplicated across the imaginary line where the one-solution message is located, another instance of the duplication property. The boundaries of the two groups duplicated across the imaginary line can easily be found. One of the boundaries is at the one-solution message and the other boundary is half way around the message spectrum from the one-solution message, specifically:

$pt_1 = \lfloor (r+1-b)/2 \rfloor \pmod r$ and

$pt_2 = \lfloor (r+1-b)/2 \rfloor + \lfloor (r-1)/2 \rfloor \pmod r$.

The message spectrum are all of the possible messages.

Most of the cryptograms are four-solutions cryptograms. An attack on the Rabin scheme can be made if three of the four-solutions messages can be found, or, possible with only two of the four-solutions messages. If the four-solutions messages are m_1, m_2, m_3, and m_4, then there exist two pairs such that the difference between the messages within the pairs is cp or cq. Therefore, if one can separate the messages into pairs, such that $m_1 = m \pmod{p}$, $m_2 = -m \pmod{p}$, $m_3 = m \pmod{q}$, and $m_4 = -m \pmod{q}$, then $m_1 - m_2$ is cp and $m_3 - m_4$ is cq. Only one of these pairs of four-solutions messages needs to be found to break the Rabin scheme. Therefore, if the cryptanalyst has two four-solutions messages, he may have one of these pairs and if he has three four-solutions messages, one of these pairs is guaranteed. There are $(p*q-p-q+1)/4$ possible four-solutions cryptograms. It is not difficult to find four-solutions messages since most messages are of the four-decryption type. However, it is extremely difficult to find two or three of the four-solutions messages that encrypt to the same four-solutions cryptogram. Therefore, an attack which uses the above method is usually not possible, whether it uses the ciphertext only attack, plaintext-ciphertext pair attack or the chosen plaintext attack. It is shown later that a chosen ciphertext attack will work with the above method.

6 PROPERTIES OF B'S IN THE RABIN SCHEME

6.1 INTRODUCTION

This chapter discusses the effects of choosing different b's on the Rabin scheme. The parameter b has no effect on the cryptograms except for a shift of the relative positions of the cryptograms with respect to the messages. The number of four-solutions, two-solutions, and one-solution cryptograms remains the same for different b's as do the relative positions of the four-solutions, two-solutions, and one-solution cryptograms with respect to each other. Some of the subproperties are counterintuitive, while other subproperties are very intuitive. The four major subproperties are as follows: 1) for b=1, 2, 3, ... (r-1)/2 the scheme has the same cryptograms as for b=-1, -2, -3, ... (1-r)/2, respectively, except the values of the cryptograms are shifted with respect to the values of the messages; 2) as b varies the number of four-solutions, two-solutions, and one-solution cryptograms remain the same. For any b not equal to 0 (mod p) or 0 (mod q) the number of cryptograms of the form z=0 (mod p) or 0 (mod q) remain the same. Also, the pattern which relates cryptograms to their respective numbers of solutions shifts with respect to the values of the messages; and 3) for b=-k (mod p) or -j (mod q) or k (mod p) or j (mod q) there is a method to find a cryptogram that equals 0 (mod p) or 0 (mod q). Therefore, the choice of b has no effect, and that the breaking of the Rabin scheme for one b breaks the Rabin scheme for all b's.

6.2 FOR B = 1, 2, 3, ... (MODULUS-1)/2 THE SCHEME HAS THE SAME CRYPTOGRAMS AS FOR B = -1, -2, -3, ... (1-MODULUS)/2, RESPECTIVELY, EXCEPT THE VALUES OF THE CRYPTOGRAMS ARE SHIFTED WITH RESPECT TO THE VALUES OF THE MESSAGES

This section shows that for b=1, 2, 3, ... (r-1)/2, the scheme has the same cryptograms as for b=-1, -2, -3, ... (1-r)/2, respectively, however the values of the cryptograms are shifted with respect to the values of the messages. This means that only half the b's give rise to different cryptograms.

THEOREM: $m(m+b)=m'(m'-b) \pmod r$

if $m'=m+b$, or $(m+m')=cp$ or cq

PROOF OF THEOREM:

Let $z=m(m+b) \pmod r$ and $z'=m'(m'+b) \pmod r$ then

$z-z'=m^2-m'^2+(m+m')b=0 \pmod r$

$=(m+m')(m-m')+(m+m')b=0 \pmod r$

$=(m+m')(m-m'+b)=0=cp*cq \pmod r$,

so, either

$m'=-m$, or

$m'=m+b$.

Therefore, either $(m+m')=cp$ or cq, or

$(m-m'+b)=0 \pmod r \rightarrow m'=m+b \pmod r$.

The second case implies that for b and -b, the same cryptograms result. ***QED.***

6.3 AS B VARIES THE NUMBER OF FOUR-SOLUTIONS, TWO-SOLUTIONS, ONE-SOLUTIONREMAIN THE SAME. FOR ANY B NOT EQUAL TO 0 (MOD P) OR 0 (MOD Q) THE NUMBER OF CRYPTOGRAMS OF THE FORM 0 (MOD P) OR 0 (MOD Q) REMAINS THE SAME. IN ADDITION THE PATTERN WHICH RELATES CRYPTOGRAMS TO THEIR RESPECTIVE NUMBER OF SOLUTIONS SHIFTS WITH RESPECT TO THE VALUES OF THE MESSAGES

This section shows that no matter which b is chosen, the number of four-solutions, two-solutions, and one-solution cryptograms remain the same. For any b not equal to cp or cq, the number of cryptograms that are cp or cq also remains the same. Also, the pattern which relates cryptograms to their respective numbers of solutions shifts with respect to the values of the messages . The shift is only a function of the b's; thus, the shift from one set of cryptograms to the other is determined by the two b's. If one of the b's chosen is $b=0$, the effect of a particular b is just a shift. Since there is only a single one-solution message for each message spectrum, one can analyze how the message shifts when b changes. Therefore, the shift for that particular b can be determined because the four-solutions, two-solutions and one-solution messages remain in the same positions relative to the one-solution message for any b, as previously discussed.

$$\frac{(b_2^2-b_1^2)}{4} \pmod r$$

for $b_2>b_1$, and

$$\frac{(b_1^2-b_2^2)}{4} \pmod r$$

for $b_1>b_2$.

PROOF:

Without loss of generality assume that b2>b1 and that the cryptogram used in the analysis is the one-solution message. For the two one-solution messages one has the following:

$m_1=-b_1/2 \pmod r$

and

$m_2=-b_2/2 \pmod r$.

Then,

$z_1=(-b_1/2)^2 + b_1(-b_1/2) \pmod r$

$z_2=(-b_2/2)^2 + b_2(-b_2/2) \pmod r$.

So,

$z_1-z_2=(-b_1/2)^2 - (-b_2/2)^2 + b_1(-b_1/2) - b_2(-b_2/2) \pmod r$

$=(-b_1/2 + -b_2/2)(-b_1/2 - -b_2/2) + b_1(-b_1/2) - b_2(-b_2/2) \pmod r$

$=-(b_1+b_2)/2 * (b_1-b_2)/2 + -(b_1/2)^2 + (b_2/2)^2 \pmod r$

$=(b_1+b_2)/2 * (b_1-b_2)/2 + (b_2^2 - b_1^2)/2 \pmod r$

$=(b_1^2-b_2^2)/4 + (b_2^2 - b_1^2)/2 \pmod r$

$=\frac{(b_2^2 - b_1^2)}{4} \pmod r$

When for b=0 the one-solution is zero, and the value of the one-solution cryptogram for $b\neq 0$ is always $-(b^2)/4 \pmod r$. Thus, the shift must be $(b_2^2 - b_1^2)/4 \pmod r$. ***QED.***

This proof demonstates that the choice of the parameter b has little effect on the strength of the Rabin scheme, and so will not protect the scheme from the clustering effect. Nor will the scheme be protected from a cryptanalyst attempting to find a two-solutions message or three of the four-solutions messages. Since a shift of $(b_{22} - b_{12})/4$ is involved in changing the b's, breaking the scheme for a particular b, such as b=0, breaks the scheme for all b. Therefore, the parameter b does not enhance the security of the scheme, in fact, by choosing the wrong b or too many b's one may

make the system less secure.

6.4 FOR B = RESIDUE (MOD P) OR RESIDUE (MOD Q) THERE IS A METHOD TO FIND A CRYPTOGRAM THAT EQUALS 0 (MOD P) OR 0 (MOD Q)

If the cryptanalyst can approximate the difference between b and cp or cq, he can find cp or cq. Thus, the choice of a particular b is very important. Let m_1 and m_2 be the two messages that cause two equivalent cryptograms, z_1 and z_2, and let m_1 and m_2 be at the other end of the message spectrum from the one-solution message. These cryptograms are equivalent because of the duplication property. If b is cp-1, cq-1, cp+1, or cq+1 (with c not equal to zero), then z_1 and z_2, are of the form dp or dq.

THEOREM: If $b=cp^*-1$ or cp^*+1, and $c\neq 0$, where cp^* is cp or cq, then:

CASE 1: b is odd with $m_1=(r-b)/2 + (r-1)/2 + 1 \pmod r$ and $m_2=(r-b)/2 + (r-1)/2 \pmod r \rightarrow z_1=z_2=dp^*$.

CASE 2: b is even with $m_1=(r-1-b)/2 \pmod r$ and $m_2=(r+1-b)/2 \pmod r \rightarrow z_1=z_2=dp^*$.

PROOF: CASE 1:

1) For $b=cp^*-1$, and $c\neq 0$, and b even, then for z_1:

$$z_1=m_1^2 + m_1*b$$

$$=\frac{(r-1-b)^2}{2} + \frac{b(r-1-b)}{2} \pmod r,$$

$$\text{but } \frac{(r-1-b)}{2} = \frac{(r-1-(cp^*-1))}{2} = \frac{(r-cp^*)}{2} \pmod r$$

$$\rightarrow z_1=\frac{(r-cp^*)^2}{2} + cp^*\frac{(r-cp^*)}{2} - \frac{(r-cp^*)}{2} \pmod r$$

$$=(cp^*)^2\frac{(dp'^*-1)^2}{2} + (cp^*)^2\frac{(dp'^*-1)}{2} - cp^*\frac{(dp'^*-1)}{2} \pmod r,$$

where if $dp^* = dp$, then $dp'^* = dq$, and if $dp^* = dq$, then $dp'^* = dp$,

$$=(cp^*)^2(cp^*\frac{(dp'^*-1)^2}{4} + cp^*\frac{(dp'^*-1)}{2} - \frac{(dp'^*-1)}{2}) \pmod r$$

$= dp^* \pmod r$

QED.

2) For z_2:

$z_2 = m_2^2 + m_2 * b \pmod r$

$z_2 = \frac{(r+1-b)^2}{2} + \frac{b(r+1-b)}{2} \pmod r,$

but $\frac{(r+1-b)}{2} = \frac{(r+1-(cp^*-1))}{2} = \frac{(r-cp^*+2)}{2} \pmod r$

$\rightarrow z_2 = \frac{(r-cp^*+2)^2}{2} + cp^*\frac{(r-cp^*+2)}{2} - \frac{(r-cp^*+2)}{2} \pmod r$

$= \frac{(-cp^*+2)^2}{2} + cp^*\frac{(-cp^*+2)}{2} - \frac{(-cp^*+2)}{2} \pmod r$

$= \frac{((cp^*)^2-4*cp^*+4)}{4} + \frac{(-(cp^*)^2 + 4*cp^*)}{4} + \frac{(2*cp^*-4)}{4} \pmod r$

$= \frac{((cp^*)^2-4*cp^*+4-2(cp^*)^2+4*cp^*+2*cp^*-4)}{4} \pmod r$

$= \frac{(-(cp^*)^2+2*cp^*)}{4} \pmod r$

$= dp^* \pmod r$

QED.

3) For $b = cp^*+1$, and $c \neq 0$, and b even, then for z_1:

$z_1 = m_1^2 + m_1 * b \pmod r$

$z_1 = \frac{(r-1-b)^2}{2} + \frac{b(r-1-b)}{2} \pmod r,$

but $\frac{(r-1-b)}{2} = \frac{(r-1-(cp^*+1))}{2} = \frac{(r-cp^*-2)}{2} \pmod r$

$\rightarrow z_1 = \frac{(r-cp^*-2)^2}{2} + cp^*\frac{(r-cp^*-2)}{2} - \frac{(r-cp^*-2)}{2} \pmod r$

$$=\frac{(-cp^*-2)^2}{2} + cp^*\frac{(-cp^*-2)}{2} - \frac{(-cp^*-2)}{2} \pmod r$$

$$=\frac{((cp^*)^2+4*cp^*+4)}{4} + \frac{(-(cp^*)^2 - 4*cp^*)}{4} - \frac{(2*cp^*-4)}{4} \pmod r$$

$$=\frac{((cp^*)^2+4*cp^*+4-2(cp^*)^2-4*cp^*-2*cp^*-4)}{4} \pmod r$$

$$=\frac{(-(cp^*)^2-2*cp^*)}{4} \pmod r$$

$$=dp^* \pmod r$$

QED.

4) For z_2:

$$z_2=m_2^2 + m_2*b \pmod r$$

$$=\frac{(r+1-b)^2}{2} + \frac{b(r+1-b)}{2} \pmod r,$$

but $\frac{(r+1-b)}{2} = \frac{(r+1-(cp^*+1))}{2} = \frac{(r-cp^*)}{2} \pmod r$

$$\rightarrow z_2=\frac{(r-cp^*)^2}{2} + cp^*\frac{(r-cp^*)}{2} + \frac{(r-cp^*)}{2} \pmod r$$

$$=(cp^*)^2\frac{(dp'^*-1)^2}{2} + (cp^*)^2\frac{(dp'^*-1)}{2} + cp^*\frac{(dp'^*-1)}{2} \pmod r,$$

where if $dp^* = dp$, then $dp'^* = dq$, and if $dp^* = dq$, then $dp'^* = dp$,

$$=(cp^*)^2\left(cp^*\frac{(dp'^*-1)^2}{4} + cp^*\frac{(dp'^*-1)}{2} + \frac{(dp'^*-1)}{2}\right) \pmod r$$

$$=dp^* \pmod r$$

QED.

CASE 2: For b odd, then: $m_1=(r-b+r-1)/2 + 1=(-1-b)/2 + 1=(1-b)/2 \pmod r$, and $m_2=(r-b+r-1)/2=(-1-b)/2=(-b-1)/2 \pmod r$.

1) For $b=cp^*-1$, and $c\neq 0$, and b odd, then for z_1,

$$z_1 = \frac{(1-b)^2}{2} + \frac{b(1-b)}{2} \pmod{r}$$

$$= \frac{(1-2*b+b^2)}{2} + \frac{(b-b^2)}{2} \pmod{r}$$

$$= \frac{(1-2*b+b^2+2*b-2*b^2)}{4} \pmod{r}$$

$$= \frac{(1-b^2)}{4} \pmod{r} \qquad (1)$$

$$= \frac{(1-(cp^*-1)^2)}{4} \pmod{r}$$

$$= \frac{(1-((cp^*)^2-2*cp^*+1)}{4} \pmod{r}$$

$$= \frac{(1-(cp^*)^2+2*cp^*-1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2+2*cp^*)}{4} \pmod{r}$$

$$= dp^* \pmod{r}$$

QED.

2) For b odd, and $b = cp^*-1$, and $c \neq 0$, then for z_2:

$$z_2 = \frac{(-1-b)^2}{2} + \frac{b(-1-b)}{2} \pmod{r}$$

$$= \frac{(b^2+2*b+1)}{4} + \frac{(-b-b^2)}{2} \pmod{r}$$

$$= \frac{(b^2+2*b+1-2*b-2*b^2)}{4} \pmod{r}$$

$$= \frac{(-b^2+1)}{4} \pmod{r} \qquad (2)$$

$$= \frac{(-(cp^*-1)^2+1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2 + 2*cp^* - 1 + 1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2 + 2*cp^*)}{4} \pmod{r}$$

$$= dp^* \pmod{r}$$

QED.

3) For $b = cp^* + 1$, and $c \neq 0$ and b odd, from equation (1):

$$z_1 = \frac{(1 - b^2)}{4} \pmod{r} \qquad (1)$$

$$= \frac{(1 - (cp^* + 1)^2)}{4} \pmod{r}$$

$$= \frac{(1 - ((cp^*)^2 + 2*cp^* + 1))}{4} \pmod{r}$$

$$= \frac{(1 - (cp^*)^2 - 2*cp^* - 1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2 - 2*cp^*)}{4} \pmod{r}$$

$$= dp^* \pmod{r}$$

QED.

4) For $b = cp^* + 1$, and $c \neq 0$, and b odd, from equation (2):

$$z_2 = \frac{(-b^2 + 1)}{4} \pmod{r} \qquad (2)$$

$$= \frac{(-(cp^* + 1)^2 + 1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2 - 2*cp^* - 1 + 1)}{4} \pmod{r}$$

$$= \frac{(-(cp^*)^2 - 2*cp^*)}{4} \pmod{r}$$

$= dp^*$ (mod r)

QED.

This theorem can be extended to include b's of the form cp-k, cp-j, cp+k, or cq+j. Let messages m_1 and m_2 be the two messages that cause two equivalent cryptograms, z_1 and z_2, and let m_1 and m_2 be at the other end of the message spectrum from the one-solution message $\pm 4*2^{(k^*-2)}$, where k* is k or j. Again the cryptograms are equivalent because of the duplication property. If b is cp-k, cq-j, cp+k, or cq-j (with c not equal to zero), then z_1 and z_2 are of the form dp or dq.

THEOREM: If $b = cp^* - k^*$ or $cp^* + k^*$ and $c \neq 0$ where cp* is cp or cq and k* is k or j, then

CASE 1: b is odd with $m_1 = (r-b)/2 + (r-1)/2 + 1 + 4*2^{(k^*-2)}$ (mod r) and $m_2 = (r-b)/2 + (r-1)/2 - 4*2^{(k^*-2)}$ (mod r) $\rightarrow z_1 = z_2 = dp^*$.

CASE 2: b is even with $m_1 = (r-1-b)/2 + 4*2^{(k^*-2)}$ (mod r) and $m_2 = (r+1-b)/2 - 4*2^{(k^*-2)}$ (mod r) $\rightarrow z_1 = z_2 = dp^*$.

PROOF: The proof proceeds identically for k=j=1. ***QED.***

7 ADDITIONAL DISCOVERED PROPERTIES OF THE RABIN SCHEME

7.1 INTRODUCTION

In the Rabin scheme, seven additional properties are of particular interest. These are: 1) cryptograms and messages of the form 0 (mod p) or 0 (mod q); 2) the encryption function which maps r possible messages into only about r/4 possible cryptograms; 3) $m=z$; 4) $m=-b$; 5) $z_1-z_2=0$ (mod p) or 0 (mod q); 6) repeated encryption; and 7) the relative speeds of the Rabin and the Rivest-Shamir-Adleman schemes.

As always, the properties of the Rabin scheme are essential to cryptanalysis, since in order to find the weaknesses of a scheme one must first find its properties. The properties lead to some very interesting cryptanalysis attacks on the Rabin scheme. Some of the properties are counterintuitive, while others are intuitive.

7.2 CRYPTOGRAMS AND MESSAGES OF THE FORM 0 (MOD P) OR 0 (MOD) Q

7.2.1 MESSAGE IS OF THE FORM 0 (MOD P) OR 0 (MOD) Q

Whether the message, m is a multiple of p or q, has a pronounced effect on the cryptogram. If the message is of the form cp or cq, then the cryptogram z is also of the form cp or cq. Therefore,

$m=cp \rightarrow z=dp$, or

$m=cq \rightarrow z=dq$.

There are $(p+q-1)$ of the form cp or cq.

7.2.2 CRYPTOGRAM IS OF THE FORM 0 (MOD P) OR 0 (MOD) Q

The effects of a cryptogram which is a multiple of cp or cq are more profound than those of the message. If the cryptogram is a multiple of cp or cq, then there is an algorithm to break the Rabin scheme. If the message is of the form cp or cq, then the cryptogram is of the form cp or cq, but not vice-versa. If the cryptogram is of the form cp or cq, the message must be of the form cp, cq, cp-b, or cq-b. Therefore,

$m+b=cp \rightarrow z=dp$, or

$m+b=cq \rightarrow z=dq.$

If another cryptogram z_1 can be found such that z_1 is of the form cp or cq, and m_1 is not of the form cp or cq, then the following property becomes apparant If m_1 is added to b to form a new message m_2, then m_2 is of the form cp or cq, and it follows that z_2 is of the form dp or dq. If m_2 is of the form cp, then z_2 is also of the form dp, but if m_2 is of the form cq, then z_2 is of the form dq. This method can be used to find additional messages and cryptograms of the form cp or cq once the first is found. When two numbers of the form cp or cq are found, then the Euclidean algorithm for g.c.d can be used, to find p and q. The probability of this attack succeeding is low, since the user will not ordinarily use a message of the form cp or cq, and the probability for a cryptogram of the form cp or cq is also low. Therefore,

$m_1 \neq cp^*$, and $(b,r)=1$, and

$z_1=m_1^2+m_1*b=cp^* \rightarrow$

$m_2=m_1+b=dp^*$, and

$z_2=m_2^2+m_2*b=ep^*$,

where p^* is either p or q.

The number of cryptograms of the form cp or cq depends on b:

for $b \neq cp^*$, one has $2(p+q-2)$ cryptograms,

for $b=cp^*$, one has $2(p^*-1) + p'^*$ cryptograms, and

for $b=0$, one has $(p+q-1)$ cryptograms.

7.2.3 SLIM CHANCE OF ATTACK WITH CRYPTOGRAMS OF THE FORM 0 (MOD P) OR 0 (MOD) Q OR MESSAGES OF THE FORM 0 (MOD P) OR 0 (MOD) Q

If z or m is found such that z=cp or cq or m=cp or cq, then p or q can easily be found. If m is cp^*, then z is also cp^*, and the Euclidean algorithm for g.c.d.'s on m and zyields p^*. If z is cp or cq simply encrypt z to get z' which is also cp^*. Therefore, one can find p^* by using the Euclidean algorithm for g.c.d.'s on z and z'.

Very few cryptograms or messages are of the form cp or cq. An attack on the Rabin scheme is possible, if a message or cryptogram is of the form cp or cq, where there are $(p+q-1)$ of these. The number of cryptograms of the form cp or cq depends on b. For $b=0$ one has $(p+q-1)$

cryptograms of the form cp or cq; for b=cp* one has 2(p*-1)+p'* cryptograms of the form cp or cq; and for b≠cp* one has 2(p+q-2) cryptograms of the form cp or cq. Where p'* is p is p* is q and p'* is q if p* is p. Therefore, for small p and q, the probability for finding messages and/or cryptograms of the form cp or cq is quite large. However, as p and q become large, the limit of

(p+q-1)/(p)(q) for messages, or

2(p+q-2)/(p)(q) for b≠cp*, or

2(p*-1)+p'*/(p)(q) for b=cp*, or

(p+q-1)/(p)(q) for b=0,

is just 1/p or 1/q. Therefore, it would be very difficult to find messages or cryptograms that are of the form cp or cq for large p and q.

7.3 THE ENCRYPTION FUNCTION MAPS ALL POSSIBLE MESSAGES INTO APPROXIMATELY ONE FOURTH OF THE RANGE

The fact that the number of possible cryptograms is only about one fourth of r is due mainly to the four-solutions, two-solutions and one-solution cryptograms. The exact number of possible cryptograms is (p+q+1+p*q)/4, which is approximately r/4, since r/4 is p*q/4. This fact means that only about one fourth of the possible cryptograms can be used, which causes bandwidth expansion. By using either r=p or q, then the brandwidth expansion would only be r/2 because of the quadratic residue properties. The bandwidth expansion is 3/4*r for r=p*q. If r is large enough, then bandwidth expansion can be minimized. By counting, one can easily find the actual number of possible cryptograms. Since any cryptogram spectrum is just a shift of the b=0 cryptogram spectrum, one can count the possible number of cryptograms for b=0, which is p*q, for p*q possible messages. from the p*q possible messages, there are (p+q-1) possible cp or cq messages, since they overlap for c=0. There are (p+q-2) possible messages which cause two-solutions cryptograms and there is one possible message that causes the one-solution cryptogram. Therefore, the rest of the messages must cause four-solutions cryptograms totalling ((p*q) - (p+q-2) - 1)=(p*q - p - q + 1) four-solutions messages. Thus, the number of possible z's is one times the number of one-solution messages, plus two times the number of two-solutions messages, plus four times the number of four-solutions messages. This results in (p + q + 1 + p*q)/4 possible cryptograms.

THEOREM: The number of different possible z's are:

$$\frac{(p*q + p + q + 1)}{4} \pmod{r}$$

PROOF:

Let

m_1-number of one-solution messages,

m_2-number of two-solutions messages, and

m_4-number of four-solutions messages.

$m_1=1$, $m_2=(p + q - 2)$, and $m_4=(p*q - (p + q - 2) -1)=(p*q - p - q + 1)$.

Thus,

the number of cryptograms caused by m_1 is: $1 \pmod{r}$,

the number of cryptograms caused by m_2 is: $\frac{(p + q - 2)}{2} \pmod{r}$, and

the number of cryptograms caused by m_4 is: $\frac{(p*q - p - q + 1)}{4} \pmod{r}$.

Therefore, the total number of cryptograms is:

$$\frac{(p*q - p - q + 1)}{4} + \frac{(p + q - 2)}{2} + 1 \pmod{r},$$

which is,

$$=\frac{(p*q - p - q + 1 + 2*p + 2*q - 4 + 4)}{4} \pmod{r}$$

$$=\frac{(p*q + p + q + 1)}{4} \pmod{r}$$

QED.

7.4 MESSAGE EQUALS THE CRYPTOGRAM

The chance of the message being equal to the cryptogram is slight; but if it occurs, the message is either of the form cp or cq, or the message is zero (which is the same as $c=0$ for the previous case), or the message is 1-b. Thus, if a message is found to equal the cryptogram, then by using the Euclidean algorithm, one can find cp or cq.

If $m=z$, then

$m=m^2+m*b \pmod r$

$0=m^2+m(b-1) \pmod r$

$0=m(m+b-1) \pmod r$,

so, either

$m=0 \pmod r$, or $m=1-b \pmod r$, or $m=cp$ or $cq \pmod r$.

7.5 MESSAGE EQUALS -B

If the message is -b and one of the p's is known, then there is a chance of finding cp or cq. Given message, m_2, is -b, and message, m_1, is $m_2-(p^*-b)$, where p^* is p or q, then the cryptograms z_1 and z_2 differ by cp or cq. From this point the subtraction of one from m_2 to produce m_3, and the addition of one to m_1 to produce m_4, will lead to cryptograms z_4 and z_3 such that their difference is cp or cq. Also, the addition of one to m_2 to produce m_3, and the subtraction of one from m_1 to produce m_4, will lead to cryptograms, z_3 and z_4, such that their difference is cp or cq.

Let $p^*=p$ or q and $m_2=-b$.

Then

$0=m_2^2 + m_2*b \pmod r \rightarrow$

$0=m_1=m_2-(p^*-b) \pmod r \rightarrow$

$z_1-z_2=cp^* \pmod r$.

7.6 TWO CRYPTOGRAMS OF THE FORM 0 (MOD P) OR 0 (MOD) Q

Let messages, m_1, m_2, m_3, and m_4 encrypt to cryptograms, z_1, z_2, z_3, and z_4 respectively. If the difference between z_1 and z_2 is cp or cq, then for m_3 equal m_1 plus some constant k, and for m_4

equal m_2 minus some constant k, then the difference between z_3 and z_4 is cp or cq. Therefore, once a set of cryptograms, differing by cp or cq is determined, many more can be found.

Let $z_1=m_1(m_1+b) \pmod r$ and $z_2=m_2(m_2+b) \pmod r$ and $p^*=p$ or q.

Then $z_1-z_2=cp^* \rightarrow$

either $(m_1-m_2)=cp^*$ or $(m_1+m_2+b)=cp^*$.

Letting $m_3=m_1+k$ and $m_4=m_2-k$ and

$z_3=(m_1+k)^2 + b(m_1+k) \pmod r$

$z_4=(m_2-k)^2 + b(m_2-k) \pmod r$,

then $z_3-z_4=cp^* \pmod r$.

7.7 REPEATED ENCRYPTION

This section deals with the properties of repeated encryption. If an encrypted message is followed by the repeated encryption of its cryptogram, there is a possibility of finding cp or cq. This property is related to the number of solutions property. If a message is repeatedly encrypted, eventually the repeated encryption will produce a cryptogram identical to the original cryptogram z. The cryptogram encrypted to the original cryptogram will be called z'. Once the first cryptogram is formed by encrypting z', several interesting properties concerning the message, m, the cryptograms, z and z'. One of the following relationships will occur, for the case of b=0: 1) z' minus m is cp or cq, 2) z' equals m, 3) z' minus z is cp or cq, or 4) z' plus m is r. If z' minus m is cp or cq, or z' minus z is cp or cq, then the Rabin scheme can be broken. If z' is equal to m, then the message is found. The only case where no information is found is when z' plus m is equal to r. Case 3) only occurs together with case 4). The other cases are mutually exclusive. Therefore, to perform a known plaintext attack, simply for a known cryptogram in the plaintext, obtain the resulting cryptogram, and repeat the procedure. For the successive finds a search continues until the last cryptogram obtained equals the original cryptogram, then one of the four cases will occur. One would eventually find cp or cq. On the other hand, to perform a chosen plaintext attack, used repeated encryption to find cp or cq providing case 4) occured infrequently.

This property is similar to the number of solutions property because if z' minus m is cp or cq, then z' is one of the other four-solutions message caused by the multiplication propertys, such that m_1 minus m_2 is cp or cq. If z' plus m equal r, then z' is one of the other four-solutions messages caused by the duplication property, such that $m_2=-m_1$. If z'=m then z' is one of the four-solution messages which is the original message. Encrypting m or z' results in the same cryptogram. If m is cp or cq, and if another message m_2 is found to cause the same cryptogram, then m_1 minus m_2 is cp or cq.

Thus, the repeated encryption property may be used as a potential attack against the Rabin scheme.

7.8 THE SPEED OF THE RABIN SCHEME RELATIVE TO THE SPEED OF THE RSA SCHEME

This section discusses the relative speed of the Rabin and the RSA schemes. As far as encryption is concerned, the Rabin scheme is faster, since it only involves taking the message to the power of two while the RSA scheme takes the message, M to some power. Therefore the Rabin scheme takes on the order of $O(1)$ time while the RSA scheme takes on the order of $O(\log_2 r)$ time to encrypt. On the other hand, the RSA and the Rabin scheme take about the same time in the decryption. Since the RSA scheme takes the cryptogram, C, to some power (mod r) and requires on the order of $O(\log_2 r)$ time. The Rabin scheme has two forms of decryption depending on the form of the primes. If the form is $p=q=4k-1$, then the decryption involves taking the cryptogram, C, to the $(p+1)/4$ power. Using the fact that:

$$L=(\sqrt{C})=C^{(p+1)/4} \rightarrow$$

$$L^2=C^{(p+1)/2}=C*C^{(p-1)/2}=C \pmod{p},$$

the Rabin scheme decryption takes on the order of $O(\log_2 r)$ time. If the primes are of the form $p=q=4k+1$, then Rabin uses a probabilistic algorithm, which is a special case of the Berlekamp's root-finding algorithm in GF(p). The algorithm finds the square root by taking the g.c.d. and also requires on the order of $O(\log_2 r)$ time to accomplish the square root. The algorithm finds the roots of $m(m+b)=z$ or $m^2+m*b+z=(m-\alpha)(m-\beta)$, where the roots of the equation $x^{(p-1)/2}-1=0 \pmod{p}$ are the quadratic residues $\gamma \in GF(p)$. If α is a quadratic residue and β is not, then

$$(m^{(p-1)/2}-1, m^2+m*b+z)=(m-\alpha),$$

so that $\beta=-(b+\alpha)$ and $\alpha \pmod{p}$.

If α and β are both quadratic residues or quadratic non-residues (mod p) with $\alpha \neq \beta$, then a different approach is needed. Let δ be such that $0 \leq \delta < p$. If $(\alpha+\delta)/(\beta+\delta)$ is a quadratic residue (mod p), then $\alpha+\delta$ and $\beta+\delta$ are still both quadratic residues or quadratic non-residues. As we choose different δ in the range $0 \leq \delta < p$, except for $\delta=-\beta$, the quotient $(\alpha+\delta)/(\beta+\delta)=\gamma$ takes on all the values in the range $0 \leq \gamma < p$ except $\gamma=1$. Therefore, for (p-1)/2 different choices of δ, the parameters $\alpha+\delta$ and $\beta+\delta$ will not both be quadratic residues or quadratic non-residues. Since we have that

$$(m-\delta)^2+(m-\delta)*b+z=(m-\alpha-\delta)(m-\beta-\delta),$$

if γ is chosen at random, then with a probability of ½ we have:

$(m^{(p-1)/2}-1,(m-\delta)^2+(m-\delta)*b+z)=m-\alpha-\delta$ or $m-\beta-\delta$.

On an average, only two values of δ need to be tried before one finds the roots. The user can easily find α or β, the real roots since he knows δ. In conclusion the computation of the g.c.d. requires on the order of $O(\log_2 r)$ operations, so the decryption of the Rabin scheme and the RSA scheme both take $O(\log_2 r)$ time.

8 AMBIGUITY PROBLEM OF THE RABIN SCHEME

8.1 INTRODUCTION

This chapter discusses the ambiguity problem of the Rabin scheme. The ambiguity problem is to decide which of the four-solution messages found in decryption is the original message. There are several possible approaches to solve the problem by: 1) the simple parity check; 2) the choice of largest solution; 3) the choice of a set of possible messages; 4) coding; and 5) the use of the Williams scheme.

Of the five possibilities only the last two seem to be the most reliable. The Rabin scheme will only be effective if a correct choice between the four-solutions messages was made.. Since the encryptions and decryptions would probably be done by computers, a method for determining which of the four-solutions message is the original message should be deterministic withour human aid. It is important to note that when the cryptograms are sent in blocks they are often context-dependent and it is difficult to determine which of the four-solutions message is the original message even with human aid.

8.2 THE SIMPLE PARITY CHECK

Parity checks can be used to resolve the ambiguity problem. A parity check consists of tacking a set of parity bits in front of the message, which are either all zero's, all one's, or some fixed set of bits. This alerts the receiver to which of the four-solutions messages or two-solutions messages is the correct message. This method does not always, work since messages that differ by only p or q may have caused the same cryptogram and such messages are so close together that the parity bits cannot determine which of the solutions is the message. In other words, the parity added to the messages should have the following property: when the parity is added, the receiver should be able to distinguish which solution is the message, even though the solutions may only be one prime apart. Ordinarily the solutions will differ greatly, but in some cases a large number of parity bits must be added to distinguish the message from all of the solutions to insure proper decryption. Adding a large number of bits increases bandwidth and makes this method undesirable. Alternatively a parity check, may be used when proper decryption is not necessary at all times. The reasoning is that different solutions will usually differ by a large amount.

8.3 THE CHOICE OF LARGEST SOLUTION

Using the largest solution as the message to resolve the ambiguity problem is possible. Unfortunately, this method will not work, however, because the largest solution is not always the correct solution. The four-solutions do not fall into groups with the solutions always occurring in the following fashion: the first solution always between 0 and r/4; the second solution between r/4+1 and r/2; the third solution between r/2+1 and 3r/4; and the fourth solution between 3r/4 and r-1. Therefore, the largest solution method does not solve the ambiguity problem since the solutions can differ by an amount as small as p or q.

8.4 THE CHOICE OF A SET OF POSSIBLE MESSAGES

Publishing a set of possible messages consisting of at most (p*q+p+q-1)/4 elements, is another possibility. This is because r distinct messages would only encrypt to (p*q+p+q-1)/4 distinct cryptograms. The method is to select one message from each of the two-solutions messages and four-solutions messages and then publishes the set, so that anyone sending messages to him must choose from the allowable messages. Again, this method does not work, because the cryptanalyst could isolate which messages were used and which avoided, and find cp or cq. In addition, the cryptanalyst could use one of the two-solutions messages and break the Rabin scheme. Even the deletion of the two-solutions message from the set would not prevent the cryptanalyst from determining cp or cq. The Williams scheme is essentially a method to publish a set of possible messages without allowing the cryptanalyst any additional information.

8.5 CODING

This section discusses the possibility of using codes to solve the ambiguity problem of the Rabin scheme. If a set of code bits are appended onto the end of each block of cryptograms, it is possible to indicate which of the four-solutions messages in the decryption is the original message, although this may require added effort, it may be the only way to alert the receiver to the correct solution. For example, tack two bits onto the end of the cryptogram stating which of the four-solution messages is the original four-solutions messages.

8.6 THE USE OF THE WILLIAMS SCHEME

This section discusses the possibility of using the Williams scheme instead of the Rabin scheme. The Williams scheme discussed in detail in this dissertation, solves the ambiguity problem

by restricting the possible sets of messages to approximately 3/16 to 1/4 of all possible messages. Therefore, the ambiguity problem no longer exists for the Williams scheme. This is similar to publishing a set of possible messages as discussed in section 7.4.

9 GENERAL ATTACKS ON THE RABIN SCHEME

9.1 INTRODUCTION

General attacks on the Rabin scheme are introduced in this chapter including how: 1) a repeated encryption attack can always be launched; 2) the Pollard algorithm can be used for a repeated encryption attack; 3) the equivalence of decryption to factoring enables a chosen ciphertext attack; 4) the equivalence of decryption to factoring does not contribute to other attacks; 5) the equivalence of decryption to factoring contributes to possible signature attacks; and 6) Rabin added patches to protect his scheme from signature attacks. These potential attacks are all byproducts from an investigation of Rabin scheme properties.

9.2 A REPEATED ENCRYPTION ATTACK CAN ALWAYS BE LAUNCHED

If the cryptanalyst repeatedly encrypts messages, he will eventually enter a loop. Once in the loop, he can take the differences between the cryptograms in the loop. One of the differences will always be cp or cq. We can define the original message to be m, the original cryptogram to be z, and the last cryptogram which encrypts to the original cryptogram to be z'. After repeated encryption the loop entered has one of the following properties: 1) z' minus m is cp or cq; 2) z' equals the m; 3) z' minus z is cp or cq; or 4) z' plus m is r. If one repeatedly encrypts by using the message first and using the resulting cryptograms thereafter, one will eventually find p or q, which will enable one to break the Rabin scheme; or find m, the desired message; or to find r, which provides no useful information. Depending on the choice of m and the value of p and q a the loop may be very short, which enables quick determination of p or q. If the wrong m is chosen, it may lead to case 4) for which a different m must be tried. Therefore, this attack of repeated encryption may be very dangerous to potential users, and the users must be careful to choose the p's which make the loops long instead of short. As p and q are increased, the loops also increase in length. The repeated encryption attack discussed so far is for $b=0$. If $b\neq 0$, then the repeated encryption attack reduces to the Pollard's algorithm for factoring r.

The chances of a successful repeated encryption attack are highly dependent on which of the four cases is encountered. The repeated encryption attack is successful if cases 1) through 3) occur. If one of the first three cases does not occur, then the best thing to do is to choose another m for repeated encryption. The speed of the repeated encryption attack will depend on the length of the repeated encryption loop. If messages corresponding to shorter loops for repeated encryption can easily be found, then the repeated encryption attack can be used very quickly to extract p or q.

We can lower bound the probability of success for the repeated encryption attack. For large r, most of the cryptograms will be four-solutions cryptograms. If we choose a message, m that is a

two-solutions message, m we will be successful. However, if the message, m, is a four-solutions message the result of the repeated encryption attack will fall in one or more of the four cases. The probability of case 1) or 4) is about 1/4, and of case 2) is about 1/2. We will succeed if either the original message is found or one of the primes is found, so we succeed if our attack falls into case 1), 2) or 3). Since case 3) only occurs with case 4), the probability of case 3) is less than 1/4. Therefore, our probability of success using the repeated encryption attack is greater than 3/4.

9.3 A VARIATION OF POLLARD'S ALGORITHM CAN BE USED FOR A REPEATED ENCRYPTION ATTACK

The Pollard algorithm for factoring large numbers is very similar to the repeated encryption method discussed in chapter 4. The basic observation of the Pollard algorithm is that for a function F such that the mapping $F:\{0, 1, \ldots, r-1\}\rightarrow\{0, 1, \ldots, r-1\}$ is random, one chooses numbers $x_0, x_1, \ldots, x_j$ from the set $\{0, 1, \ldots, r-1\}$ and computes the equivalences:

$x_0 = f(x_{j+1})$
$x_1 = f(x_{j+2})$
.
.
.
$x_j = f(x_{2j})$,

then the occurrence of cycling will occur in $O(r^{1/2})$ steps. The way to detect the cycle is to compute x_j and x_{2j} for $j = 1, 2, \ldots$. Then the occurrence $x_j = x_{2j}$ will happen before $i>k$, where k is the tail of the rho. Rho is the shape that the cryptograms trace as they are repeatedly encrypted. The tail of the rho is the number of times the function must be calculated before the x's get into the head of the rho or the cycle part of the rho.

For a polynomial function F, the easiest to calculate is usually chosen to be

$F(x) = x^{2\pm}1 \pmod r$,

where $r = p*q$ in the Rabin scheme. However, in the Rabin scheme the function F is also a mapping from the sets $\{0, 1, \ldots, p-1\}$ and $\{0,1,\ldots,q-1\}$ onto themselves, so that there are two smaller rhos that can be multiplied together to get the one large rho for r.

Therefore, when $x_j = x_{2j}$ on one of the smaller rhos, the function has already started to cycle on the smaller rho, and the g.c.d.$(x_{2j}-x_j, r) =$ p or q, whichever is smaller. When $x_j = x_{2j}$ for the larger rho, and the g.c.d.$(x_{2j}-x_j, r) =$ p or q, whichever prime is larger. Therefore, the Pollard method will work if one schecks each time for the g.c.d.$(x_{2j}-x_j, r) =$ p or q. This method expects to find one of the smallest prime, say p, in order $O(p^{1/2})$ time, and all the prime factors in $O(r^{1/4})$ time

regardless of the number of factors. This method is almost equivalent to the repeated encryption method discussed before, except that method used here is the function $x^2 \pm 1$ instead of x^2.

9.4 THE EQUIVALENCE OF DECRYPTION TO FACTORING ENABLES A CHOSEN CIPHERTEXT ATTACK

The proof of equivalence of decryption to factorization of r enables a chosen ciphertext attack, defined as an attack in which one set of plaintext-ciphertext pairs is known and the cryptanalyst has a black box, which represents the decryption mechanism. In the Rabin scheme if a plaintext-ciphertext pair, $m \rightarrow z$; is known, then it is possible to mount a chosen ciphertext attack, by sending z as the ciphertext to the receiver. If the receiver decrypts the ciphertext, z, and the sender acquires the decrypted ciphertext, m_1, then the sender knows a pair of solutions to the decryption of z. Therefore, if the decryption algorithm is random, the sender has a 50% chance of breaking the Rabin scheme:

$m = m_1 \pmod{p}$, and $m = -m_1 \pmod{q}$, or
$m = -m_1 \pmod{p}$, and $m = m_1 \pmod{q}$.

So with probability of ½ one has

$(m - m_1, r) = p$ or q.

Therefore, the chance of a chosen ciphertext attack on the Rabin scheme is very high, if the receiver gives out the decrypted ciphertext.

9.5 THE EQUIVALENCE OF DECRYPTION TO FACTORING DOES NOT CONTRIBUTE TO OTHER ATTACKS

9.5.1 HOW PROOF OF EQUIVALENCE OF DECRYPTION TO FACTORIZATION OF R DOES NOT CONTRIBUTE TO CHOSEN PLAINTEXT ATTACK

The proof of equivalence of decryption to factorization of r does not contribute to chosen plaintext attacks. A chosen plaintext attack is defined as an attack in which the cryptanalyst has a black box, which represents the encryption mechanism, and can always be launched in a public-key cryptosystem. Therefore, the chosen plaintext attack does not help the cryptanalyst otherwise all public-key systems would be insecure. Since decryption was proven equivalent to factorization, the chance that the cryptanalyst can break the scheme with only a chosen plaintext attack is as slight as that of factoring r.

The cryptanalyst has the plaintext and ciphertext of any plaintext he wishes. If the cryptanalyst can somehow get the receiver to decrypt the ciphertext for him, the cryptanalyst then once again has a chosen ciphertext attack, as previously discussed.

9.5.2 HOW PROOF OF EQUIVALENCE OF DECRYPTION TO FACTORIZATION OF R DOES NOT CONTRIBUTE TO KNOWN CIPHERTEXT ATTACK

The proof of equivalence of decryption to factorization of r does not contribute to ciphertext attack. A ciphertext attack is defined as an attack in which the cryptanalyst tries to break the scheme with only the ciphertext. This is even more difficult than a chosen plaintext attack, since the cryptanalyst does not even know what the plaintext is. The only hope for the cryptanalyst is to factor r, so the problem is once again reduced to factoring r.

9.5.3 HOW PROOF OF EQUIVALENCE OF DECRYPTION TO FACTORIZATION OF R DOES NOT CONTRIBUTE TO KNOWN PLAINTEXT-CIPHERTEXT PAIR ATTACK

The proof of equivalence of decryption to factorization of r does not contribute enough to a plaintext-ciphertext pair attack to make such an attack dangerous. A plaintext-ciphertext pair attack is defined as an attack in which the cryptanalyst has a plaintext-ciphertext pair. This attack is a degenerate chosen plaintext attack in which the cryptanalyst only has plaintext-ciphertext pairs and cannot produce any more. The possibility of a successful attack using this method relies heavily on chance. If the cryptanalyst can somehow have the receiver decrypt the ciphertext for one of the plaintext-ciphertext pairs, then the cryptanalyst has a probability of ½ of breaking the scheme under the same analysis as the chosen ciphertext attack. If the cryptanalyst finds two plaintext-ciphertext pairs with the same ciphertext, then the cryptanalyst has a probability of ½ of breaking the scheme under the same analysis as the chosen ciphertext attack. Therefore, unless the cryptanalyst is very lucky and is able to find two plaintext-ciphertext with the same ciphertext, or is able to have the receiver produce another set of plaintext for a given ciphertext, there is very little chance of breaking the scheme.

9.6 THE EQUIVALENCE OF DECRYPTION TO FACTORING CONTRIBUTES TO POSSIBLE SIGNATURE ATTACK

9.6.1 HOW REDUCTION OF FACTORING TO FORGING SIGNATURES IS UNDESIRABLE

This section will deal with signature attacks, especially how reduction of factoring to forging signatures is undesirable. If the Rabin signature scheme involved only decryption of the message using one's decryption key, then the cryptanalyst could launch a signature attack by having the user sign any message. If the user signs the message that is the ciphertext part of a known plaintext-ciphertext pair, and the cryptanalyst acquires the signature then he has launched a chosen ciphertext attack. Therefore, it is unwise to have the signature scheme equivalent to decryption for the Rabin scheme. Rabin patches this problem in his own scheme.

Suppose factoring can be reduced to forging signatures, then one can factor by forging signatures. If factoring were proven equivalent to forging signatures, then the cryptanalyst could simply have a user sign a ciphertext message, and acquire the signature in order to launch a chosen ciphertext attack. If is successful, then the cryptanalyst can factor r and break the scheme; however, if the reduction of factoring to forging signatures is not possible, then he cannot factor r even though he can forge signatures. Therefore, the reduction of factoring to forging signatures is undesirable and paradoxical since normally one would like to prove equivalence to factoring r to strengthen one's scheme. In this case it weakens the scheme.

9.6.2 RABIN ADDED PATCHES TO PROTECT HIS SCHEME FROM SIGNATURE ATTACKS

The Rabin signature scheme provides patch so that factorization is not equivalent to forging signatures. Suppose that a user S, wants to sign a message, m, so he adds an additional suffix word, s, of an agreed upon length to the message. The suffix is the output of some random function for each message to be signed. Let | be the concatenation function. User S compresses the new message m|s by a hashing function,

$$C(m|s)=c,$$

such that $c \leq r$. The computation of C is known publicly, so anyone can check the correctness of c. Then user S must check if the equation,

$$x(x+b)=c \pmod{r}, \qquad (*)$$

is still solvable. This means that $n=c+d^2$ is a quadratic residue (mod p) and (mod q), and is essentially solving (n|p) and (n|q), which can be done in a g.c.d. type fashion. If the resulting equation is not solvable, then the user S chooses another random s_1, and then tries c_1 to see if it satisfies equation (*). When user S finds an s_i that produces a solvable c_i, then he solves it for x. Therefore user S does not take the square root of any messages that are potential cryptograms, thus insuring invulnerability to a signature attack.

10 GENERAL ATTACKS ON THE WILLIAMS SCHEME

10.1 INTRODUCTION

This chapter discusses general attacks on the Williams scheme, including how: 1) the equivalence of decryption to factoring enables a chosen ciphertext attack; 2) the equivalence of decryption to factoring does not contribute to possible signature attacks; 3) the equivalence of decryption to factoring does not contribute to other attacks; 4) Williams added patches to protect his scheme from chosen ciphertext and signature attacks; and 5) there is no repeated encryption attack or Pollard's algorithm attack on the Williams scheme.

10.2 THE EQUIVALENCE OF DECRYPTION TO FACTORING ENABLES A CHOSEN CHIPHERTEXT ATTACK

This section discusses a chosen ciphertext attack against the Williams scheme. In this attack, the cryptanalyst chooses a ciphertext encrypted in the wrong manner and introduces it into the system as real ciphertext. The cryptanalyst hopes that the receiver believes the ciphertext to be authentic, and consequently releases the decoded chosen ciphertext which will enable the cryptanalyst to find p or q. Let the cryptanalyst, A, select an X such that $2(2X+1)<r$ and $(2*X+1|r)=1$. Then A sends $K=(2(2*X+1))^{2e} \pmod r$ to receiver B, which is normally $K'=(4(2*X+1))^{2e}$. If B believes that it is an authentic ciphertext, then he will calculate $M=D^1(D^2(K)) \pmod r$, and if A can somehow get M from B, then A can break B's system with probability 1. This is different than in the Rabin scheme where the probability of breaking the system is only ½ even if A acquires the decrypted chosen ciphertext.

The method by which A can break B's system is fairly simple. A calculates $D=((D^1)^{-1}(M))$, and then notes that $D=(2(2*X+1))^{2ed}=2(2*x+1)(2(2*x+1))^{(p-1)(q-1)/4}$. Since A knows X and D, he can calculate $(2(2*X+1))^{(p-1)(q-1)/4}$. Since

$$(2(2*X+1)|r)=-1,$$

A can factor B's r by simply calculating

$$((2(2*X+1))^{(q-1)(p-1)/4}-1,r)=p \text{ or } q.$$

The reason is as follows: since $(2(2*X+1)|r)=-1$, one must have either

$$(2(2*X+1)|p)=1, \text{ or}$$
$$(2(2*X+1)|q)=1.$$

If this is so then we have either

$(2(2*X+1))^{(p-1)/2}=1 \pmod{p}$, or
$(2(2*X+1))^{(q-1)/2}=1 \pmod{q}$,

which implies,

$(2(2*X+1))^{(p-1)(q-1)/4}=1 \pmod{p}$, or
$(2(2*X+1))^{(q-1)(p-1)/4}=1 \pmod{q}$, respectively,

which implies,

$((2(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod{p}$, or
$((2(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod{q}$, respectively,

which implies,

$p|((2(2*X+1))^{(p-1)(q-1)/4}-1$, or
$q|((2(2*X+1))^{(p-1)(q-1)/4}-1$, respectively,

which implies,

$((2(2*X-, 1))^{(p-1)(q-1)/4}-1,r)=$ p or q.

Without a patch the Williams scheme is vulnerable to this attack, therefore Williams later added a patch.

10.3 THE EQUIVALENCE OF DECRYPTION TO FACTORING DOES NOT CONTRIBUTE TO POSSIBLE SIGNATURE ATTACK

The signature attack proposed on the Rabin scheme if the signature were merely a decryption or square-root function does not apply here. In fact, because of the way Williams set up his signature scheme, there is no need for patching the signature scheme, and it is not equivalent to factoring. This is so because his signature scheme does not decrypt the input, but rather performs half of an encryption and half of a decryption. The signature for some user, A, with some message, M, is not $S=D^{2A}(D^{1A}(M))$, but is $S=D^{2A}(E^{1A}(M))$. This signature can then be checked by solving

$$D^{1A}(E^{2A}(S))=D^{1A}(E^{2A}(D^{2A}(E^{1A}(M))))=M \pmod{r}.$$

This will obviously be true if the original message was M, because

$$E^{2A}(D^{2A}(M))=(M)^{2ed}=D^{2A}(E^{2A}(M)) \pmod{r}.$$

Only the user A could have made the signature, S, since he is the only one with the decryption function, D^{2A}.

If user A signs a message, he will not provide B with enough useful information for factoring r. For the cryptanalyst B can only obtain $S=D^{2A}(E^{1A}(M))$, M, and $E^{1A}(M)$. In this case $(E^{1A}(M)|r)=1$, so B has insufficient enough information to factor r.

On the other hand, if A made a mistake and his first encryption function was such that $(E^{1A}(M)|r)=-1$, then B can factor r. If B knows that $(E^{1A}(M)|r)=-1$, then B gives A a message, M, such that $(2*M+1)|R)=1$. Since A's first encryption function is non-Jacobi, $(E^{1A}(M)|r)=-1$, he will use E^{1A} to get $(2(2*M+1))$. Since $(2|r)=-1$, we have that $((2(2*M+1))|r)=-1$. User A will sign the message as

$$S=D^{2A}(E^{1A}(M))=(2(2*M+1))^{2d} \pmod{r}.$$

Then B receives the signed message, S, and calculates

$$E^{2A}(S)=(2(2*M+1))^{2ed}=2(2*M+1)(2(2*M+1))^{(p-1)(q-1)/4} \pmod{r},$$

so B can solve for $(2(2*M+1))^{(p-1)(q-1)/4} \pmod{r}$.
A can factor B's r by simply calculating

$$((2(2*X+1))^{(q-1)(p-1)/4}-1,r)=p \text{ or } q. \qquad (**)$$

The reason for this is as follows: since $(2(2*X+1)|r)=-1$, one must have either

$(2(2*X+1)|p)=1$, or
$(2(2*X+1)|q)=1$.

If this is so then we have either:

$(2(2*X+1))^{(p-1)/2}=1 \pmod{p}$ or
$(2(2*X+1))^{(q-1)/2}=1 \pmod{q}$,

which implies,

$(2(2*X+1))^{(p-1)(q-1)/4}=1 \pmod{p}$ or
$(2(2*X+1))^{(q-1)(p-1)/4}=1 \pmod{q}$, respectively,

which implies,

$((2(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod{p}$ or
$((2(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod{q}$, respectively,

which implies,

$p|((2(2*X+1))^{(p-1)(q-1)/4}-1$
$q|((2(2*X+1))^{(p-1)(q-1)/4}-1$, respectively,

which implies,

$((2(2*X+1))^{(p-1)(q-1)/4}-1,r) = p \text{ or } q.$

If, on the other hand, $(E^{1A}(M)|r)=1$, then the first encryption of M will be $(4(2*M+1))$ (mod r). Since $(4|r)=1$, we have $((4(2*M+1))|r)=1$. Repeating the above procedure, we obtain the same results with $(4(2*M+1))$ replacing $(2(2*M+1))$ down to step (**). At step (**) we have the following:

$((4(2*M+1))^{(p-1)(q-1)/r}-1,r)\neq p \text{ or } q.$

The reason for this is as follows: since $(4(2*X+1)|r)=1$, either

$(4(2*X+1)|p)=1$ and $(4(2*X+1)|q)=1$. or
$(4(2*X+1)|p)=-1$ and $(4(2*X+1)|q)=-1$.

If this is so then either

$(4(2*X+1))^{(p-1)/2}=1 \pmod p$ and
$(4(2*X+1))^{(q-1)/2}=1 \pmod q$, or

$(4(2*X+1))^{(p-1)/2}=-1 \pmod p$ and
$(4(2*X+1))^{(q-1)/2}=-1 \pmod q$,

which implies,

$(4(2*X+1))^{(p-1)(q-1)/4}=1 \pmod p$ and
$(4(2*X+1))^{(p-1)(q-1)/4}=1 \pmod q$, or

$(4(2*X+1))^{(q-1)(p-1)/4}=-1 \pmod p$ and
$(4(2*X+1))^{(q-1)(p-1)/4}=-1 \pmod q$, respectively,

which implies,

$((4(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod p$ and
$((4(2*X+1))^{(p-1)(q-1)/4}-1)=0 \pmod q$, or

$((4(2*X+1))^{(p-1)(q-1)/4}+1)=0 \pmod p$ and
$((4(2*X+1))^{(p-1)(q-1)/4}+1)=0 \pmod q$, respectively,

which implies,

$p|((4(2*X+1))^{(p-1)(q-1)/4}-1$ and
$q|((4(2*X+1))^{(p-1)(q-1)/4}-1$, or

$p|((4(2*X+1))^{(p-1)(q-1)/4}+1$ and

$q|((4(2*X+1))^{(p-1)(q-1)/4}+1$, respectively,

which implies,

$((4(2*X+1))^{(p-1)(q-1)/4}-1,r) = 1$ or r.

So the Williams signature scheme seems to be secure against signature attacks without making a patch. Since the Williams scheme is not vulnerable to signature attacks, his signature scheme is essentially a patch built into his public-key scheme.

10.4 EQUIVALENCE OF DECRYPTION TO FACTORING DOES NOT CONTRIBUTE TO OTHER ATTACKS

In this case the equivalence of decryption to factorization of r again contributes to chosen ciphertext attack but not to the other forms of attack. Since decryption is equivalent to factorization, the cryptanalyst simply performs a chosen ciphertext attack and retrieves the message corresponding to the incorrectly encrypted ciphertext, and can then factor r. This situation is somewhat paradoxical, since proving equivalence of decryption to factorization of r is in some ways beneficial, while in other ways it is not. One would think that it would always be beneficial, but this is not the case as shown in the chosen ciphertext attack. Therefore, proof of equivalence of decryption to factorization of r is not always desirable.

10.5 WILLIAMS ADDED PATCHES TO PROTECT HIS SCHEME FROM CHOSEN CIPHERTEXT AND SIGNATURE ATTACKS

To solve the problem for the ciphertext attack, Williams proposes a patch to make his system secure from this attack. To avoid the chosen ciphertext attack, each user B of the system requests user A to send

$E^B(M)$, Q, and $C(M,D^{2A}(E^{1A}(Q))$,

inplace of sending only $E^B(M)$. Q should also change each time a new message is sent, where Q is some plaintext message subject to some previously agreed upon conditions. The function, C(K,N), is a conventionally cryptographic function where K is the key and N is the message. The cryptanalyst cannot determine M from $E^B(M)$ or find $D^{2A}(E^{1A}(Q))$ without factoring r. Thus, he cannot determine M from $C(M, D^{2A}(E^{1A}(Q))$, even if he knows the form of C.

This procedure protects B from a chosen ciphertext attack. Suppose A sends B some X, which is supposed to be $E^B(M)$. Using X, B calculates M, and using M as the key for C(M, $D^{2A}(E^{1A}(Q))$), B can retrieve $D^{2A}(E^{1A}(Q))$. He can then determine if M was indeed a valid message, since he can check whether:

$$D^{1A}(E^{2A}(D^{2A}(E^{1A}(L))))=Q \qquad (*)$$

is true. If it is not true, then B knows something is wrong, and if it is, then A cannot be tricking B, since he already knows M. The equation (*) serves as a signature scheme for M.

10.6 THERE IS NO REPEATED ENCRYPTION OR POLLARD'S ALGORITHM ATTACK ON THE WILLIAMS SCHEME

There is no real possibility of a repeated encryption attack or Pollard's algorithm attack against the Williams scheme. This is because one cannot always encrypt a cryptogram, C, since $(2(2*C+1))<r$ for $((2*C+1)|r)=-1$, or $(4(2*C+1))<r$ for $((2*C+1)|r)=1$, may not always be true so a repeated encryption attack cannot be launched.

11 CONCLUSIONS AND FUTURE RESEARCH

11.1 INTRODUCTION

We conclude that the Rabin and Williams schemes have some potential problems, and that users of such schemes should be aware of possible chosen ciphertext attacks. In chapter nine and ten several methods of attack on the Rabin and Williams schemes were presented. Some were more promising than others, hence it is very important for each user to choose the p's, b's and m's with great care to prevent possible attack.

The ciphertext should not be decrypted and randomly revealed publicly. Rather, one should ensure that the sender knows the decrypted message, otherwise the decrypted message could be used to launch a chosen ciphertext attack. The reason for the possible differences in the decrypted message and the original message is caused by the multiple decryptions in the Rabin scheme and is caused by a non-Jacobi ciphertext in the Williams scheme. The security against the chosen ciphertext attack can be accomplished in both the Rabin and the Williams schemes with the patch by Williams, but this is impractical and implementation of the secure RSA scheme maybe more feasible.

If primes are chosen such that they differ by a small amount, then the number of two-solutions, the number of z's and m's being cp or cq, and the length of the repeated encryption attack loops are all minimized. However, if the primes are chosen such that they differ by a small amount, then a particular prime will be about $\sqrt{r}$ and it will be easy to factor. Therefore the chosen primes should be close enough to minimize the above effects and differ enough to make the factoring of r difficult. Although this choice may be difficult, it is essential for minimization of cryptanalytic attack.

The b's should also be chosen unequal to cp or cq, and so it is not known how close they are to cp or cq. It is unwise to change the b's very often, since then the cryptanalyst has a greater chance of finding cp or cq. Pollard's algorithm for factoring r does not work for $b=0$. Therefore, it seems that the use of the parameter b is more detrimental than helpful. The use of b's actually helps the cryptanalyst, so it is recommended that the use of b's should be eliminated in order to reduce the risk of potential attacks.

The choice of m's is very important. The m's must not be cp or cq or cause a two-solutions cryptogram; otherwise, potential attacks are possible. Even if all of the input parameters are carefully chosen to ensure no possible leak of information on the primes, the chance of successful potential attacks exists by using the repeated encryption algorithm to break the scheme. This is because a chosen plaintext attack can always be attempted on any public-key scheme, and there is no way to prevent the cryptanalyst from trying a repeated encryption attack.

The ambiguity problem must be solved with either additional code bits or by switching to the Williams scheme.

Therefore, at present, the Rabin and the Williams schemes may not be suitable for high-speed satellite communications due to the threat of a chosen ciphertext attack. Strengthening the Rabin and the Williams schemes with a patch will require extra computation and time, so one may favor the RSA scheme in order to avoid the chosen ciphertext attack.

11.2 DIRECTIONS FOR FUTURE RESEARCH

The method described below details how cryptanalysis was done on the Rabin scheme. Many different pairs of primes were used, and all possible m's were encrypted for each pair of primes in an attempt to find as many properties as possible. Many plots were also used. One of the possible areas of future research is to attempt to use this type of cryptanalysis on future public-key schemes. Some of the properties of the schemes are initially extracted mathematically, others can be found by using computer simulation. Once the properties have been found, the person attempting cryptanalysis can concentrate on using the properties to find possible attacks on the scheme.

12 BIBLIOGRAPHY

REFERENCES

[Adleman]

Adleman, L., *Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography,* Department of Mathematics and Laboratory of Computer Science, M.I.T..

Adleman, L., "The use of Public-Key Cryptography in Communication System Design," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 20-23, Nov. 1978.

[Arazi]

Arazi, B., *A Public-Key Cryptosystem based on adding Pseudo-Random values to the text,* Department of Electrical Engineering, Ben Gurion University of Negev Beer-Sheba, Israel.

[Branstad]

Branstad, D. K., "Security of Computer Communication," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 33-40, Nov. 1978.

[Campbell]

Campbell, C. M., "Design and Specification of Cryptographic Capabilities," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 15-19, Nov. 1978.

[Davis]

Davis, R. M., "The Data Encryption Standard in Perspective," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 5-9, Nov. 1978.

[Diffie]

Diffie, W., and Hellman, M. E., "Exhaustive cryptanalysis of the NBS Data Encryption Standard," *Computer,* vol. 10, no. 6, pp. 74-84, June 1977.

Diffie, W., and Hellman, M. E., "Multiuser cryptographic techniques," in Proc. Nat. Computer Conf. (New York, NY), June 7-10, 1976.

Diffie, W., and Hellman, M. E., "New directions in cryptography," *IEEE Tran. Inform. Theory,* vol. IT-22, pp. 644-654, Nov. 1976.

Diffie, W., "The Outlook for Computer Security," *Mini-Micro Systems,* pp. 43-44, Oct. 1978.

Diffie, W., and Hellman M. E., "Privacy and Authentication: An Introduction to Cryptography," *Proc. IEEE,* vol. 67, pp 402-403, March 1979.

[Ehrsam]

Ehrsam, W. F., Matyas, S. M., and Meyer, C. H., Tuchman, W. L., "A cryptographic key management scheme for implementing the Data Encryption Standard," IBM Syst. J., vol. 17, no. 2, pp. 106-125, 1978.

[Federal Register]

Federal Register, "Proposed Federal Information Processing Data Encryption Standard," *Cryptologia,* Vol. 1, no. 3, pp., 292-306, July 1977.

[Feistel]
Feistel, H., "Cryptography and Computer Privacy," *Scientific American,* Vol. 228, no., 5, pp.15-23, May 1973.

[Friedman]
Friedman, W. F., "Cryptology," *Encyclopedia Britanica,* vol. 6, pp. 844-851, 1967.

[Gait]
Gait, J., "Validating the correctness of hardware implementations of the NBS Data Encryption Standard," National Bureau of Standard, Special Pub. 500-20.

[Government Services Administration]
"Telecommunications: Compatibility requirements for use of the Data Encryption Standard," Proposed Federal Standard 1026, General Services Administration, Oct. 13, 1977.

"Telecommunications: Security requirements for use of the Data Encryption Standard," Proposed Federal Standard 1027, General Services Administration, Aug. 25, 1977.

[Gersho]
Gersho, A., *On perfect Secrecy Encryption of Analog Signals,* Bell Laboratories, Murray Hill, New Jersey, 07974, April 11, 1979.

[Grossman]
Graossman, E. K., Tuckerman, B., "Analysis of a Weakened Feistel-Like Cipher," IBM Thomas J. Watson Research Center Yorktown Heights, New York, 10598, pp. 46.3.1-46.3.5, 1978.

[Guy], R. K., "How to factor a number', *Congressus Numeratium XVI, Proceedings Fifth Maitoba Conference on Numerical Mathematics,* Winnipeg, 1976, pp. 49-89.

[Heaton]
Heaton, D. L., and Wright, H. O., "LSI implementation of proposed Data Encryption Standard," presented at the Nat. Computer Conf., New York, N.Y., June 7-10, 1976.

[Hellman]
Hellman, M. E., *A Crypanalytic Time-Memory Trade-off,* Electrical Engineering, Stanford University, Stanford, Cal..

Hellman, M. E., "An overview of Public-Key Cryptography," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 24-31, Nov. 1978.

Hellman, M. E., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., Pohlig, S., and Schweitzer, P., "Results of an initial attempt to Cryptanalyze the NBS Data Encryption Standard," Electrical Engineering Dep., Stanford Univ., Stanford, CA., SEL 76-042, Sept. 9, 1976.

[Herlestam]
Herlestan, T., Critical remarks on some public-key cryptosystems, *BIT,* 18 (1978), Staff of Defense Dept. of Signal Security, Helsingborg, Sweden, pp. 493-496, Sept. 22, 1978.

[Ingemarsson]
Ingemarsson, I., "Security Problems in the Transmission of Negotiable Documents," *ICC 1979.*

[Kahn]
Kahn, D., "Cryptology," *Encyclopedia Americana,* vol. 8, pp. 276-285, 1976.

Kahn, D., *The Codebreakers, The Story of Secret Writing,* New York: Macmillan, 1976.

[Kent]
Kent, S. T., "A Comparison of Some Aspects of Public-Key and Conventional Cryptosystems," *ICC 1979.*

[Kinnucan]
Kinnucan, P., "Data Encryption Gurus: Tuchman and Meyer," *Mini-Micro Systems,* pp. 54-60, Oct. 1978.

[Kirchhofer]
Kirchhofer, K. H., "Are Analog Voice Security Systems Obsolete?", *ICC 1979.*

[Knuth]
Knuth, D. E., *The Art of Computer Programming, Vol. II: Seminumerical Algorithms,* Addison-Wesley, 1969, pp. 293.

Knuth, D.E. *The Art of Computer Programming, Vol. III: Sorting and Searching.* Addison-Wesley, Reading, Mass. 1973.

[Matyas]
Matyas, S. M., and Meyer, C. H., "Generation, distribution and installation of cryptographic keys," IBM Syst. J., vol 17, no. 2, pp. 126-137, 1978.

[Merkle]
Merkle, R. C., and Hellman, M. E., "Hiding information and signatures in trap door knapsacks," *IEEE Trans. Inform. Theory,* vol. IT-24, pp. 525-530, Spet. 1978.

Merkle, R. C., "Secure communication over insecure channels," *Commun. ACM,* vol. 21, pp. 294-299, Apr. 1978.

[Meyer]
Meyer, C. H., Tuchman, W. L., "Putting Data Encryption to Work," *Mini-Micro Systems,* pp.46-53, Oct. 1978.

[Morris]
Morris, R., Sloane, N. J. A., Wyner, A. D., "Assessment of the National Bureau of Standards proposed federal data encryption standard," *Cryptologia,* vol. 1, pp. 281-291, July 1977.

Morris, R., "The Data Encryption Standard Retrospective and Prospects," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 11-14, Nov. 1978.

[National Bureau of Standards]
"Data Encryption Standard," National Bureau of Standards, Federal Information Processing Standard (FIPS) Publication No. 46, Jan. 1977.

[Orceyre]
Orceyre, M. J., and Heller, R. M., "An Approach to Secure Voice Communication Based on the Data Encryption Standard," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 5-9, Nov. 1978.

[Pohlig]
Pohlig, S. C., Hellman, M. E., *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance,* Department of Electrical Engineering, Stanford University, Stanford California, Nov. 3, 1976.

[Rabin]
Rabin, M. O., *Digitalized Signatures and Public-Key Functions as Intractable as Factorization,* M.I.T. Laboratory for Computer Science, Technical Report LCS/TR-212, Jan. 1979.

[Rivest]
Rivest, R. L., Shamir, A., and Adleman, L., "On digital signitures and public-key cryptosystems," *Commun. ACM,* vol. 21, pp. 120-126, Feb. 1978.

Rivest, R. L., "Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem," *Cryptologia,* vol. 2, no. 1, pp. 62-65, Jan. 1978.

[Schroeppel]
Schroeppel, R. and Shamir, A., *A $TS^2 = O(2^n)$ Time/Space Trade-off for Certain NP-Complete Problems,* Department of Mathematics, M.I.T..

[Shamir]
Shamir, A., *A Fast Signature Scheme,* M.I.T. Department of Mathematics, May 1978.

Shamir, A., *How to Share a Secret,* M.I.T. Department of Mathematics, Feb. 1979.

Shamir, A., Zippel, R. E., *On the security of the Merkle-Hellman Cryptographic Scheme,* M.I.T..

[Simmons]
Simmons, G. J., and Norris, M. M., "Preliminary comments on the M.I.T. public-key cryptosystem," *Cryptologia,* vol. 1, pp. 406-414, Oct. 1977.

[Sinkov]
Sinkov, A., *Elementary Cryptanalsis, A Mathematical Approach,* New York: Random Hose, New Mathematical Library, no. 2, 1968.

[United States Senate Select Committee on Intelligence]
United States Senate Select Committee on Intelligence, "Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard," *IEEE Communications Society Magazine,* Vol. 16, no. 6, pp. 52-55, Nov. 1978.

[Williams]
Williams, H. C., *A Modification of the RSA Public-Key Encryption Procedure,* University of Manitoba, Department of Computer Science, Scientific Report No. 91, 1979.

Williams, H. C., and Schmid, B., *Some Remarks concerning the M. I. T. Public-Key Cryptosystem,* University of Manitoba, Department of Computer Science, Scientific Report No. 91, 1979.

[Wyner]
Wyner, A. D., "A Technique for Analog Voice Encryption," *ICC* 1979.

Biographical Note

Moses Hsingwen Ma was born on March 15, 1958 in New York, New York. He attended Montgomery College while in high school for advanced math courses. His undergraduate institution was Massachusetts Institute of Technology where he completed his Bachelor of Science and Master of Science degrees in the Electrical Engineering and Computer Science department. He attended M.I.T. from September, 1976 to the present. He has three years work experience in industry. He is an Eagle Scout and a member of the Eta Kappa Nu Electrical Engineering Fraternity.