ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 5, October 2012

Block Cipher Principles on Cryptography

Mayuri Khatri and Nitin Shukla

***Abstract*— The history of cryptography is long and goes back at least 4,000 years to the Egyptians, who used hieroglyphic codes for inscription on tombs. Since then many cryptosystems, also called ciphers, have been developed and used. Many of these old ciphers are much too weak to be used in applications today, because of the tremendous progress in computer technology. There are essentially two types of encryption schemes, one-key and two-key ciphers. In one-key ciphers the encryption of a plaintext and the decryption of the corresponding ciphertext are performed using the same key. Until 1976 when Diffie and Hellman introduced *public-key* or two-key cryptography all ciphers were one-key systems. Therefore one-key ciphers are also called conventional cryptosystems. Conventional cryptosystems are widely used throughout the world today, and new systems are published from time to time. There are two kinds of one-key ciphers, stream ciphers and block ciphers. In stream ciphers a long sequence of bits is generated from a short string of key bits, and is then added bitwise modulo 2 to the plaintext to produce the ciphertext. In block ciphers the plaintext is divided into blocks of a fixed length, which are then encrypted into blocks of ciphertexts using the same key. Block ciphers can be divided into three groups: Substitution ciphers, transposition ciphers and product ciphers.**
In the following a few examples of the different types of block ciphers are given.

Notation: Let *AM* and *AC* be the alphabets for plaintexts and ciphertexts, respectively. Let *M* = *m*0,*m*1, . . . ,*mn*−1 be an *n*-character plaintext, s.t. for every *i*, *mi* ∈ *AM* and let *C* = *c*0, *c*1, . . . , *cn*−1 be a ciphertext, s.t. for every *i*, *ci* ∈ *AC*. We assume that an alphabet *AX* is isomorphic with *INAX*...

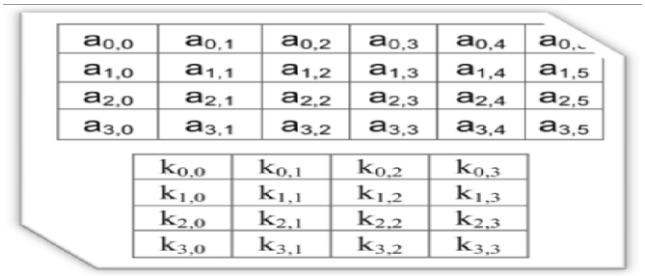

Fig 1: State (with Nb = 6) and encryption key (with Nk =4)

***Index Terms*— Cryptography, text encryption, block cipher, Advanced Encryption Standard.**

Manuscript received Oct 5, 2012.

***Mayuri Khatri**, Computer Technology and Applications Department , Rajiv Gandhi Technical University/ Shri Ram Institute of Technology, Jabalpur, (e-mail: mayuri.khatri3012@gmail.com). Jabalpur, India, 09479466709, Nitin Shukla, Computer Technology and Applications Department, Rajiv Gandhi Technical University/ Shri Ram Institute of Technology, Jabalpur, 08878143146.*

I. INTRODUCTION

In *cryptography*, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called *blocks*, with an unvarying transformation that is specified by a symmetric key. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data.

The modern design of block ciphers is based on the concept of an *iterated* product cipher. Product ciphers were suggested and analyzed by Claude Shannon in his seminal 1949 publication *Communication Theory of Secrecy Systems* as a means to effectively improve security by combining simple operations such as substitutions and permutations. Iterated product ciphers carry out encryption in multiple rounds, each which uses a different subkey derived from the original key. A widespread implementation of such ciphers is called a Feistel network, named after Horst Feistel, and notably implemented in the DES cipher. Many other realizations of block ciphers, such as the AES, are classified as substitution-permutation networks.

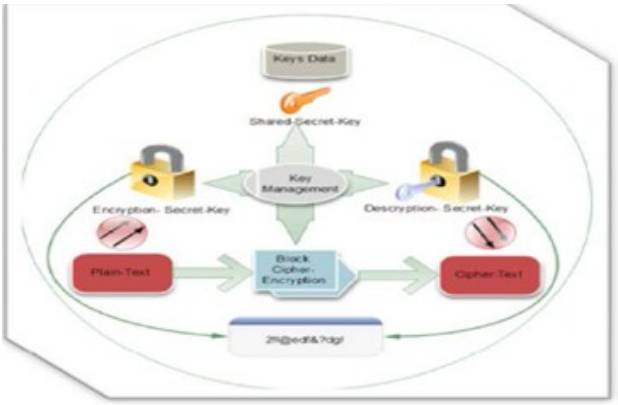

Figure 2: A Basic Cryptographic System

Objective of the Thesis

The public-key algorithm uses a one-way function to translate plaintext to ciphertext. Then, without the private key, it is very difficult for anyone (including the sender) to reverse the process (i.e., translate the ciphertext back to plaintext). A one-way function is a function that is easy to apply, but extremely difficult to invert. The most common one-way function used in public-key cryptography involves factoring very large numbers. The idea is that it is relatively easy to multiply numbers, even large ones, with a computer; however, it is very difficult to factor large numbers.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 1

The only known algorithms basically have to do a sort of exhaustive search (Does 2 go in to? Does 3? 4? 5? 6? and so on). With numbers 128 bits long, such a search requires performing as many tests as there are particles in the universe. For instance, someone wishing to receive encrypted messages can multiply two very large numbers together. She keeps the two original numbers a secret, but sends the product to anyone who wishes to send her a message. The encryption/decryption algorithm is based upon combining the public number with the plaintext. Because it is a one-way function, the only way to reverse the process is to use one of the two original numbers. However, assuming the two original numbers are very large, their product is even bigger; it would be impractical for an adversary to try every possibility to determine what the two original numbers were.

II. RSA – PUBLIC KEY CRYPTOGRAPHY ALGORITHM:

1) Introduction to RSA Algorithm:

RSA is one of the most popular and successful public key cryptography algorithms. The algorithm has been implemented in many commercial applications. It is named after its inventor's Ronald L. Rivest, Adi Shamir, and Leonard Adleman. They invented this algorithm in the year 1977. They utilized the fact that when prime numbers are chosen as a modulus, operations behave "conveniently". They found that if we use a prime for the modulus, then raising a number to the power (prime - 1) is 1.

RSA algorithm simply capitalizes on the fact that there is no efficient way to factor very large integers. The security of the whole algorithm relies on that fact. If someone comes up with an easy way of factoring a large number, then that's the end of the RSA algorithm. Then any message encrypted with the RSA algorithm is no more secure.

2) RSA Algorithm:

The encryption and decryption in the RSA algorithm is done as follows. Before encryption and decryption is done, we have to generate the key pair and then those keys are used for encryption and decryption.

a) Key Generation:

The first step in RSA encryption is to generate a key pair. Two keys are generated of which one is used as the public key and the other is used as the private key. The keys are generated with the help of two large prime numbers. The keys are generated as follows

1. Generate two large random primes p and q.
2. Compute n which is equal to product of those two prime numbers, n = pq
3. Compute $\varphi(n) = (p-1)(q-1)$.
4. Choose an integer e, $1 < e < \varphi(n)$, such that $\gcd(e, \varphi(n)) = 1$.
5. Compute the secret exponent d, $1 < d < \varphi(n)$, such that $ed \equiv 1 \pmod{\varphi(n)}$.
6. The public key is (n, e) and the private key is (n, d). The values of p, q, and $\varphi(n)$ should also be kept secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

b) Encryption:

Encryption is done using the public key component e and the modulus n. To whomever we need to send the message, we encrypt the message with their public key (e,n). Encryption is done by taking an exponentiation of the message m with the public key e and then taking a modulus of it. The following steps are done in encryption.

1. Obtain the recipient's public key (n,e)
2. Represent the plaintext message as a positive integer $m < n$
3. Compute the ciphertext $c = m^{\wedge e} \bmod n$.
4. Send the ciphertext c to the recipient.

c) Decryption:

Decryption is done using the Private key. The person who is receiving the encrypted message uses his own private key to decrypt the message. Decryption is similar to the encryption except that the keys used are different.

1. Recipient uses his private key (n,d) to compute $m = c^{\wedge d} \bmod n$.
2. Extract the plaintext from the integer representative m.

The RSA algorithm has been implemented in many applications and it is currently one of the most popularly used encryption algorithm. RSA algorithm is based fully on mathematics and in the next section we will see the mathematics behind RSA.

III. CONCLUSION

Cryptography can be a technology that develops, but as long as security is made by man, cryptography is as good as the practice of people who uses it. This paper focused on the different security issues for providing a secure and effective cryptography technique over the block cipher. Most of these issues occurred when users leave keys unattended, keys that were chosen were easy to remember or maintain the same keys for years. This can be resolved by the suggested model, using the encrypting key that existed independently as an external tool by managing keys sequentially.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 2, Issue 5, October 2012

IV. FUTURE ENHANCEMENT

- Sequentially, providing a secure and flexible cryptography mechanism raises the needs for analyzing and comparing different encryption algorithms for the aim of enhancing the security during the encryption process.
- Hence, this paper suggested a cryptography mechanism in the block cipher by managing the keys sequentially.
- These keys will works dependently for extracting and generating the content relation to be managed later by the key management that helps to communicate and share sensitive information.
- In particular, the importance of thorough, consistent key management processes among public safety agencies with interoperable functions cannot be overstated.
- This model aims to secure dissemination, loading, saving, and eliminating faults of keys to make encryption implementations effective.
- There are inherent possibilities if suitable key management processes are not accompanied because of the intricacy of dispensing keys to all block in a certain fashion.
- This risk can be meaningfully appeased through sufficient key controls and proper education on encryption key management.

REFERENCES

[1] Ashwak M,AL-Abiachi, Faudziah Ahmad, KuRuhana,"A Competitive Study of Cryptography Techniques over Block Cipher", IEEE 2011 UKSim 13th International Conference on Modelling and Simulation, **IEEE 2011.**

[2] W. Ehrsam, *et al.*, "A cryptographic key management scheme for implementing the Data Encryption Standard," *IBM Systems Journal,* vol. 17pp.106-125, 2010.

[3] W. Stallings, *Cryptography and network security: principles and practice*: Prentice Hall, 2010.

[4] B. Jyrwa and R. Paily, "An area-throughput efficient FPGA implementation of the block cipher AES algorithm,"2010, pp. 328-332.

[5] A. Barenghi, *et al.*, "Low voltage fault attacks to AES And RSA on general purpose processors," *IACR eprint archive,* vol. 130, 2010.

[6] S. Heron, "Advanced Encryption Standard (AES)," *Network Security,* vol. 2009, pp. 8-12, 2009.

[7] J. Katz and Y. Lindell, *Introduction to modern cryptography*: Chapman & Hall/CRC, 2008.

[8] J. Amigo, *et al.*, "Theory and practice of chaotic cryptography," *Physics Letters A,* vol. 366, pp. 211-216, 2007.

[9] N. Potlapally, *et al.*, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing,* pp.128-143, 2006.

[10] K. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *Signal Processing , IEEE Transactions on,* vol. 52, pp. 2975-2991, 2004.

[11] X. Zhang and K. Parhi, "Implementation approaches for the advanced Encryption standard algorithm," *Circuits and Systems Magazine, IEEE,* vol. 2, pp. 24-46, 2003.