LECTURE NOTES ON Classical Cryptographic Techniques (Substitution Ciphers System)

By
Dr. Samaher Hussein Ali

College of Information Technology, University of Babylon, Iraq
Samaher_hussein@yahoo.com
Classical Cryptographic Techniques

have two basic components of classical ciphers: **Substitution** and **Transposition**

![Diagram of Classical Ciphers: Substitution and Transposition](image)

### Substitution Ciphers System

- Simple substitution system (mono)
- Homophonic substitution system
- Polyalphabetic substitution system

In **Substitution Ciphers** letters are replaced by other letters, such as the word message in the following:

<table>
<thead>
<tr>
<th>Original</th>
<th>Substitution</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>MESSAGE</td>
<td></td>
<td>PHVVDJH</td>
</tr>
<tr>
<td>KEY=3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>YQEEMSQ</td>
</tr>
<tr>
<td>KEY=12</td>
<td></td>
<td>HZNNVBZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLZZHNL</td>
</tr>
<tr>
<td>KEY=7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. **Simple Substitution System** \ Mono Substitution System

- Additive Cipher
- Multiplicative Cipher
- Affine Cipher
- Reverse Cipher (27-P)

**Additive Cipher**

Let \( C = \text{Cipher Text} \)
\( P = \text{Plain Text} \)
\( K = \text{Key; } K = 2, 3, \ldots, 25 \)
\( n = 26 \), of English alphabetic

**Example:** Let, Plain text = help , key =3 ( or using Ceaser Method)

Plain text:  **HELP**
Cipher text:  **KHOS**

---

Dr. Samaher Hussein Ali

Notes of Lecture 3
Substitution Ciphers System

❖ Additive Cipher (The Caesar cipher)

Key=3

Outer: plaintext
Inner: ciphertext

For a key K=3,
plain text letter: ABCDEF...UVWXYZ
ciphertext letter: DEFGHI... XYZABC

Example:
TREATY IMPOSSIBLE is translated into
WUHDWB LPSRVVLEOH
Substitution Ciphers System

Multiplicative Cipher

C = (P*K) Mod n

P = (C * Inv(K)) Mod n

Let C= Cipher Text
P= Plain Text
K= Key; K= 2,3,...............25
n =26 , of English alphabetic

Example: Let, Plain text = help , key =3

Plain text: HELP
Cipher text: XOJV

Note: we can find the inv(key) as following

(K* Inv(K)) Mod n =1

Example: Let, Key=3
(3 * X) mod 26=1
(3*9) mod 26 = 27 mod 26 =1 ----→ inv(3) = 9
Substitution Ciphers System

Note: The number of useful key in multiplicative
Key inverse key
3  9
5  21
9  3
11 19
15  7
17 23
19 11
21  5
23 17
25 25

Example: Let, Key=5
(5 * X) mod 26=1
(3*21) mod 26 = 105 mod 26 =1 ----→ inv(5) = 21

Example: Let, Plain text = MY DOCUMENT , key =21, Find the cipher text using Multiplicative Cipher

Sol: Key = 21 ; inv(21)=5
C=(P*K) Mod 26

Plain text:   MY Document
Cipher text:  ..........

Then , P=(C* Inv(K)) Mod 26

Cipher text:  ..........
Plain text:   MY Document
**Affine Cipher**

Affine cipher: It is a hybrid between an additive and multiplicative methods.

\[ C = ((P \times K_1) + K_2) \mod n \]

\[ C = ((P + K_2) \times K_1) \mod n \]

\[ P = ((C - K_2) \times \text{Inv}(K_1)) \mod n \]

\[ P = ((P \times \text{Inv}(K_1) - K_2) \mod n \]

**Key Terms:**
- **K1** = Multiplicative cipher key
- **K2** = Additive cipher key
As a result, classical ciphers: substitution and transposition.

**Fig. Expanding of Classical cipher Methods**