CRYPTOGRAPHY

Aayushi Jangid

BASICS OF CRYPTOGRAPHY

1.1 INTRODUCTION

In today's world when hacking and computer data robbery and theft are common phenomena, it is very important to protect data and information that is sent over a particular network. And that is where the need for cryptography arises.

Cryptography is the science of writing the data or information in a secret code. It involves encryption and decryption. The data that can be understood without any special efforts is called as the plaintext. This data can be converted into the secret code and this process is called as the encryption. This encrypted data is called as the cipher text. This encrypted text can be converted back into the plaintext by a key and this process is called as the decryption. Thus, cryptography consists of both, the encryption and the decryption process.

1.2 FRIENDS AND ENEMIES IN CRYPTOGRAPHY:

There are three names that are most popular in the cryptographic terms i.e. Bob, Alice and Trudy.

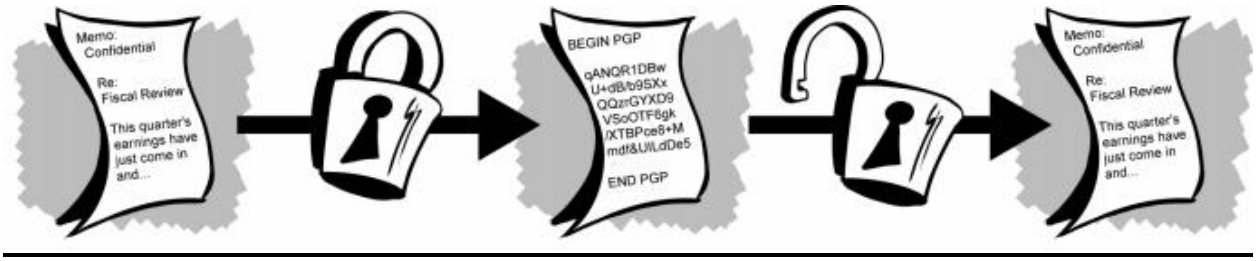
Bob and Alice want to communicate sincerely without any leakage of messages and Trudy might intercept in those messages to harm its contents. These names are very popular in network security world. These Bob and Alice may be web browser or server for electronic transactions, DNS Servers, online banking client/server, routers exchanging routing table updates etc.

1.2 HISTORY OF CRYPTOGRAPHY

It is believed that the first instance of cryptography was seen around 4000 years ago in the Egyptian city of MENET KHUFU where the hieroglyphic inscriptions on the tomb of the nobleman KHNUMHOTEP II were written with a number of unusual symbols to confuse or obscure the meaning of the inscriptions.

One of the other techniques of cryptography, called as substitution cipher in the modern terminology was used by Julius Caesar, however, this technique was first developed by the Greek writer Polybius but its first recorded use was made by Julius Caesar. In this technique, Julius Caesar encoded his messages by substituting the letters in the text by the alphabet that was three letters towards the right.

SCHEMATIC REPRESENTATION OF CRYPTOGRAPHY



Plaintext Encryption Cipher text Decryption Plaintext

3 PURPOSES AND NEED OF CRYPTOGRAPHY:

Cryptography is needed to ensure the confidentiality and authentication of the data passed through any untrusted or unreliable network like the internet. The cryptographic techniques enable a signal to be encrypted so that it can be easily transmitted over any insecure channel like the internet so that it can be read and understood only by the person for whom it is intended.

Cryptography is generally used to ensure the following functionalities:

- It has to ensure the authenticity of the message.
- It provides a mechanism to ensure that the sender has sent a particular message.
- It makes sure that over whichever network does the information passes, only the receiver for whom the message is intended can understand the message, and no one else.

4 WORKING OF CRYPTOGRAPHY:

The cryptographic phenomenon works on the basis of some mathematical algorithms along with a key. This key is being used for encryption as well as for the decryption of the data. The key used for these two processes can be either same or it can be different as well in various different types of cryptography.

5 TYPES OF CRYPTOGRAPHY:

There are primarily three different types of cryptography:

- Public Key Cryptography or Asymmetric Cryptography
- Secret Key Cryptography or Symmetric Cryptography
- Hash Functions.

However, the first two types of cryptography are more important than the hash functions.

5.1 PRIVATE KEY CRYPTOGRAPHY:

In this cryptographic technique, the same key is used for both the encryption as well as the decryption of the messages i.e. Bob and Alice share

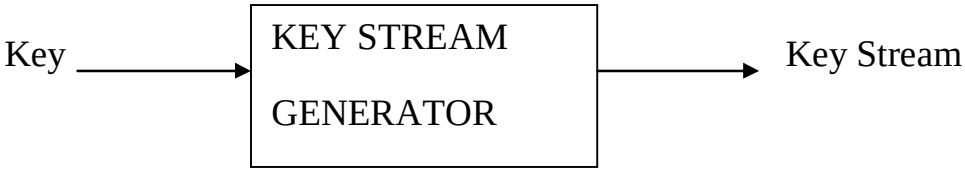
the same key for sending and then receiving the messages by its decryption.

There are two types of symmetric or private key ciphers:

- Stream ciphers
- Block ciphers

The stream ciphers encrypt only one bit at a time. They use the key stream generator and they combine each bit of key stream with each bit of plaintext to get bit of cipher text.

5.1.1 STREAM CIPHERS:



If we assume that
M (i): ith bit of the message
K (i): ith bit of the key stream
C (i): ith bit of the cipher text

Then,

$C(i) = M(i) \oplus K(i)$
$M(i) = C(i) \oplus K(i)$
Where $\oplus$ is the exclusive or operator.

But, there are certain problems with the stream ciphers and these problems include:
[1]. The attacker receives certain amount of the cipher text and he can guess the corresponding plaintext through the exclusive or operator as:
$K = M \oplus C$
$M' = K \oplus C'$
[2]. There is often a large amount of predictable and repetitive data in communication messages.
[3]. The attacker obtains two sequences of cipher texts C and C' generating with the same key sequence as
$C \oplus C' = M \oplus M'$
And there are very well known methods for decryption of those messages whose XOR are given.
[1]. It supports a large amount of integrity problem as well. Suppose the attacker knows C and M and wants to change M to M'. He can very easily do it by calculating
$C' = C \oplus (M \oplus M')$

And then send C' to destination.

Example of the stream cipher is RC4 cipher. RC4 is a popular stream cipher. In this case key can be from 1 to 256 bytes. It is used in WEP for 802.11 and can be used in SSL.

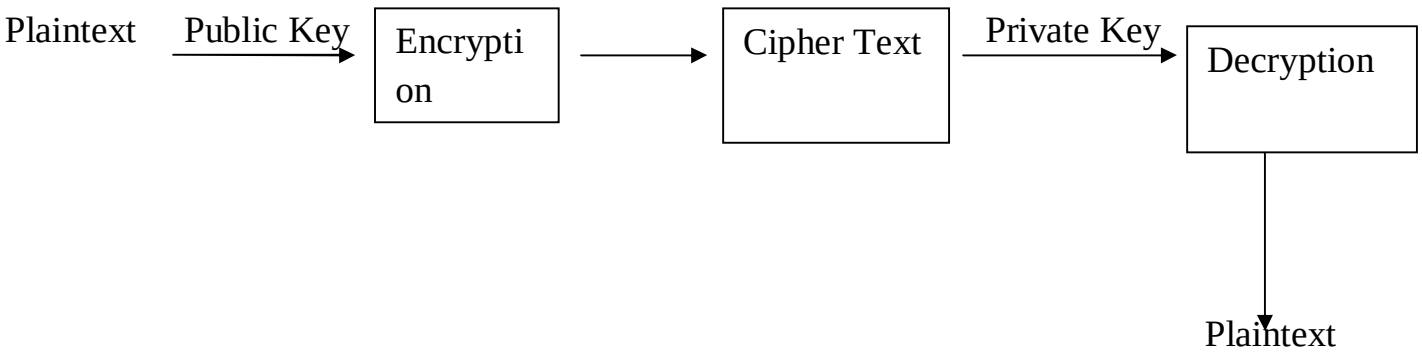
5.1.2 BLOCK CIPHERS:

In the block ciphers, message to be encrypted is processed in block of k bits and 1-to-1 mapping is used to map k-bit block of plaintext to k-bit block of cipher text. In general, about 2k! Mappings are required. But, the problem with this approach is that this requires a table with a lot of entries. But, to solve this we can use a prototype function.

PUBLIC KEY CRYPTOGRAPHY:

In public key cryptography, a pair of different keys is used. One key is called as the public key and is used for encryption of messages i.e. the messages are encrypted using the recipient's public key and the second key is called as the private key and is kept secret. This key is used by the recipient to decrypt the messages.

The keys are related mathematically but it is not practically possible to figure out the private key from the public key.



There are two main techniques for public key cryptography:

[1]. Public key encryption:

In this technique, two keys are used for the purpose of encryption and decryption as described above.

[2]. Digital Signatures:

In this case, a message signed with the sender's private key can be verified by anyone who knows the sender's public key to verify that the sender has actually received that message. This will ensure confidentiality and security.

In general, one of the two algorithms is used for public key cryptography. They are

a) RSA Algorithm
b) Diffie-Hellman Algorithm

5.2.1 RSA ALGORITHM OR RIVEST, SHAMIR, ADELSON ALGORITHM:

Some important things that one needs to know before learning this algorithm is:

[1]. We need a public key K+ and a private key K- for Bob such that

$$K^+(K^-(m)) = m$$

[2]. Given the public key K+ it should be impossible to compute the private key.

[3]. a mod b= remainder of a when divided by b.

and hence by properties,

$$(a \bmod n)^d \bmod n = a^d \bmod n$$

Now, the concept of the RSA Algorithm is as follows:

In the RSA Algorithm, a message is considered as a bit pattern and each of these bit patterns can be uniquely represented by a number.

Thus, encrypting a message is equivalent to encrypting a number.

The algorithm steps are as follows:

[1]. Choose two large prime numbers p and q.

[2]. Compute n=p*q

[3]. Compute z= (p-1) (q-1)

[4]. Choose e with e<n that has no common factors with z.

[5]. Choose d such that ed-1is exactly divisible by z.

[6]. Then, the public key is (n, e) and the private key is (n, d).

RSA Encryption and Decryption:

Given the public and the private keys, the encryption and decryption can be done as follows:

- To encrypt message with m<n, compute
  $c = m^e \bmod n$
- And, to decrypt the received bit pattern, c, we compute
  $m = c^d \bmod n$

The RSA algorithm is secure because factorizing a big number is hard.

5.2.2 DIFFIE-HELLMAN ALGORITHM

The Diffie-Hellman algorithm possesses the following steps:

- Allow two entities to agree on shared key. But does not provide encryption.
- p is a large prime; g is a number less than p. p and g are made public
- Alice and Bob each separately choose 512-bit random numbers, SA and SB that are the private keys.
- Alice and Bob compute public keys:
  $TA = g^{SA} \bmod p$; $TB = g^{SB} \bmod p$;
- Alice and Bob exchange TA and TB in the clear
- Alice computes $(TB)^{SA} \bmod p$
- Bob computes $(TA)^{SB} \bmod p$
- shared secret:
  $S = (TB)^{SA} \bmod p = = g^{SASB} \bmod p = (TA)^{SB} \bmod p$
- Even though Trudy might sniff TB and TA, Trudy cannot easily determine S.
- Problem: Man-in-the-middle attack:

Alice doesn't know for sure that TB came from Bob; may be Trudy instead.

6 APPLICATIONS OF CRYPTOGRAPHY:

The cryptographic systems mainly support those applications in which there are no conceivable law enforcement interests in having access to master keys. For example- ATM, Satellite TV decoders, fire alarm, burglar alarm signaling etc.

The cryptographic techniques have generally nothing to do with the secrecy of the message. Rather, they are mainly concerned with protecting the tampering of data.

The main organization that does this for big companies like Intel, Microsoft etc. is Walt Disney. Walt Disney refuses to release the digital versions of their videos until unless a high level security is provided to them.

Further, the primary and the main purpose of cryptography is network security.

CONCLUSIONS:

Internet security is very important and cryptography is a very important part of it. It is very important to ensure the secrecy of your messages and it can be efficiently done through the use of cryptography. So, in my opinion everybody should have a basic idea of cryptography.

Cryptography is a particularly interesting field because of the reason that it does not involve the secrecy of messages; rather, it involves the security of messages. However, there are many attacks onto the cryptographic algorithms as well but since they are all tested they can be relied upon for protecting the messages.

ACKNOWLEDGMENTS:
I would like to thank my mom-dad, my family and friends (esp. Nupur, Shalini and Dakshi) for supporting me throughout. A special mention to my grandparents Mrs. and Dr.B.P.Jangid and my uncles Mr.Virendra Singh, Dr.B.S.Rathore and Mr. Abdul Kaleem Khan for their constant encouragement throughout.

REFERENCES:

[1]. Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall.
[2]. Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
[3]. Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). Security Requirements for Cryptographic Modules. Gaithersburg, MD: National Institute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[4]. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.
[5]. Schneier, B. (1996). Applied Cryptography, 2nd Ed. New York: John Wiley & Sons.
[6]. Cryptography Research Inc.'s cryptography.com Site
[7]. Crypto Log: The Internet Guide to Cryptography
[8]. RSA's Cryptography FAQ
[9]. Wikipedia pages on cryptography