Introduction to Cryptography

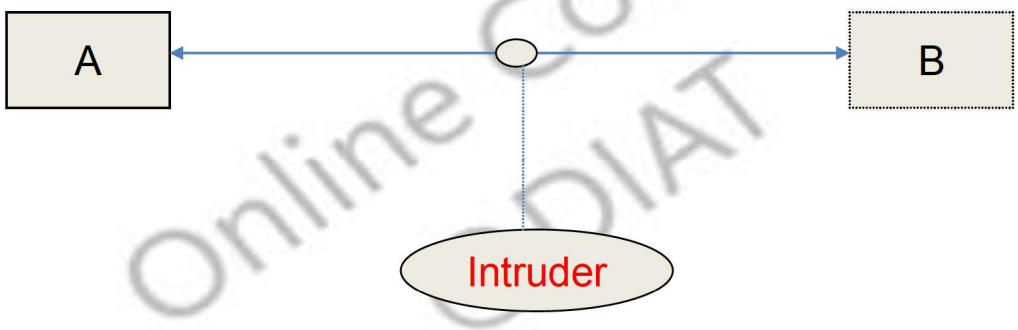
(--Foundation of information security--)

By:
Arun Mishra

Text Book:

- "Cryptography & Network Security" by William Stallings, Pearson Education Asia.
- Kahate A, "Cryptography & Network Security", Tata McGraw Hill, 2004.
- Reference Books
- "Applied Cryptology" by Schiner Bruce, John Wiley & Sons, 2001.
- "Introduction to Cryptography with Coding Theory" by Wade Trappe & Lawrence CWashington, New Jersey, Pearson Education, 2006.
- Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security: PrivateCommunication in a Public World", Prentice Hall of India Private Limited.
- Behrouz A. Forouzan, "Cryptography and Network Security", McGraw Hill

Why study cryptography?



Communications security

Who is the Opponent

- It can be our Computer
- Human
- User Application / System Process/ Program

The General Goals of Cryptography

- We consider the confidentiality goal:
  - Alice and Bob are Friends and wants that only authorized parties (Alice & Bob) are able to understand the data.
  - Eve is a rival
  - Alice wants to send secret messages (M_1,M_2,…) to Bob over the Network
  - Rival Eve wants to read the messages (M_1,M_2,…)
  - Assumption: The network is OPEN: Eve is able to eavesdrop and read all data sent from Alice to Bob.
  - Effect: Alice must not send messages (M_1,M_2,…) directly – they must be "scrambled" or encrypted using a 'secret code' unknown to Eve but known to Bob.

The General Goals ..Contd

- Consider the Integrity goal:
  - Alice may send a message to Bob, this does not need to be encrypted.
  - Eve is a rival
  - Over the Network Any one can examine the message
  - Rival Eve wants to alter the content of message
  - Assumption: The network is OPEN: Eve is able to eavesdrop and read/altered all data sent from Alice to Bob.
- Effect: Alice does not want the contents of the message get changed , the message that arrives is the same as the message that was originally sent.

  - The integrity needs to be preserved. Message must send along with Hash value.

The General Goals ..Contd

- Consider the Availability goal:
  - Alice, authorized party, may create and stored information.
  - Eve is a rival
  - Over the Network Any one can examine the information/message
  - Rival Eve wants to make the information unavailabe.
  - Effect: Information created by authorized party, say Alice, must be accessible to authorized entities only. Access control provides protection against unauthorized assess to information.- Password & Digital Signature

Basic Terms

- Encryption: scrambling a message using a cryptographic algorithm.
- Plaintext: the message before it gets encrypted.
- Ciphertext: scrambled version of the message.
- Cipher: the algorithm involve in scrambling/encryption

Basic Terms (cont.)

- Decryption: the process of converting scramble text back to the original plaintext.
- Cryptanalysis: the science of breaking cryptographic codes/algorithms.
- Cryptanalyst: a person who breaks cryptographic codes; also referred to as “the attacker”.

Classical Ciphers

- Substitution cipher: change each element of the plaintext with another element.
- Transposition (or permutation) cipher: change the order of the elements of the plaintext.
- Product cipher: apply multiple stages of substitutions and transpositions

Types of ciphers

- Private key cryptosystems
  - One secret key is shared between sender and receiver
- Public key cryptosystems
- Sender and receiver can communicate using their public keys

Concepts

- A private key cipher is composed of two algorithms
  - encryption algorithm E
  - decryption algorithm D
- Only one key **K** is used for encryption & decryption
- **K** has to be distributed before the communication

Notations

- Encrypt a plaintext P: required two components a key K & an encryption algorithm E
  C = E(K,P)
- Decrypt a ciphertext C: required the same key K and the decryption algorithm D
  P = D(K,C)

- Note: P = D(K,C) = D(K, E(K,P))

A Simple Example

The plaintext:

1	1	1	0	0	0	1	1	0	1	0	0	0	0	1	0	1	0	0	0	0	1	0

The key:

1	1	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0

The ciphertext:

0	0	1	1	0	0	1	0	0	0	1	1	1	0	0	0	0	1	1	0	1	0	0	1

Example Contd..

ciphertext:

0	0	1	1	0	0	1	0	0	0	1	1	1	0	0	0	0	1	1	0	1	0	0	1

XOR'd with key

1	1	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0

yields plaintext

1	1	1	0	0	0	1	1	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0

Requirements

- Distinguish cryptographic system by:
  - Type of encryption methods used
    - substitution / transposition
  - Number of keys used
    - single-key or private / two-key or public
  - Way in which plaintext is processed
    - Block (typically 64 or 128 bits) / stream (1 bit)

Cryptanalysis

- Goal is to get key not just message
- General approaches:
  - Cryptanalytic attack
  - Brute-force attack

More Definitions

- Unconditional security
  - With unlimited computation power or time, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the plaintext
- Computational security
  - With the available computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

Symmetric-Key Ciphers

Playfair Cipher

- Monoalphabetic cipher: Not Secure
-
- One approach to improving security is to encrypt multiple letters at a time.

- The **Playfair Cipher** is the best known such cipher.

- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

Key Matrix

- Use a 5 x 5 matrix.
- Fill in letters of the key.....without duplicates .
- Fill the rest of matrix with other letters.
- E.g., key = WONDERFUL.

W	O	N	D	E
R	F	U	L	A
B	C	G	H	I/J
K	M	P	Q	S
T	V	X	Y	Z

Encrypting and Decrypting

Plaintext is encrypted two letters at a time.

1. If a pair is a repeated letter, insert filler like 'X'.
2. If both letters fall in the same row, replace each with the letter to its right (circularly).
3. If both letters fall in the same column, replace each with the letter below it (circularly).
4. Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

Security of Playfair Cipher

- A brute force attack on a Playfair..... difficult.
- The size of the key domain is 25! (factorial 25).

Hill Cipher

- Takes m successive plaintext letters and substitutes for them m cipher text letters.
- Uses simple linear equations
- Numbered alphabet: a = 0, b = 1, c = 3, etc.

Hill – key is matrix

$$\begin{matrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{matrix}$$

- Generalize to any size, larger blocks
- Matrix must be invertible

Contd.

- C=(KP)mod 26
- Where C and P are column vectors.
- K is a square matrix (encryption Key)

Strength

- Completely hides single-letter frequencies
- It is strong against a CipherText-only attack

- But.....
- Easily broken with a known PlainText attack

One Time Pad

- Each plain text symbol is encrypted with a random key
- The key has the same length as the plaintext and is chosen completely in random.
- **Challenges**

  There is the practical problem of making large quantities of random keys

  Another problem is key distribution and protection

  Key can be used once

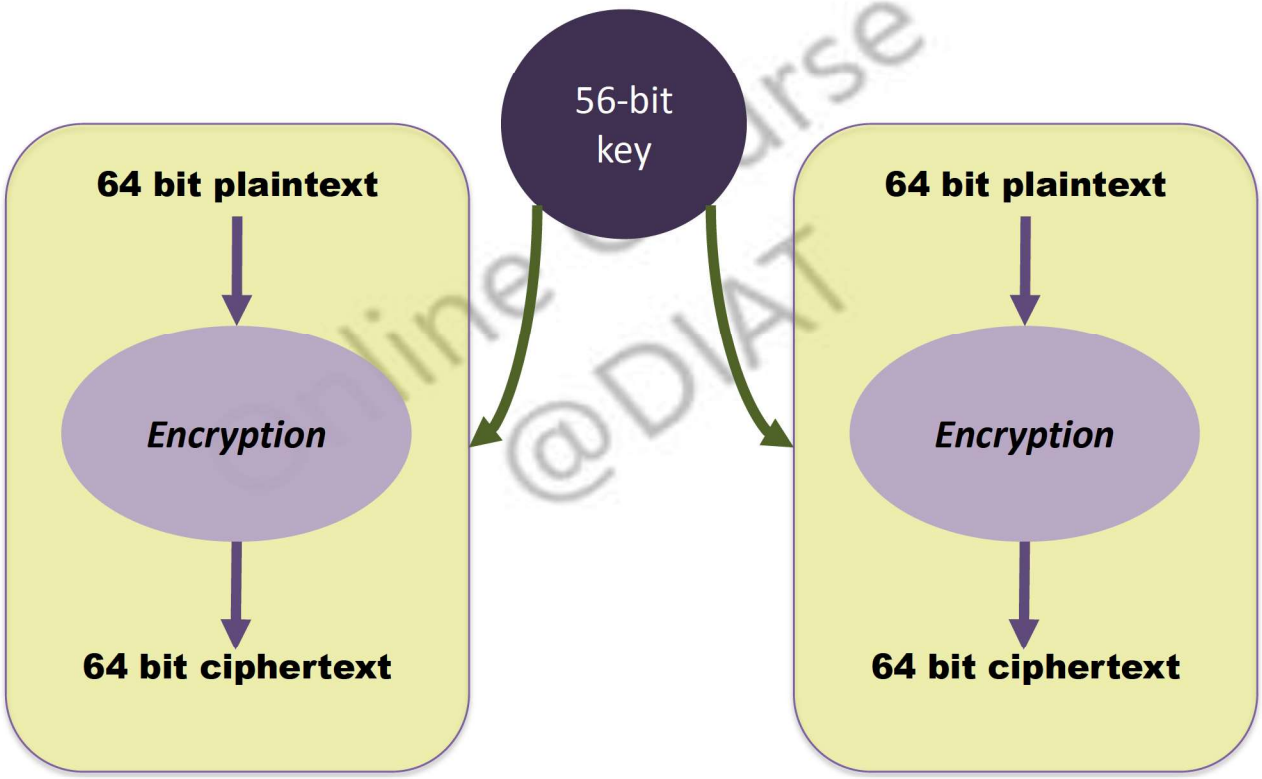
Data Encryption Standard (DES)

Types of Symmetric key Ciphers

- Block Ciphers: Where a block of data is encrypted
- Stream Ciphers: where block size=1

DES is a block cipher, as shown in Figure

Padding bits can be added



Contd..

Most symmetric block ciphers are based on a Feistel Cipher Structure

Claude Shannon and Substitution-Permutation Ciphers

- Shannon introduced idea of substitution-permutation (S-P) networks in 1949
- Form basis of modern block ciphers
- S-P nets are based on the two primitive cryptographic operations:
- Substitution (S-box): may have different number of input and output bits (m*n substitution unit).
- Permutation (P-box): Straight, Compress, Expansion.....invertability
- Provide confusion & diffusion of message & key

Contd..

Ref: https://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/Crypto/slides/DES.pdf

”