ISSN 2250-0987
Varsha sahni et al, UNIASCIT, Vol 2 (2), 2012, 225-228

ENCRYPTION TECHNIQUES OF CRYPTOGRAPHY

[1]Varsha sahni, [2] Jaspreet kaur , [3]Deepshikha atwal ,[4]Indu Aeri
Assistant. Professor
CT institute of engineering and technology

***Abstract*-- In cryptography, encryption is the process of transforming information referred to as plaintext using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption (i.e., to make it unencrypted).**

***Keywords*--** Cipher, encryption, symmetric key, security, mono, poly, substitution, public

I. INTRODUCTION

When we use the Internet, we're not always just clicking around and passively taking in information, such as reading news articles or blog posts -- a great deal of our time online involves sending others our own information. Ordering something over the Internet, whether it's a book, a CD or anything else from an online vendor, or signing up for an online account, requires entering in a good deal of sensitive personal information. A typical transaction might include not only our names, e-mail addresses and physical address and phone number, but also passwords and personal identification numbers (PINs).

The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way we live and work. It's extremely easy to buy and sell goods all over the world while sitting in front of a laptop. But security is a major concern on the Internet, especially when you're using it to send sensitive information between parties.

there's a whole lot of information that we don't want other people to see, such as:

- Credit-card information
- Social Security numbers
- Private correspondence
- Personal details
- Sensitive company information
- Bank-account information

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. But the most popular forms of security all rely on **encryption**, the process of encoding information in such a way that only the person (or computer) with the **key** can decode it[1].

II. HISTORY OF ENCRYPTION

In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures.
Ancient Babylonian merchants used *intaglio*, a piece of flat stone carved into a collage of images and some writing to identify themselves in trading transactions. Using this mechanism, they are producing what today we know as 'digital signature.' The public knew that a particular 'signature' belonged to this trader, but only he had the intaglio to produce that signature.

Of course, technology today has evolved at such rapid pace that the need to protect information grows with the lessening reliability of older encryption techniques. Basic modern encryption is not much different from the ancient civilizations' substitution using symbols. Translation table, lends itself very well in making a piece of data generally unreadable. However computers today are much too advanced that translation table is easily broken and thus no longer viable. Instead encryption today has grown into such specialized field that involve mathematical, non-linear cryptosystem that even a relatively powerful computers take months or even years to break the ciphertext.

III. ENCRYPTION TECHNIQUES

Data encryption systems generally belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

A. Symmetric Key

In **symmetric-key encryption**, each computer has a secret key (code) that it can use to encrypt a packet of

information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message[2].

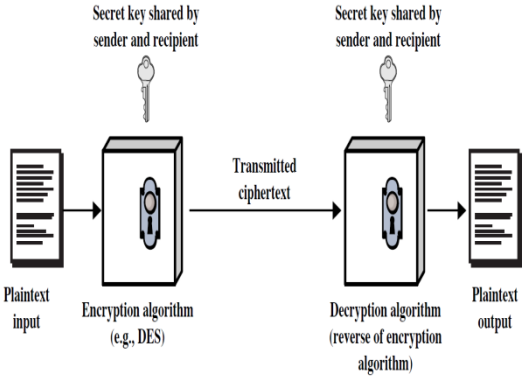

Fig1 symmetric key encryption technique

Symmetric key encryption uses same key, called secret key, for both encryption and decryption. Users exchanging data keep this key to themselves. Message encrypted with a secret key can be decrypted only with the same secret key.

The algorithm used for symmetric key encryption is called secret-key algorithm. Since secret-key algorithms are mostly used for encrypting the content of the message they are also called content-encryption algorithms.

The major vulnerability of secret-key algorithm is the need for sharing the secret-key. One way of solving this is by deriving the same secret key at both ends from a user supplied text string (password) and the algorithm used for this is called password-based encryption algorithm. Another solution is to securely send the secret-key from one end to other end. This is done using another class of encryption called asymmetric algorithm, which is discussed later.

Strength of the symmetric key encryption depends on the size of the key used. For the same algorithm, encrypting using longer key is tougher to break than the one done using smaller key. Strength of the key is not liner with the length of the key but doubles with each additional bit.

1. *Advantages of symmetric key encryption :*
   - The encryption process is simple
   - each trading partner can use the same publicly known encryption algorithm - no need to develop and exchange secret algorithms
   - security is dependent on the length of the key
2. *Drawbacks of Symmetric Encryption*
   - A shared secret key must be agreed upon by both parties
   - if a user has n trading partners, then n secret keys must be maintained, one for each trading partner
   - Authenticity of origin or receipt cannot be proved because the secret key is shared
   - Management of the symmetric keys becomes problematic
3. *Symmetric encryption vulnerabilities*

   - **Breaking symmetric encryption**

   There are two methods of breaking symmetric encryption - brute force and cryptanalysis. Brute Force Attack is a form of attack in which each possibility is tried until success is obtained[3]. Typically, a cipher text is deciphered under different keys until plaintext is recognized. No encryption software that is entirely safe from the brute force method, but if the number of possible keys is high enough, it can make a program astronomically difficult to crack using brute force. But the more bits in a key, the more secure it is, so choose software with as many bits as possible.
   Cryptanalysis is a form of attack that attacks the characteristics of the algorithm to deduce a specific plaintext or the key used.

   - **Weak passwords**
     In every kind of encryption software, there is some kind of password that must be created so that the recipients of the information can read it. Creating a strong password that cannot be easily guessed is just as important as choosing a good algorithm or strong encryption software.
   - Remembering passwords
     If you forget your password, you will not be able to decrypt data that you have encrypted. Be sure to make a backup copy of your password and store it in a safe place.
   - Secret keys exchanging and storing
     Symmetric key encryption algorithms require sharing the secret key - both the sender and the receiver need the same key to encrypt or decrypt data. Anyone who knows the secret key can decrypt the message. So it is essential that the sender and receiver have a way to exchange secret keys in a secure manner. The weakness of symmetric encryption algorithms is that if the secret key is discovered, all messages can be decrypted. So, secret key need to be changed on a regular basis and kept secure during distribution and while using.

B. Asymmetric key encryption

Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made public (it can even be sent in mail), called public-key. Hence this is also called Public Key Encryption.

A private key is typically used for encrypting the message-digest; in such an application private-key algorithm is called message-digest encryption algorithm[4]. A public key is typically used for encrypting the secret-key; in such a application private-key algorithm is called key encryption algorithm.

Public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key. The key pair is based on prime numbers (numbers that only have divisors of itself and one, such as 2, 3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys.

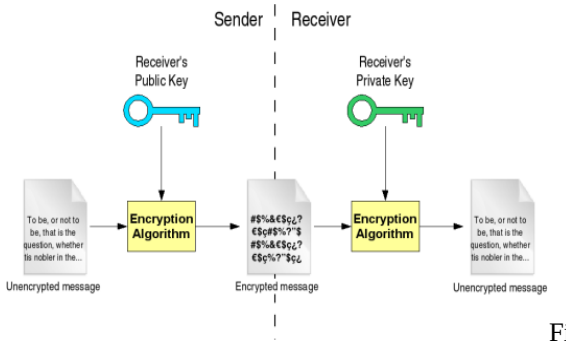

Fig:2

Fig2 asymmetric key encryption technique

1. Advantages of asymmetric key encryption:

Two parties don't need to have already shared their secret in order to communicate using encryption and that both authentication and non-repudiation are possible.

2. Disadvantages of asymmetric algorithms

Complex when compared to symmetric encryption which means that messages take longer to encrypt and decrypt and that you still need to verify the authenticity of the public key, usually via some form of out-of-band communication.

IV. SUBSTITUTION ENCRYPTION TECHNIQUE

A substitution cipher is a method of encryption by which units of plaintext are replaced with ciphertext according to a regular system. the "units" may be single letters pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution[5].

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice-versa.

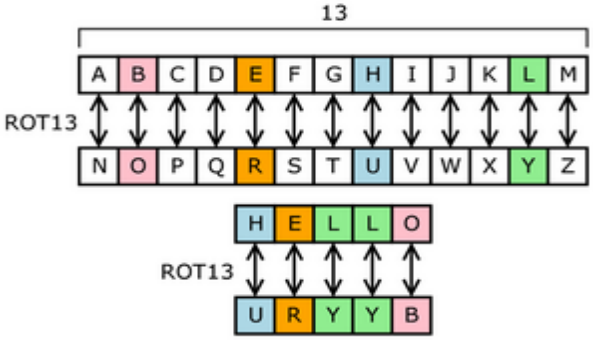

Fig3(a): Monoalphabetic cipher

Message: JAMESBONDNEEDSBACKUP
Code: JEONDAUASNESCPMBDEBK

J	E	O	N	D	A	U
A	S	N	E	S	C	P
M	B	D	E	B	K	

Fig3(b): Transposition cipher

V. DIGITAL SIGNATURES

Integrity is guaranteed in public-key systems by using *digital signatures*. A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation (e.g. through the intervention of a malicious user)

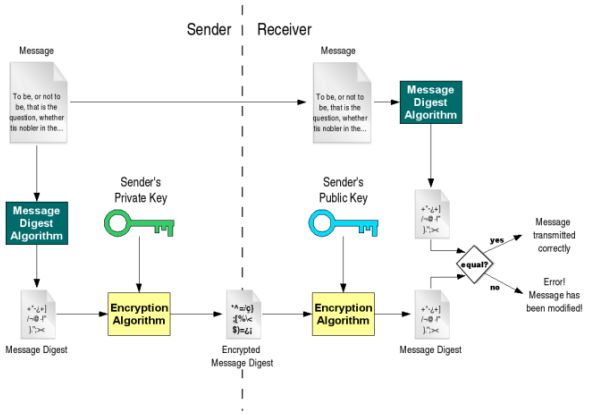

Fig 4.digital signature

The digital signature for a message is generated in two steps:

1. A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: It is always smaller than the message itself and Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.
2. The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*.

The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:

1. Using the sender's public key, decrypts the digital signature to obtain the message digest generated by the sender[6].
2. Uses the same message digest algorithm used by the sender to generate a message digest of the received message.
3. Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver). If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

VI. CONCLUSION

Since data security is of paramount importance to Organizations/Enterprises, they are investing heavily for physical security, information security, etc. Some organizations do not allow taking out of information without prior approvals & security checks. The IT & MIS departments of the organizations have introduced fool-proof systems which prevent taking out of data using floppies or via e-mail. Such organizations have also introduced Internet Sentinels which prevent sending the data via Internal mail as well as preventing attachments for secret artifacts. Sometimes, Organizations / Enterprises need to destroy secret/proprietary information after using it – so that it cannot be used. It is often seen that data stored on hard disks – if deleted can be recovered even after deletion using certain recovery tools. Thus sometimes even the magnetic media has to be destroyed along with the data. This meant physical destruction of data stores which was proving very costly for companies and some other solution better solution was required to allow re-use of data stores. Thus encryption of data proved to be a very strong solution as data may be recovered but only in encrypted form preventing any use.

REFERENCES

[1] Advanced Encryption Standard. National Institute of Standards and Technology, FIPS-197, Nov. 2001.
[2] ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems, first ed. Wiley, Jan. 2001, p. 282.
[3] ANVIN, H. P. SYSLINUX.http://syslinux.zytor.com/.
[4] ARBAUGH, W., FARBER, D., AND SMITH, J. A secure and reliable bootstrap architecture. In Proc. IEEE Symp. on Security and Privacy (May 1997), pp. 65–71.
[5] BAR-LEV, A. Linux, Loop-AES and optional smartcard based disk encryption. http://wiki.tuxonice.net/EncryptedSwapAndRoot, Nov. 2007.
[6] BARRY, P., AND HARTNETT, G. Designing Embedded Networking Applications: Essential Insights for Developers of Intel IXP4XX Network Processor Systems, first ed. Intel Press, May 2005, p.