Unit-3

Information Security and Cryptography

- Classical Encryption Methods
- Asymmetric Key Cryptography
- Confidentiality, Integrity, Authentication and Non-Repudiation
- Digital Signature

Information security:

- Information security, sometimes shortened to infosec, is the practice of protecting information by reducing information risks.
- It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information.

Cryptography:

- The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.
- Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it.
- Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

Some Basic Terminology Some Basic Terminology

- **Plaintext** - original message.
- **Ciphertext** - coded message.
- **Cipher** - algorithm for transforming plaintext to ciphertext.
- **Key** - info used in cipher known only to sender
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)**- recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)**- study of principles/ methods of deciphering ciphertext without knowing key.
- **Cryptology** - field of both cryptography and cryptanalysis.

Classical Encryption Methods

1. Substitution Method
2. Transposition Method
3. Rotor Machines
4. Steganography

Substitution Method:

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

i. Caesar Cipher:

- This is the earliest known example of a substitution cipher.
- Each character of a message is replaced by a character three position down in the alphabet.
- plaintext: are you ready
- ciphertext: DUH BRX UHDGB

ii. Monoalphabetic and Polyalphabetic Cipher

- **Monoalphabetic cipher** is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.
- In simple words, if the alphabet 'p' in the plain text is replaced by the cipher alphabet 'd'. Then in the entire plain text wherever alphabet 'p' is used, it will be replaced by the alphabet 'd' to form the ciphertext.

- **Polyalphabetic cipher** is far more secure than a monoalphabetic cipher. As monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message.
But polyalphabetic cipher, each time replaces the plain text with the different ciphertext.

iii. Playfair Cipher

- Playfair cipher is a substitution cipher which involves a 5X5 matrix. Let us discuss the technique of this Playfair cipher with the help of an example:
- Plain Text: meet me tomorrow
- Key: KEYWORD
- **Step 1**: Create a 5X5 matrix and place the key in that matrix row-wise from left to right. Then put the remaining alphabets in the blank space.
-

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

- Note: If a key has duplicate alphabets, then fill those alphabets only once in the matrix, and I & J should be kept together in the matrix even though they occur in the given key.
- **Step 2**: Now, you have to break the plain text into a pair of alphabets.
- **Plain Text**: meet me tomorrow
- **Pair**: me et me to mo rx ro wz

Note

- Pair of alphabets must not contain the same letter. In case, pair has the same letter then break it and add 'x' to the previous letter. Like in our example letter 'rr' occurs in pair so, we have broken that pair and added 'x' to the first 'r'.
- In case while making pair, the last pair has only one alphabet left then we add 'z' to that alphabet to form a pair as in our above example, we have added 'z' to 'w' because 'w' was left alone at last.
- If a pair has 'xx' then we break it and add 'z' to the first 'x', i.e. 'xz' and 'x_'.

- **Step** 3: In this step, we will convert plain text into ciphertext. For that, take the first pair of plain text and check for cipher alphabets for the corresponding in the matrix. To find cipher alphabets follow the rules below.

Note

- If both the alphabets of the pair occur in the same row replace them with the alphabet to their immediate right. If an alphabet of the pair occurs at extreme right then replace it with the first element of that row, i.e. the last element of the row in the matrix circularly follows the first element of the same row.
- If the alphabets in the pair occur in the same column, then replace them with the alphabet immediate below them. Here also, the last element of the column circularly follows the first element of the same column.
- If the alphabets in the pair are neither in the same column and nor in the same row, then the alphabet is replaced by the element in its own row and the corresponding column of the other alphabet of the pair.

- Pair: me et me to mo rx ro wz
- Cipher Text: kn ku kn kz ks ta kc yo

iv. Hill Cipher

- Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26 with a scheme A = 0, B = 1, …, Z = 25
- To encrypt a message, column vector n x 1 is multiplied key n × n matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

Example:

- Plain Text: Hello
- Key: four

Step 1: create a matrix based on key $\begin{bmatrix} F & O \\ U & R \end{bmatrix} = \begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix}$

Step 2. Write the plain text as a column vector and write their corresponding number

➔ $\begin{bmatrix} h \\ e \end{bmatrix} \begin{bmatrix} l \\ l \end{bmatrix} \begin{bmatrix} o \\ z \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} \begin{bmatrix} 14 \\ 25 \end{bmatrix}$

Step 3: multiply each column vector with key matrix and find the mod 26 of each element

➔ $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 91 \\ 208 \end{bmatrix} \text{(mod 26)} = \begin{bmatrix} 13 \\ 0 \end{bmatrix}$

➔ $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 209 \\ 407 \end{bmatrix} \text{(mod 26)} = \begin{bmatrix} 1 \\ 17 \end{bmatrix}$

➔ $\begin{bmatrix} 5 & 14 \\ 20 & 17 \end{bmatrix} * \begin{bmatrix} 14 \\ 25 \end{bmatrix} = \begin{bmatrix} 420 \\ 705 \end{bmatrix} \text{(mod 26)} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$

Example

91/26=3.5-3=0.5*26=13

208/26=8-8=0*26=0

Step 4: convert the result column vector to their respective characters

➔ $\begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ a \end{bmatrix}, \begin{bmatrix} 1 \\ 17 \end{bmatrix} = \begin{bmatrix} b \\ r \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{bmatrix} e \\ c \end{bmatrix}$

Cipher Text = NABREC

v. One-time Pad

- One-time Pad (Vernam Cipher) is a method of encrypting alphabetic text
- In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).
  In this algorithm, the length of the should be equal to the length of the plain text.

Example:

Plain text: Are you there
Key this is hello

Step 1: Assign the number for both plaintext and the key

Plain text:	A	R	E	Y	O	U	T	H	E	R	E
	0	17	4	24	14	20	19	7	4	17	4

Key:	T	H	I	S	I	S	H	E	L	L	O
	19	7	8	18	8	18	7	4	11	11	14

Step 2 : Add the number of plain text and number of key.

19 17 12 42 22 38 26 11 15 28 18

Step 3: If the number is greater than or equal to 26 then subtract from 26 and rewrite

19 17 12 16 22 12 0 11 15 2 18

Step 4: Write the alphabets for the corresponding character

T R M Q W M A L P C S

Cipher text= TRMQWMALPCS

2. Transposition Method

- Transposition Ciphers are a bit different to Substitution Ciphers.
- In a Transposition cipher, the letters are just moved around.
- The letters or words of the plaintext are reordered in some way, fixed by a given rule (the key).
- One of the examples for the transposition is given below
  Plain Text: meet me Tomorrow
- The plain text is written in diagonal form as given below

The first row : memtmro
The second row: eteoorw

- Combine first row and second row.
- **Cipher Text**: MEMTMROETEOORW

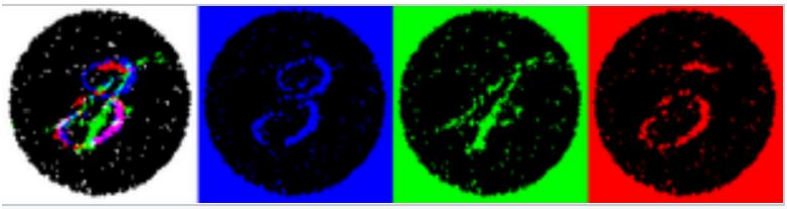
3. Rotor Machines

- Electric rotor machines were mechanical devices that allowed to use encryption algorithms that were much more complex than ciphers, which were used manually.
- They were developed in the middle of the second decade of the 20th century.
- They became one of the most important cryptographic solutions in the world for the next tens of years.
- The main idea that lies behind rotor machines is relatively simple.
- One can imagine a simple device, similar to a typewriter, with a number of keys used to input text produces some random text based on the machine's algorithm.

4. Steganography

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection.
- The secret data is then extracted at its destination.
- The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).
- Since steganography is more of an art than a science, there is no limit to the ways steganography can be used. Below are a few examples:

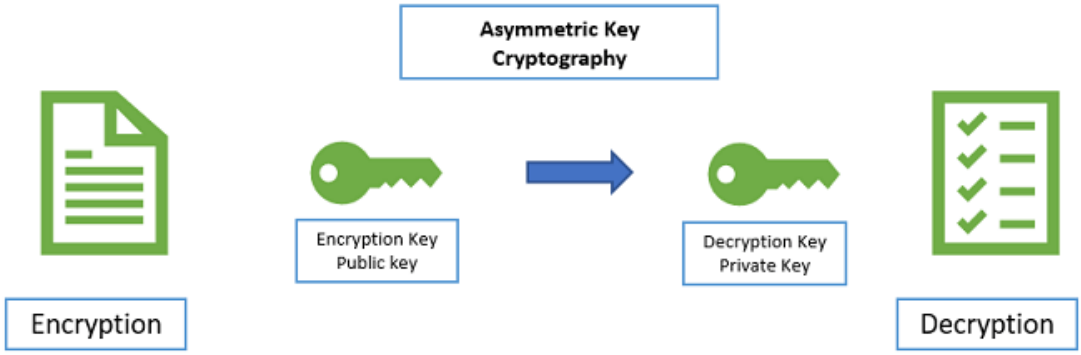
i. Playing an audio track backwards to reveal a secret message
ii. Playing a video at a faster frame rate (FPS) to reveal a hidden image
iii. Embedding a message in the red, green, or blue channel of an RGB image



The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

Asymmetric Key Cryptography:

- Asymmetric Encryption, also known as Public-Key Cryptography is a relatively new concept.
- Unlike “normal” (symmetric) encryption, Asymmetric Encryption encrypts and decrypts the data using two separate yet mathematically connected cryptographic keys.
- These keys are known as a ‘Public Key’ and a ‘Private Key.’
- One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption.
- As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.



Goals of cryptography:

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

Confidentiality

- Confidentiality is most commonly addressed goal.
- The meaning of a message is concealed by encoding it.
- The sender encrypts the message using a cryptographic key.
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender.

Integrity

- Integrity Ensures that the message received is the same as the message that was sent.
- Uses hashing to create a unique message digest from the message that is sent along with the message.
- Recipient uses the same technique to create a second digest from the message to compare to the original one.
- This technique only protects against unintentional alteration of the message.
- A variation is used to create digital signatures to protect against malicious alteration.

Authentication

- Authentication is verifying the identity.
- In other word you prove to the system that you are the person you claim to be by showing some evidence. For example, entering user id and password to login.

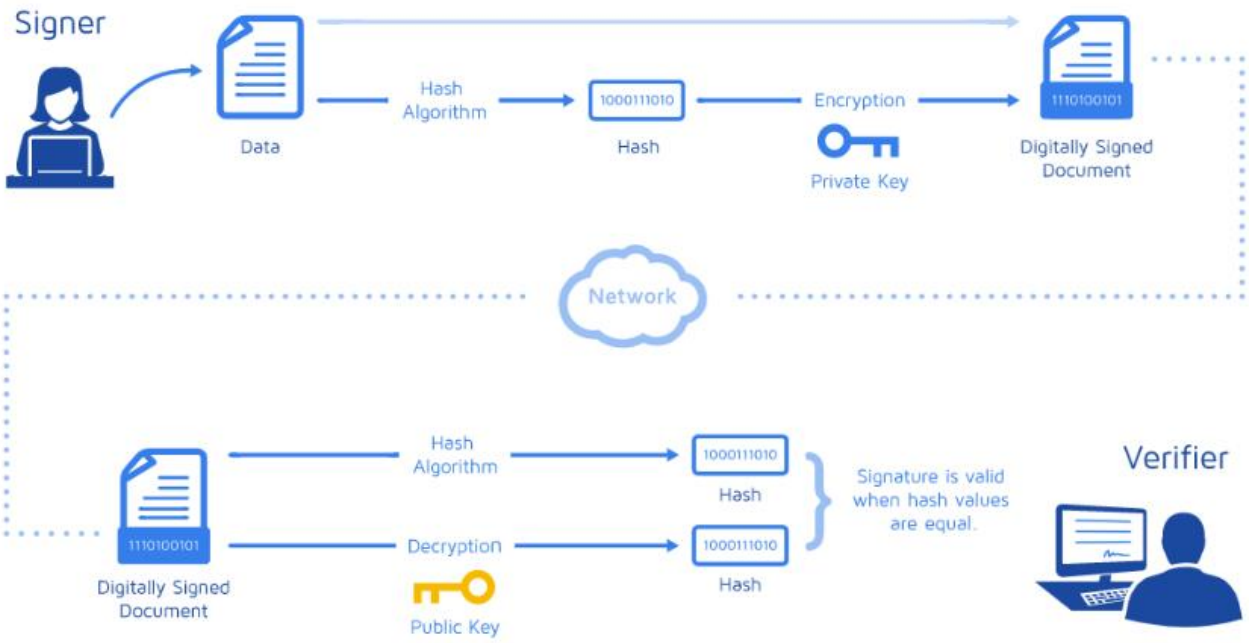
Non-Repudiation

- Nonrepudiation is the assurance that someone cannot deny something.
- Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Digital Signature:

- A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages or electronic documents.
- A signature confirms that the information originated from the signer and has not been altered.
- It provides the highest levels of security and universal acceptance.

Working of Digital Signature



Sender's side

- When the sender electronically signs a document two keys are generated: Public and Private.
- The private key is kept by the signer and it should be kept securely. On the other hand, the receiver must have the public key to decrypt the message.
- Then the Hash function is used on the document to create Hash, which is also known as digest.
- Then the private key is used to encrypt hash.
- The document is sent to the recipients along with the sender's public key.

Receiver's side

- The recipient receives the document and decrypts the encrypted hash with the sender's public key certificate.
- A cryptographic hash is again generated on the recipient's end using the same hash function that the sender used.
- Both cryptographic hashes(of sender and receiver) are compared to check its authenticity.
- If they match, the document hasn't been tampered with and is considered valid.