Introduction to Security
Lecture Dated 27-3-07

Introduction to Cryptography

The few main properties for Cryptography is

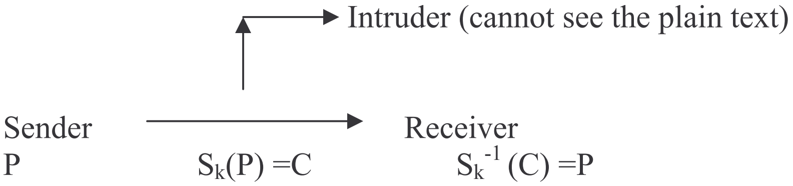
1. Privacy: (Secrecy) :

   No third party should be able to read the message.
2. Authentication (Integrity)

   The third party should not be able to impersonate the message. (write or update the message)
3. Non Repudiation :

   The sender once sends a message cannot deny that he has sent one. Receiver should be able to prove in the court of law that he received the message from a particular sender.

SHARED KEY CRYPTOSYSTEM



Intruder (cannot see the plain text)

Sender Receiver

P $S_k(P) = C$ $S_k^{-1}(C) = P$

P:Plain text
K: Parameter (Key)
C: Cipher Text
S: Encryption algorithm
S^{-1}: Inverse of Encryption Algorithm
$S_k(P) = C$ can also be written as $S(K, P) = C$

The Key for Plain text to Cipher text transformation and for Cipher text to plain text transformation is Same (That is why it is shared Key Cryptosystem)

- This system gives us the privacy.
- The same system can also be used to give Integrity if only a particular sender that this key
- $S(K, P') = C'$ Should be hard to do (That is if intruder chooses P' , It should be hard for him to find C' without knowing K)
- This system does not support non Repudiation.
- Key has to be kept secret

Question: Whether the algorithm should be kept secret or not?
Ans: In military applications algorithm is required to be kept secret.
In commercial application initially the algorithm was kept secret. (GSM kept the algorithm to be secret for long time)
But now it is not so. If algorithm is kept secret in commercial applications then there is possibility of leakage of information through the employees and all. Sometimes it is even possible to guess the algorithm. So the Cryptosystem which depend on the secrecy of the algorithm becomes weak.
System should not depend on the secrecy of key and not of algorithm

CRYPTANALYSIS: (Intruders job)

Generating plain text out of cipher text without knowing the key OR generating the Cipher text out of plain text without knowing the key.

Forms of Cryptanalysis:

1. Cipher Text only attack: In this intruder knows the cipher Text only and try to decipher plain text out of it.
Eg. In Substitution cipher suppose intruder knows that the plain text in English, he can use the frequency count of the alphabets to decipher (fact: certain alphabets are more frequent)

2. Known Plain text attack: In this intruder knows some mapping of the plain text and cipher text. But he doesn't have the choice to which part he knows the mapping.

3. Chosen Plain text attack: In this intruder can choose the plain text and get the cipher text out of it.

4. Chosen Text attack: In this intruder is allowed to choose the cipher text also correspond to which it gets the plain text.

SECURITY GAURANTEES:

1. Unconditional Guarantee: No matter how much time and computer power is provided Intruder won't be able to crack.

Eg. One time pad:

AT the sender:::: M bits of Msg XOR M bits of Key= M bits of Cipher text
At the Receiver:::: M Bits Cipher Text XOR M bits of Key = M bits of plain text

-Key can be use just once

2. Computational guarantee
If infinite time and infinite power is give Intruder may be able to crack. But it may hard to crack with in given time and computational power.

SOME EXAMPLES

How to go about in designing a cryptosystem:

1- Substitution Cipher: Substitute the letter with some other letters
2- Transposition Cipher: Bit position may be transposed
3- Poly alphabetic Cipher: Different portion of message uses different schemes of substitution
4- Codes: substitute words with codes

Codes Vs Ciphers
Codes reduces redundancy so it is harder to crack the code than to crack the cipher

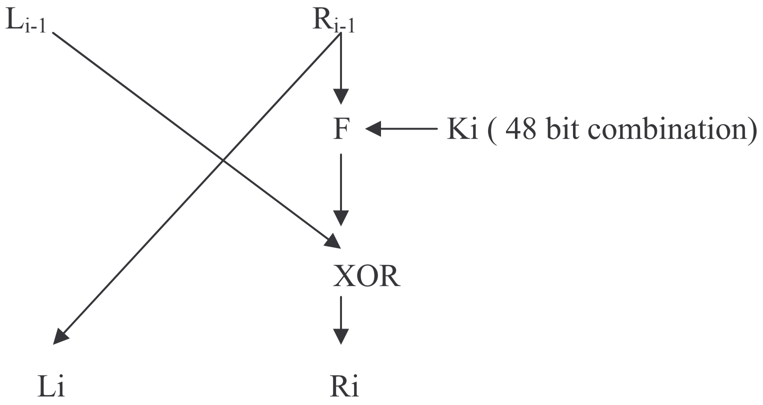
General Cryptosystems use these methods as ingredients. There will be sequence of steps which constitutes the system.

DES (Digital Encryption Standard)

It takes 64 bit plain text, 64 bit key and gives 64 bit cipher text

Step 1. one round of permutation
Step 2 : 16 rounds of identical operation
Step 3 : Reverse permutation

Step 2 operation is as follows



F is the combiner function
It take 32 bit of data and 48 bit of key to give 32 bit , which is then XORed with L_{i-1}

- It is very difficult for the intruder to reverse all steps.
- Can be cracked in 2^55 tries
- 64 bit key had actually 56 bits and 8 bits of parity
- S(P)=C then S(P')= C' (if you invert the bits you get inversion of the cipher)

TRIPLE DES:
In this DES is applied three times. Generally first with key K1 then with key K2 and then again with key K1.

PUBLIC KEY SYSTEMS

- Key is not shared
- Some part of the key is public and some part of the key is private

$$A \longrightarrow B$$

Privacy
- A while sending will encrypt the message with Public key of B S(public key of B,M)
- The decryption will require private key of B

Integrity
- While sending A will encrypt it with the private key of A itself S(private key of A, M)

This also ensures Non repudiation

Public key distribution

Key distribution is Shared key systems is difficult. It is generally done offline. Every pair needs a Secret key.

The public key cryptosystem can be used for distribution of the key. The shared key cryptosystems has less computational overhead than the Public key.

The shared key can be agreed upon any number of times. So there can be different key for different sessions, which again increases the security.

Diffie Hellman Key Excahnge

It has Galois Field which defines it mathematical operations like multiplication exponentiation.

- Fact used: Exponentiation is easy but its reverse is hard
- The α is Galois parameter

A
Selects a random no. X_A
Finds α ^X_A

B
Selects a random number X_B
Finds α ^X_B

Sends α ^ X_A →

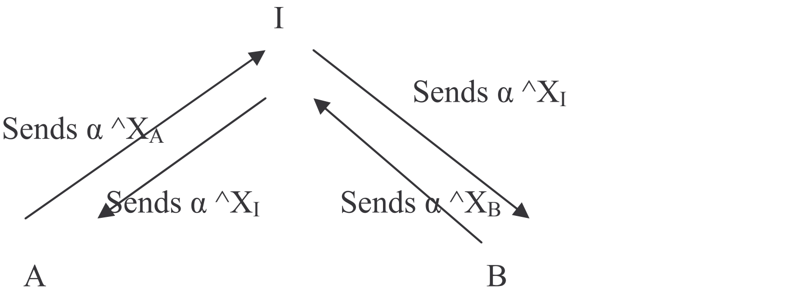
← Sends α ^ X_B

Calculates (α ^ X_B)^ X_A

Calculates (α ^ X_A)^ X_B

And this acts as the secret Key

The problem with Deffie hellman algorithm
Man In the middle Attack



Selects a random no. X_A
Finds α ^ X_A

Selects a random number X_B
Finds α ^ X_B

- Typical example is fake ATMs in the Shopping malls