IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 3, Issue 5, May 2015, 39-46

ENCRYPTION ALGORITHMS WITH EMPHASIS ON PROBABILISTIC ENCRYPTION & TIME STAMP IN NETWORK SECURITY

PINKI SINGH & RUCHIR BHATNAGAR

Research Scholar, Department of CSE & Mewar University, Chittorgarh, Rajasthan, India

ABSTRACT

Encryption is the process of converting a plain text message in to cipher text which can be decoded back in to the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryption which form the basis of network security. Encryption schemes are based on block or stream cipher.

The type of the length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In Conventional symmetric encryption a single key is used. With this key the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and decryption key are different. ONE is a public key by which the sender can encrypt the message and the other is a private key by which the recipient can decrypt the message.

KEYWORDS: Block Ciphers, Des Algorithm, Numerical Model for Data Development

INTRODUCTION

The necessicity of information security within an organization have undergone major changes in the past and present times. In the earlier times physical means is used to provide security to data. With the advent of computers in every field, the need for software tools for protecting files and other information stored on the computer became important. The important tool designed to protect data and thwart illegal users is computer security. With the introduction and revolution in communications, one more change that affected security is the introduction of distributed systems which requires carrying of data between terminal user and a set of computers. Network security measures are needed to protect data during their transmission. The mechanisms used to meet the requirements like authentication and confidentiality are observed to be quite complex.

To identify and support the security services of an organization at its effective level, the manager needs a systematic way. One approach is to consider three aspects of information security that is Security attack, Security mechanism and Security services. Security attack identifies different modes by which intruder tries to get unauthorized information and the services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. There is no single mechanism that will provide all the services specified. But we can identify a very important mechanism that supports all forms of information integrity is cryptographic technique. Encryption of information is the most common means of providing security.

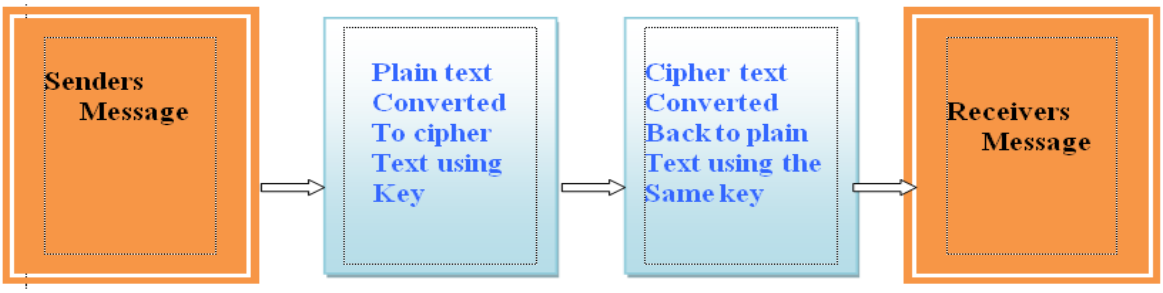

Figure 1: Encryption Model

This general model shows that there are four basic tasks in designing a particular security service.

- Designing an algorithm for performing encryption & decryption process.
- Generating the secret information with the help of algorithm of step 1.
- ujuj3. Identifying methods for the distribution and sharing of secret information.
- Identifying rules to be used by both the participating parties to make it secured.

A crypto system is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and public key. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 2.

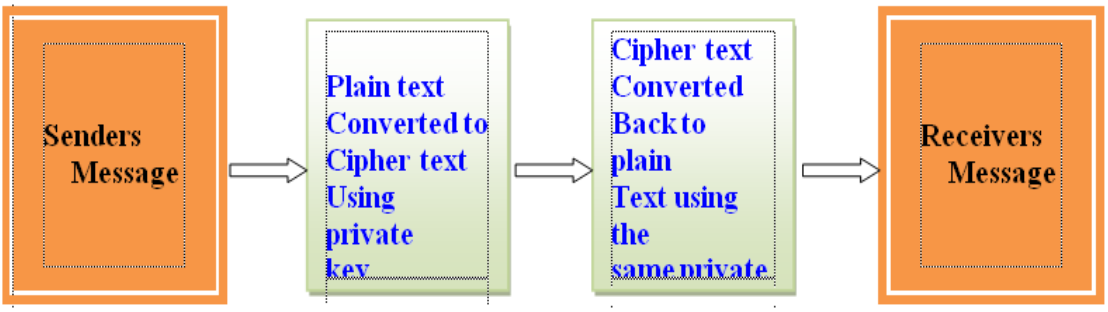

Figure 2: Symmetric-Key Encryption

The process of symmetric-key encryption can be very fast as the users do not experience any significant time delay because of the encryption and decryption. Symmetric-key encryption provides security to data as the key is shared only by the participating parties. It also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be confident that it is communicating with the other as long as the decrypted messages specify a meaningful sense.

Cipher Text Only Attack: Here the intruder is in hold of cipher text only. The crypto analyst has cipher text of several messages, all of which have been encrypted using the same encryption algorithm. The crypto analyst's job is to recover the plain text or the key used to encrypt the messages, in order to decrypt other part of messages encrypted with the same keys.

Known Plaintext Attack: The crypto analyst is in possession of pairs of known plain text and cipher text. His job is to get the key used to encrypt the messages or an algorithm to decrypt any messages encrypted with the same key.

Chosen Plaintext Attack (CPA): Here the crypto analyst is in hold of not only cipher text but also parts of chosen plain text. Here the intruder is identified to be placed at encryption site to do the attack. Differential crypto analysis is an example of this mode.

Chosen Cipher Text Attack (CCA): Under the CCA model, the crypto analyst is in possession of chosen cipher text and corresponding plain text being decrypted from the private key. After it has chosen the messages, however, it only has access to an encryption machine.

Chosen Text: In this model, the analyst posses the encipher algorithm, Cipher text to be decrypted, chosen plain text messages and corresponding cipher texts, fabricated cipher text with the corresponding decrypted plain texts developed by the private key.

SYMMETRIC ENCRYPTION SCHEMES

With *symmetric-key encryption***,** the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 1.1. Implementations of symmetrickey encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Block Ciphers

Block ciphers take as input the key and a block, often the same size as the key. Further, the first block is often augmented by a block called the initialization vector, which can add some randomness to the encryption.

DES Algorithm

The most widely used encryption scheme is based on Data Encryption Standard (DES). There are two inputs to the encryption function, the plain text to be encrypted and the key. The plain text must be 64 bits in length and key is of 56 bits. First, the 64 bits of plain text passes through an initial permutation that rearranges the bits. This is fallowed by 16 rounds of same function, which involves permutation & substitution functions. After 16 rounds of operation, the pre output is swapped at 32 bits position which is passed through final permutation to get 64 bit cipher text

Electronic Code Book (ECB) Mode: ECB mode divides the plaintext into blocks m1, m2, ..., mn, and computes the cipher text ci = Ei(mi). This mode is vulnerable to many attacks and is not recommended for use in any protocols. Chief among its defects is its vulnerability to splicing attacks, in which encrypted blocks from one message are replaced with encrypted blocks from another.

Triple DES

Given the potential vulnerability of DES to brute force attack, a new mechanism is adopted which uses multiple

encryptions with DES and multiple keys. The simplest form of multiple encryptions has two encryption stages and two keys. The limitation with this mechanism is it is susceptible to meet in the middle attack. An obvious counter to meet in the middle attack and reducing the cost of increasing the key length, a triple encryption method is used, which considers only two keys with encryption with the first key, decryption with the second key and fallowed by encryption with the first key. Triple DES is a relatively popular alternative to DES and has been adopted for use in key management standards.

DES: A variant of DES called a homophonic DES is considered. The DES algorithm is strengthened by adding some random bits into the plaintext, which are placed in particular positions to maximize diffusion, and to resist differential attack. Differential attack makes use of the exclusive-or homophonic DES. In this new scheme, some random estimated bits are added to the plaintext. This increases the certain plaintext difference with respect to the cipher text.

PUBLIC-KEY ENCRYPTION

The most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption. *Public-key encryption* (also called *asymmetric encryption*) involves a pair of keys a *public key* and a *private key*, used for security & authentication of data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with one key can be decrypted only with other key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, a combination of symmetric & Asymmetric schemes can be used in real time environment. This is the approach used by the SSL protocol.

Key Length and Encryption Strength: In general, the strength of encryption algorithm depends on difficulty in getting the key, which in turn depends on both the cipher used and the length of the key. For the RSA cipher, the strength depends on the difficulty of factoring large numbers, which is a well-known mathematical problem. Encryption strength is often described in terms of the length of the keys used to perform the encryption, means the more the length of the key, the more the strength. Key length is measured in bits. For example, a RC4 symmetric-key cipher with key length of 128 bits supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher.

It means 128-bit RC4 encryption is 3 x 10^{26} times stronger than 40-bit RC4 encryption. Different encryption algorithms require variable key lengths to achieve the same level of encryption strength.

RSA Key Generation Algorithm

- Two large prime numbers are considered. Let them be p,q.
- Calculate n = pq and (Ø) phi = (p-1)(q-1).
- Select e, such that 1 < e < phi and gcd(e, phi) = 1.
- Calculate d, the private key, such that de =1 mod phi.

  One key is (n, e) and the other key is (n, d). The values of p, q, and phi should also be kept secret.
- N is known as the *modulus*.

- E is known as the *public key*.
- D is known as the *secret key*.

Encryption

Sender A does the following:-

- Get the recipient B's public key (n, e).
- Identify the plaintext message as a positive integer m.
- Calculate the ciphertext $c = m^{\wedge e} \bmod n$.
- Transmits the ciphertext c to receiver B.

Decryption

Recipient B does the following:-

- Consider his own private key (n, d) to compute the plain text $m = c^{\wedge d} \bmod n$.
- Convert the integer to plain text form.

Digital Signing

Sender A does the following:-

This concept can also be used in digital signing as well. The message to be transmitted is converted to some message digest form. This message digest is converted to encryption form using his private key. This encrypted message digest is transmitted to receiver.

Signature Verification

Recipient B does the following:-

Using the sender's public key, the received message digest is decrypted. From the received message, the receiver independently computes the message digest of the information that has been signed.

If both message digests are identical, the signature is valid. Compared with symmetric-key encryption, public-key encryption provides authentication & security to the data transmitted but requires more computation and is therefore not always appropriate for large amounts of data.

PROBABILISTIC ENCRYPTION SCHEMES

In public key encryption there is always a possibility of some information being leaked out. Because a crypto analyst can always encrypt random messages with a public key, he can get some information. Not a whole of information is to be gained here, but there are potential problems with allowing a crypto analyst to encrypt random messages with public key. Some information is leaked out every time to the crypto analyst, he encrypts a message.

With probabilistic encryption algorithms a crypto analyst can no longer encrypt random plain texts looking for

correct cipher text. Since multiple cipher texts will be developed for one plain text, even if he decrypts the message to plain text, he does not know how far he had guessed the message correctly. To illustrate, assume a crypto analyst has a certain cipher text ci. Even if he guesses message correctly, when he encrypts message the result will be completely different cj. He cannot compare ci and cj and so cannot know that he has guessed the message correctly. Under this scheme, different cipher texts will be formed for one plain text. Also the cipher text will always be larger than plain text. This develops the concept of multiple cipher texts for one plain text. This concept makes crypto analysis difficult to apply on plain text and cipher text pairs.

An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. The encryption key relates encryptions to the decryption key. The key generator is considered to be a probabilistic algorithm, which prevents an adversary from simply running the key generator to get the decryption key for an intercepted message. The following concept is crucial to probabilistic cryptography

KEY DISTRIBUTION MECHANISM

In most of the schemes, a key distribution centre (KDC) is employed which handles the task of key distribution for the participating parties. Generally two mechanisms are employed.

In the first mechanism user A, requests KDC for a session with another user say, B. Initially the KDC sends session key encrypted with private key of A, to the user A. This encrypted session key is appended with encrypted session key by private key of B. On receiving this User A, gets session key and encrypted message with private key of B. This encrypted message is sent to B, where B decrypts it and gets the session key. Now both A & B are in hold of session key which they can use for secured transmission of data. Other wise it is the KDC which sends encrypted session key to the participating parties based on the request of user.

In the second mechanism, the scenario assumes that each user shares a unique master key with the key distribution centre. In such a case, the session key is encrypted with the master key and sent to participating parties.

A more flexible scheme, referred to as the control vector [10]. In this scheme, each session key has an associated control vector consisting of a number of fields that specify the uses and restrictions for that session key. The length of the control vector may vary. As a first step, the control vector is passed through a hash function that produces a value which is equal to encryption key length. The hash value is XOR ed with the master key to produce an output that is used as key to encrypt the session key. When the session key is delivered to the user the control vector is delivered in its plain form. The session key can be recovered only by using both master key that the user shares with the KDC and the control vector. Thus the linkage between session key & control vector is maintained. Some times keys get garbled in transmission. Since a garbled key can mean mega bytes of unacceptable cipher text, this sis a problem. All keys should be transmitted with some kind of error detection and correction bits. This is one way errors of key can be easily detected and if required the key can be reset.

CONCLUSIONS

In this work a ternary system with a 3 digit number is used. So the sequence generated is a 27 digit number. By using a n-ary vector, the length of the vector can be further increased. But this does not guarantee in the increase in number of basins formed. The number of values of generated sequence will increase in each basin. Thus the new model provides a new probabilistic substitution mechanism where each character of plain text is replaced by two or three characters of cipher text depending on the chosen key. And also the model develops multiple cipher texts for one plain text. The algorithm provides almost equal security at low computational overhead. And also the given algorithm is free from differential and linear crypto analysis, which makes it suitable in data encryption. The limitation with this algorithm is more data has to be transmitted than the actual data which demands for more band width requirements.

REFERENCES

1. Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult.
2. Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption Scheme, On Line March 2007, www.citeseer.ist.psu.edu.
3. Bluekrypt 2009: Cryptographic Key length Recommendations, http://www.keylength.com
4. Blum L., Blum M, Shub M.: A simple unpredictable pseudo random number generator.
5. Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
6. Sage.math.Washington.edu/home/jetchev/Public.html/docs/jetchev-talk.ppt- Broadcast encryption schemes.
7. 7. Brassard G.: Modern Cryptology, a tutorial lecture Notes on computer science, (325) ,(spring-verlas) .
8. Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.
9. Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non Specialists, EURASIP Journal, Vol 07, Article 10.
10. Donavan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations & Management, IEEE Symposium 2008, PP 787-790.
11. Dorothy E. Denning et al.: Time Stamps in Key Distribution Protocol, Communication of ACM, Vol 24, Issue 8, Aug 1981, pp 533-536.
12. E.C.Park, I.F.Blake: Reducing communication overhead of Key Distribution Schemes for Wireless Sensor Networks: Computer Communications & Networks, ICCCN 2007, pp 1345-1350.
13. Georg J.Fuchsbauer: An Introduction to Probabilistic Encryption, 'Osjecki Matematicki List 6(2006), pp37-44.
14. Guo D, Cheng L.M., Cheng L.L: A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks, Applied Intelligence, Vol 10, No.1, Jan 99, pp 71-84.

15. Hamid Mirvazri, Kashmiran Jumari Mahamod Ismail, Zurina Mohd. Hanapi: Message based Random Variable Length Key Encryption Algorithm, Journal of Computer Science, pp 573-578, 2009.

16. Hianyi Hu, Gufen Znu, Guanning Xu: Secret Scheme for Online Banking based on Secret key Encryption, Second International Workshop on Knowledge Discovery & Data Mining, Jan 23-25 2009.