Analytical Study on Cryptographic Techniques and its Loopholes

Annu Mishra
Department of Computer Engineering
JIMS, Affiliated to IP University, New Delhi, India

Abstract— Cryptography is a technique used from decades to secure and protect the information and send the data from one place to another without the fear of having been read out by some unauthorized and unauthenticated means. Several ways has been developed in this field to make the information more secure and avoid trespassing. However these methods may have some loopholes or shortcoming which leads to the leakage of information and thus raising a question of information security. The cryptographic technique is used not only to provide the security but also it deals with data integrity, confidentiality and non-repudiation issues. In this paper I have discussed various cryptographic techniques and the limitations of those techniques as well. Some cryptographic algorithms are briefly described and their impact on the information is also mentioned.

Key words: Cryptography, Information Security, Encryption, Decryption, Symmetric Cryptography, Asymmetric Cryptography Private Key, Public Key

I. INTRODUCTION

Cryptography is a method to secure the original information or what we call as the plaintext so that it can be sends through the network without having the fear of being gained by someone else who is not the intended recipient. Data exchange is used in many fields like military, banking, government projects, corporate transactions etc. Apart from securing this information, the objective of cryptography includes data integrity, non-repudiation and authentication. There are several ways to encrypt the data using various algorithms. Every day number of ways are being developed and tested to convert the plaintext into the encrypted one. The use of algorithm highly depends on type of information, sender and the receiver and medium of transfer. In some cases the crypt algorithm is highly complex whereas in some cases simple methods can be suggested. Various techniques to secure the information are discussed in this paper along with their pitfalls too. It is very hard to say that any particular technique is free of flaws as even the best algorithm has certain flaws in it. The cryptographic algorithm is used as a weapon against the eavesdropping in present world. The World Wide Web and the Mobile Networking are growing voluminously and thus securing the data over these large networks becomes very important. The major concept associated with cryptography is Encryption which means to hide the actual information or to make it unreadable into some format and the second term associated in parallel is Decryption which means to unhide the data. The symmetric and asymmetric cryptography techniques used since several decades has been now improvised and made stronger than before. Both the techniques are discussed in the next section.

II. SYMMETRIC CRYPTOGRAPHY TECHNIQUES

The symmetric techniques are those methods in which a single key is used to encrypt and decrypt the data and this secret key is shared among the sender and receiver in advance before transferring the data. We call this key as Private Key.

There are four general categories of Symmetric Cryptography

- Ceaser Cipher
- Playfair
- Monoalphabetic
- Polyalphabetic
- Deffie Hellman Key Exchange Technique

A. Ceaser Cipher Technique

This method is one of the simplest and oldest methods of substitution. The idea is to substitute each letter of the plaintext with 3 letters ahead of it.

For e.g.:

- Plain: abcdefghijklmnopqrstuvwxyz
- Key: defghijklmnopqrstuvwxyzabc
- Plaintext: let me send you message
- Cipher text: ohw ph vhqg brx phvvdjh
- Loophole: In this method is that every letter has a fixed substitution and thus it is very easy to guess the key.

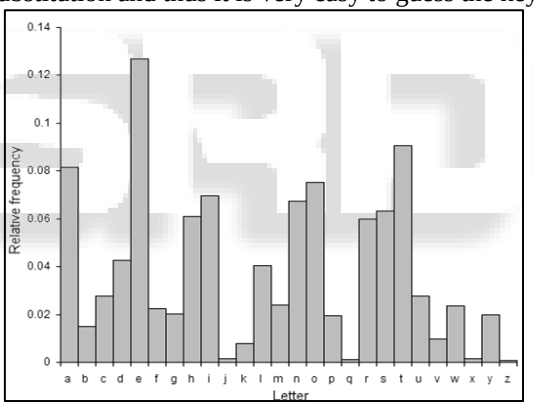

Fig. 1: Distribution of English alphabets and their frequency of occurrence.

The distribution of the letters in a typical sample of English language has a predictable and distinctive shape. A Caesar shift "rotates" this distribution of alphabets, and it is possible to determine the shift by observing the resultant frequency graph and hence determine the text easily.

B. Playfair Technique

Developed by Charles Wheatstone, this method proved to be one of the best known techniques of that time during the World War II. The steps involved are:

1) Choose the Keyword

a) Rules

- No repetition of letters

2) Create Table

a) Rules

- Create a 5×5 matrix and insert the key into it and fill the remaining cell by other alphabets.
- Letter ‘j’ not to be included in the matrix

3) Plaintext

a) Rules

- Split the text into pairs
- If the plaintext is of odd length then make it even by appending letter 'x' in the end string
- Replace the repeating letters with letter 'x'.

4) Insert the pairs into the matrix separately

a) Rules

- If both the letters are in same column then move each of them one letter down and if we reach the table end then wrap around
- If both the letters are in same row then move each of them one letter right and if we reach the table end then wrap around
- If the letter forms a rectangle then swap it with the letter present at the end of the rectangle.

5) Example

Let us encrypt the plaintext "memory" and let us choose key as "security". Now we build a 5×5 matrix as

s	e	c	u	r
i	t	y	a	b
d	f	g	h	k
l	m	n	o	p
q	v	w	x	z

Table 1: 5×5 Matrix with Keyword "Security"

Now the plaintext "memory" can be break down into pair of letters as: me, xo, ry. The pair "me" is in same column, so we can move one letter down and thus we get "vt". Similarly "xo" are also in same column so we get "ux" and for the pair "ry" we get "ca". Thus, finally we get "vtuxca" as cipher text for the plaintext "memory".

a) Loophole

The letters changes itself but their frequency does not change. Thus the attacker may easily obtain the plaintext from the frequency analysis table. Another limitation of this method is that it has a five cross five matrix that can store on 25 uppercase characters or 25 lowercase characters due to which it is unable to store both uppercase and lowercase characters together in a single matrix. Apart from this, the whitespaces and other different characters are not possible to be stored.

C. Monoalphabetic Technique

This is another type of Symmetric Technique in which the letters are replaced by fixed alternates. One of the oldest monoalphabetic techniques is the ATBASH Technique in which the first alphabet is replaced by the last letter of the alphabet order.

For e.g.:

- Plain: abcdefghijklmnopqrstuvwxyz
- Key: zyxwvutsrqponmlkjihgfedcba
- Plaintext: let me send you message
- Cipher text: ovg nv kvmw blf nvhhztv
- Loophole: Anyone can easily identify the letters as it is simply based on ascending and descending order of alphabets. Thus even the immature in the field of cryptography can easily identify the pattern and thus the information may get revealed.

D. Polyalphabetic Technique

This method is way better than the monoalphabetic substitution technique as it works on the concept that the same alphabet can be altered with different alphabets. One of the oldest methods of this kind is ALBERTI Cipher. Alberti formed two rings the outer ring and the inner ring.

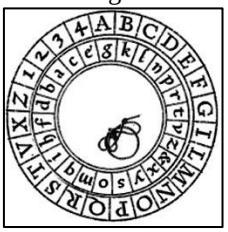

Fig. 2: Alberti formed two rings

The outer ring refers to the letters of the plaintext and the inner circle refers to the letters to be substituted. After certain conversions the inner ring is rotated and thus the corresponding substitution changes.

1) Loophole

The loophole of the Alberti Cipher the repeating key. If an expert cryptanalyst could find out the length of the key, he can treat the cipher text as a number of interwoven Caesar Ciphers, which can all individually be broken. Both Kasiski and Friedman have developed a mathematical test to determine the length of the key. A weakness of Alberti Cipher is that somehow the shifts in alphabets are necessary to be communicated to the recipient. Therefore, to enable it an index letter is chosen on the inner ring that indicates on the outer ring referring which position it corresponded to. This corresponding present in outer capital letter is then inserted in the cipher text at the position where the shift happens. The result of this is a cipher text that is primarily written in lowercase, but occasionally at some places contains an uppercase letter too. For someone unfamiliar to the Alberti cipher and trying to break the code, this cipher text would be very hard to break. However, if the code breaker is aware of the method of the Alberti cipher, it would very obvious to recognize the pattern, and therefore extremely easy and simple to break.

E. Deffie Hellman Key Exchange Technique

This technique was developed by Whitfield Deffie and Martin Hellman to exchange the keys. The technique is used for key exchange among the sender and receiver. The idea is to share the keys generated by each end via the open network available without the threat that the keys will be read or recognized by some third party who is unauthorized or unauthenticated. The basic principle is described below:

- Let us assume person Mark, who chooses two prime numbers. Let the prime numbers be g and p. After choosing the numbers, Mark announces the numbers to the John and both agrees upon the number g and p.
- John, then picks a secret number a. This number is remembered by the receiver and it does not even write the number anywhere else and then compute A=g^a mod p. Similarly Mark picks a secret number say b and computes B=g^b mod p. The previously announced numbers g and p remains same for the computation on both the ends because they have previously agreed upon the keys.
- Now both the sender and receiver send the public key generated by them to each other via an open channel.
- After receiving the public key from each other the two parties then calculates number X.

Mark calculates X by using its personal key as A^b mod p which means (g^a) ^b mod p and John calculates B^a

mod p which means (g^b) ^a mod p. We can see that both Mark and John can now calculate the same number X without knowing each other's personal and the major advantage is that this number X is not transmitted via the communication channel.

a) Loophole

The major limitation of Deffie Hellman is that it lacks the authentication issue within it. The "man in middle" attack is one of the most common problems associated with it.

III. Asymmetric Cryptography Techniques

The asymmetric technique also known as public key cryptography, involves two keys which are known as private and the public key. The sender encrypts the source information using the public key of the recipient and sends it through the network. The receiver on the other hand decrypts the information using its private key. There are several methods of Asymmetric Cryptography. These are:

- RSA
- ElGamal public key cryptosystem

A. RSA Cryptography

Named after Ron Rivest, Adi Shamir, and Leonard Adleman, this is a very strong way of encrypting the information. As in asymmetric technique, this method uses two keys for encryption and decryption each. The method is discussed below:

1) Method of generating public-key

- Select two prime numbers P and Q
- Multiply n = P*Q
- Select e such that 1<e<θ (n) where θ(n) = (P-1)*(Q-1)
- Now Public key is made up of n and e

2) Method of generating private-key

- Calculate θ (n) = (P-1)*(Q-1)
- Calculate D = (k* θ (n) + 1)/e for some integer k

Now let us encrypt and decrypt message using these keys

a) Plaintext: HE

Generating public-key:

Let P=53 and Q=59

n = 53*59 = 3127

Let e = 3

b) Cipher text: HE

Cipher text: HE is changed into number form as H=8, E=5

Thus Cipher text C = 85^3 mod 3127 = 614125 mod 3127=1233

Now the receiver decrypts the cipher text using its own private key D which can be calculated as D = (k* θ (n) +1)/e for let say k=2.

Thus, D= (2*3016+1)/3 = 2012. So using this key we can now decrypt the data as 1233^2012 mod 3127

This gives the result as 85 which when converted to English alphabet gives HE as our plaintext.

3) Loophole

The idea behind RSA is that it is difficult to factorize the large integers. However both public and private keys are derived from the large prime number that we choose. Thus strength of encryption is directly proportional to length of the prime number that we choose. So, if someone enables to factorize large number can easily find out both the keys very easily. Typically the RSA uses the key of length 1024 bits or 2048 bits long. However 2048 bit length is preferred over 1024 bit length as the complexity to find the key increases exponentially. Another limitation of RSA is that its speed is too slow. The RSA encryption and decryption algorithm need number of calculation and thus the speed becomes slow when compared to the symmetric cryptographic algorithm. With the increase in the key length to ensure safety, the computation also becomes greater and the speed becomes slower.

B. Elgamal Public Key Cryptosystem

ElGamal is one of the oldest asymmetric cryptography. Its difficulty depends upon computing discrete logarithms of large prime numbers. To understand the algorithm let us suppose a scenario that Mark begins by publishing the information which consists of a public key and an algorithm. Mark picks

- A large prime number says p_A of 200 to 300 digits,
- And a primitive element α_A modulo p_A
- A (possibly random) integer d_A where 2≤d_A≤p_A –2. Mark then computes
- β_A≡α_A^d_A (mod p_A).

Mark's public key is (p_A, α_A, β_A). His private key is d_A.

John on the other hand encrypts a short message (short as this method is unsuitable for long messages to be transferred) say SM (SM <p_A) and sends it to Mark in this way:

- John picks a random integer I (which he does not share with anyone).
- John then computes R≡α_A^I (mod p_A) and T ≡β_A^I SM (mod p_A), and then discards I.

After the computation, John sends his encrypted message (R, T) to Mark. Now when Mark receives the encrypted message (R, T) from John, he decrypts the message using his private key d_A by computing T*R^-d_A. Now even if some unauthenticated or the unauthorized means wants to read the cipher text (R, T), it cannot perform the desired calculation because it is unaware of d_A. However if the attacker somehow gets to know d_A, still it is very difficult to find the discrete logarithm of a large number consisting of 200 to 300 digits.

1) Loophole

ElGamal Cryptography has the disadvantage that the cipher text is twice as long as the plaintext. Thus it is preferable to be used for short messages instead of long messages. Another loophole associated with the method is its slow speed. Due to very large and complex calculations, the speed of this technique is quite slow. Thus it cannot be recommended for those crucial messages that need to be delivered on time.

IV. Conclusion

Cryptography is a tool which makes out data transmission secure and apart from this it also provides data integrity, non-repudiation and confidentiality. Out of symmetric and asymmetric key cryptography, the public key cryptography or the asymmetric cryptography has become an indispensable component for our global digital communication network. These networks support a many basic communities like mobile phones, internet, social networks, and cloud computing and distributed resources. There are number of cryptography techniques in practice now a days and each of them is overwhelmed with lots of functionalities and

technical complexities which makes it hard for the attacker or the hacker to obtain the original data that is being transmitted via the open network system available. However with almost every technique there is some loophole associated which makes the technique weak at some point. The solution to overcome this issue can be either of the two ways: One way may be to find the loophole of each and every technique and then work on it to make it more secure and restricted. On the other hand, the solution is that we come up with more and more number of strong and secure cryptographic techniques so as to transfer the data fearlessly through the network available.

REFERENCES

[1] Menezes AJ, Oorschot PCV and Vanstone SA, Handbook of applied cryptography. Boca Raton, Florida, USA: CRC Press; 1997.
[2] B. A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.
[3] Coron, J. S., "What is cryptography?" IEEE Security & Privacy Journal, 12(8), 2006, pp. 70-73.
[4] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126.
[5] Wei, X., Z. Li and Y. Zhu, 2011. On the RSA algorithm and application. J. Honghe Univ., 4: 31-32.
[6] Hershey, J. E. Cryptography Demystified. New York: McGraw-Hill, pp. 162-166, 2003.
[7] Diffie, W. and Hellman, M. "New Directions in Cryptography." IEEE Trans. Info. Th. 22, 644-654, 1976.
[8] C .Shannon,. "Communication Theory of Secrecy Systems ". Bell Syst, (1949), Tech. J., Vol (28), pp: 656-715.
[9] H.Kenneth, "Elementary Number Theory and Its Applications "Third Edition. Addison-Wesley,(1992): Germany
[10] R. Rivest. The MD4 message digest algorithm. In Proceedings of Crypto '90, volume 537 of LNCS. Springer-Verlag, 1990.
[11] S. Murdoch. Hot or not: Revealing hidden services by their clock skew. In Proceedings of the 13th ACM Conference on Computer and Communications Security, pages 28–36, 2006.
[12] V. Gligor and P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In Proceedings of fast software encryption (FSE) '01, volume 2355 of LNCS, pages 92–108. Springer-Verlag, 2001.

