Cryptography
Cryptography

- The pre-fix "crypt" means that "hidden" and therefore the suffix "graphy" stands for "writing."

- A cryptology algorithmic rule is employed to write in code a message change from plaintext to ciphertext. And then decode the message change from ciphertext back to plaintext.

- Two forms of cryptology algorithms

  1. Symmetric
  2. Asymmetric
Components Of Cryptography

Plaintext.: It is the data to be protected during transmission.

Ciphertext: Encrypted or encoded information.

Key: It is referred as a number on which the algorithm is based upon.

Encryption Algorithm: It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

Decryption Algorithm: The process of turning ciphertext into readable plaintext. It requires decryption key.

Digital signature: The concept of Digital signature lies in authenticating the identity of the sender of a message. It is a verifying process of the sender's identity.
Features of Cryptography

Confidentiality:
Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:
Information cannot be changes in transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:
The creator/sender of information cannot deny his or her intention to send information at later stage.

Authentication:
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.
Symmetric Key Cryptography

• This is also called Secret Key or Private Key cryptography.
• In this the same key is used for encryption and decryption.
• Hence the key is shared by the sender and receiver and must be kept secret.
• It is shown in following diagram.
Symmetric Key Cryptography

a. A shared secret key can be used in Alice-Bob communication

b. A different shared secret key is recommended in Bob-Alice communication
Asymmetric Key Cryptography

This is as well known as public key cryptography.
• In this every entity has two keys:
  - A public key well-known to any or all.
  - A private key well-known only to itself.

• When A needs to send a personal or private message to B, A encrypts the message uses B’s public key.
• B then decrypts the message uses his own non-public or private key.
• When B needs to send a non-public message to A, B encrypts the message utilizes A’s public key.
• A then decrypts the message utilizes his own non-public or private key.
Asymmetric Key Cryptography

a. Bob’s keys are used in Alice-Bob communication

b. Alice’s keys are used in Bob-Alice communication

Dig(B). References The McGraw-Hill Companies, Inc.
Types of Ciphers

**Substitution Cipher**: This offers an alternative to the plaintext. It is also called as Caesar cipher.

**Polyalphabetic Substitution Cipher**: In this cipher, a mixed alphabet is used to encrypt the plaintext, but at random points it would change to a different mixed alphabet which indicates the change with an uppercase letter in the Ciphertext.

**Transposition Cipher**: This cipher is also called as Rail Fence Cipher and is a permutation of the plaintext.

**Permutation Cipher**: The positions held by plaintext are shifted to a regular system in this cipher so that the ciphertext constitutes a permutation of the plaintext.
Substitution cipher Example

A substitution cipher is one where each symbol is replaced by another symbol. If the replacement rule does not vary, the cipher is a monoalphabetic substitution cipher.

The text we will encrypt is ‘robert attacked the guard with a knife'.

Keys for the simple substitution cipher usually consist of 26 letters (compared to the caeser cipher's single number).

An example key is:

| plain alphabet: | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Cipher alphabet:| p | h | q | g | i | u | m | e | a | y | l | n | o | f | d | x | j | k | r | c | v | s | t | z | w | b |

An example encryption using the above key:

plaintext: robert attacked the guard with a knife
ciphertext: kdhikc pccqlig cei mvpkg tace p lfau
Transposition Cipher

For example, the plaintext is “golden temple is situated in Amritsar city” and the secret random key chosen is “APPLE”. We arrange this text horizontally in table with number of column equal to key value alphabetically. The resulting text is shown below.

<table>
<thead>
<tr>
<th>A</th>
<th>P</th>
<th>P</th>
<th>L</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>g</td>
<td>o</td>
<td>l</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>n</td>
<td>t</td>
<td>e</td>
<td>m</td>
<td>p</td>
</tr>
<tr>
<td>l</td>
<td>e</td>
<td>i</td>
<td>s</td>
<td>s</td>
</tr>
<tr>
<td>i</td>
<td>t</td>
<td>u</td>
<td>a</td>
<td>t</td>
</tr>
<tr>
<td>e</td>
<td>d</td>
<td>i</td>
<td>n</td>
<td>a</td>
</tr>
<tr>
<td>m</td>
<td>r</td>
<td>i</td>
<td>t</td>
<td>s</td>
</tr>
<tr>
<td>a</td>
<td>r</td>
<td>c</td>
<td>i</td>
<td>t</td>
</tr>
<tr>
<td>y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The ciphertext is obtained by reading column vertically downward ranging from first to last column.

**The ciphertext is:**

gniemayepstast dmsanti otetdrr leiuiic
Railfence cipher

The key for the railfence cipher is just the number of rails. To encrypt a text, e.g.
‘defend the east wall of the castle’
Key: 3
Solution: We write it out in a special way on a number of rails (the key here is 3)

d n e t l h s
 e e d h e s w l o t e a t e
f t a a a f c l

The ciphertext is read off along the rows:
dnetlhseedheswloteateftaafcl
Thank You