
# NETWORK PROTOCOLS & SECURITY
# 23EC2210 R/A/E

Topic:

## Substitution Techniques

Session – 35

# Substitution Ciphers

# Substitution Techniques

A character of plaintext is replaced by another character

or

A sequence of bits of plain text is replaced by another sequence of bits.

# Caesar Cipher

- It replaces each letter by next 3rd letter
  example: meet me after the toga party
  PHHW PH DIWHU WKH WRJD SDUWB
- Can define transformation as:
  plain: 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 = IN
  cipher :D E F G H I J K L M N O P Q R S T U V W X Y Z A B C = OUT

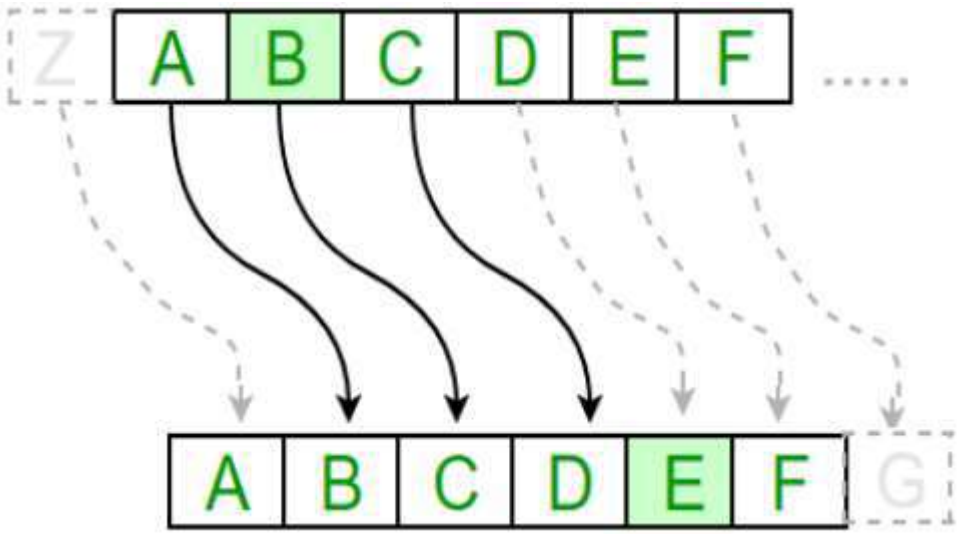
- If a=0, b=1, … *z* =25, then for each plaintext letter P, substitute the ciphertext letter *C*,
  $C = E(k, p) = (p + k) \bmod (26)$ for Encryption
  $p = D(k, C) = (C - k) \bmod (26)$ for Decryption
  where *k takes on a value in the range 1 to 25.*

# Caesar Cipher

- The Caesar cipher includes substituting each letter of the alphabet according to the positions of the key values down the alphabet.

- It is also known as additive cipher.

For example, with a shift of 1, A would be replaced by B, B would become C, and so on.



# Caesar Cipher…

## Mathematical Representation:

Caesar cipher can be represented using modular arithmetic by first transforming the letters into The encryption numbers, according to the scheme, A = 0, B = 1,…, Z = 25.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

The formula of encryption is:

**En (x) = (x + n) mod 26**

The formula of decryption is:

**Dn (x) = (xi - n) mod 26**

Where,

**E** denotes the encryption
**D** denotes the decryption
**x** denotes the letters value
**n** denotes the key value (shift value)

Note: If any case (Dn) value becomes negative (-ve), in this case, we will add 26 in the negative value.

# Brute-Force Cryptanalysis of Caesar Cipher

| KEY | | | | | | |
|---|---|---|---|---|---|---|
| | PHHW | PH | DIWHU | WKH | WRJD | SDUWB |
| 1 | oggv | og | chvgt | vjg | vgic | rctva |
| 2 | nffu | nf | bgufs | uif | uphb | qbsuz |
| 3 | meet | me | after | the | toga | party |
| 4 | ldds | ld | zesdq | sgd | snfz | ozqsx |
| 5 | kccr | kc | ydrcp | rfc | rmey | nyprw |
| 6 | jbbq | jb | xcqbo | qeb | qldx | mxoqv |
| 7 | iaap | ia | wbpan | pda | pkcw | lwnpu |
| 8 | hzzo | hz | vaozm | ocz | ojbv | kvmot |
| 9 | gyyn | gy | uznyl | nby | niau | julns |
| 10 | fxxm | fx | tymxk | max | mhzt | itkmr |
| 11 | ewwl | ew | sxlwj | lzw | lgys | hsjlq |
| 12 | dvvk | dv | rwkvi | kyv | kfxr | grikp |
| 13 | cuuj | cu | qvjuh | jxu | jewq | fqhjo |
| 14 | btti | bt | puitg | iwt | idvp | epgin |
| 15 | assh | as | othsf | hvs | hcuo | dofhm |
| 16 | zrrg | zr | nsgre | gur | gbtn | cnegl |
| 17 | yqqf | yq | mrfqd | ftq | fasm | bmdfk |
| 18 | xppe | xp | lqepc | esp | ezrl | alcej |
| 19 | wood | wo | kpdob | dro | dyqk | zkbdi |
| 20 | vnnc | vn | jocna | cqn | cxpj | yjach |
| 21 | ummb | um | inbmz | bpm | bwoi | xizbg |
| 22 | tlla | tl | hmaly | aol | avnh | whyaf |
| 23 | skkz | sk | glzkx | znk | zumg | vgxze |
| 24 | rjjy | rj | fkyjw | ymj | ytlf | ufwyd |
| 25 | qiix | qi | ejxiv | xli | xske | tevxc |

# Caesar Cipher - brute-force cryptanalysis

- Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

  1. The encryption and decryption algorithms are known.
  2. There are only 25 keys to try.
  3. The language of the plaintext is known and easily recognizable.

# Caesar Cipher Example

Given,

Plaintext: JAVATPOINT

Key(shift) value: 3

**Encrypted Message/ Cipher text:**

MDYDWSRLQW

$E_n(x) = (x + n) \bmod 26$

| | | |
|---|---|---|
| Plaintext: J → 09 | $E_n$: (09 + 3) mod 26 | Ciphertext: 12 → M |
| Plaintext: A → 00 | $E_n$: (00 + 3) mod 26 | Ciphertext: 3 → D |
| Plaintext: V → 21 | $E_n$: (21 + 3) mod 26 | Ciphertext: 24 → Y |
| Plaintext: A → 00 | $E_n$: (00 + 3) mod 26 | Ciphertext: 3 → D |
| Plaintext: T → 19 | $E_n$: (19 + 3) mod 26 | Ciphertext: 22 → W |
| Plaintext: P → 15 | $E_n$: (15 + 3) mod 26 | Ciphertext: 18 → S |
| Plaintext: O → 14 | $E_n$: (14 + 3) mod 26 | Ciphertext: 17 → R |
| Plaintext: I → 08 | $E_n$: (08 + 3) mod 26 | Ciphertext: 11 → L |
| Plaintext: N → 13 | $E_n$: (13 + 3) mod 26 | Ciphertext: 16 → Q |
| Plaintext: T → 19 | $E_n$: (19 + 3) mod 26 | Ciphertext: 22 → W |

# Caesar Cipher Example...

Ciphertext: MDYDWSRLQW

**Decrypted Message:**

JAVATPOINT

$$D_n(x) = (x_i - n) \bmod 26$$

If any case ($D_n$) value becomes negative (-ve), in this case, we will add 26 in the negative value.

| | | |
|---|---|---|
| Ciphertext: M → 12 | $D_n$: (12 - 3) mod 26 | Plaintext: 09 → J |
| Ciphertext: D → 03 | $D_n$: (03 - 3) mod 26 | Plaintext: 0 → A |
| Ciphertext: Y → 24 | $D_n$: (24 - 3) mod 26 | Plaintext: 21 → V |
| Ciphertext: 3 → D | $D_n$: (03 - 3) mod 26 | Plaintext: 0 → A |
| Ciphertext: 22 → W | $E_n$: (19 + 3) mod 26 | Ciphertext: 22 → W |
| ⋮ | ⋮ | ⋮ |

# Mono alphabetic Cipher

- Rather than just shifting the alphabet could shuffle the letters arbitrarily
- But, Here, Each plaintext letter maps to a different random cipher text letter
- Hence key is 26 letters long

  Letters: abcdefghijklmnopqrstuvwxyz
  Key : DKVQFIBJWPESCXHTMYAUOLRGZN
  Plaintext: ifwewishtoreplaceletters
  Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
- If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then $10^{26}$ Keys are possibe, is it secure ? No.

# Mono alphabetic Cipher

- Monoalphabetic Cipher is a cipher where the letters of the plain text are mapped to ciphertext letters based on a single alphabetic key.
- Key is 26 letters long
- It is a one to one mapping.

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
```

```
Plaintext:  ifwewishtoreplaceletters
Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA
```

# Monoalphabetic Cipher example

| a | b | c | d | e | f | g | h | i | j |
|---|---|---|---|---|---|---|---|---|---|
| Q | W | E | R | T | Y | U | I | O | P |
| k | l | m | n | o | p | q | r | s | t |
| A | S | D | F | G | H | J | K | L | Z |
| u | v | w | x | y | z | | | | |
| X | C | V | B | N | M | | | | |

```
Plain text: Live the moment
Encrypted message: SOCT ZIT DGDTFZ
Decrypted message: live the moment
```

# Playfair Cipher

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher.

In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. because Playfair is reasonably fast to use and requires no special equipment.

So we can go for multiple letters substitution at a time. The Play fair Cipher is an example of 2 letter substitution at a time.

# Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword
- fill the letters of keyword in table first, then other letters.
- For Example, using the keyword MONARCHY the table is

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

# Playfair Cipher

- The Playfair cipher was the first practical **digraph substitution cipher.**
- The Playfair cipher encrypts pairs of letters (digraphs), instead of single letters.
- This is significantly harder to break.

## Method:

- The Playfair cipher uses a 5 by 5 table containing a key word or phrase.
- To generate the table, one would first fill in the spaces of the table with the letters of the keyword (dropping any duplicate letters).
- Then fill the remaining spaces with the rest of the letters of the alphabet in order (to reduce the alphabet to fit you can either omit "Q" or replace "J" with "I").
- In the example to the right, the key is "keyword".

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

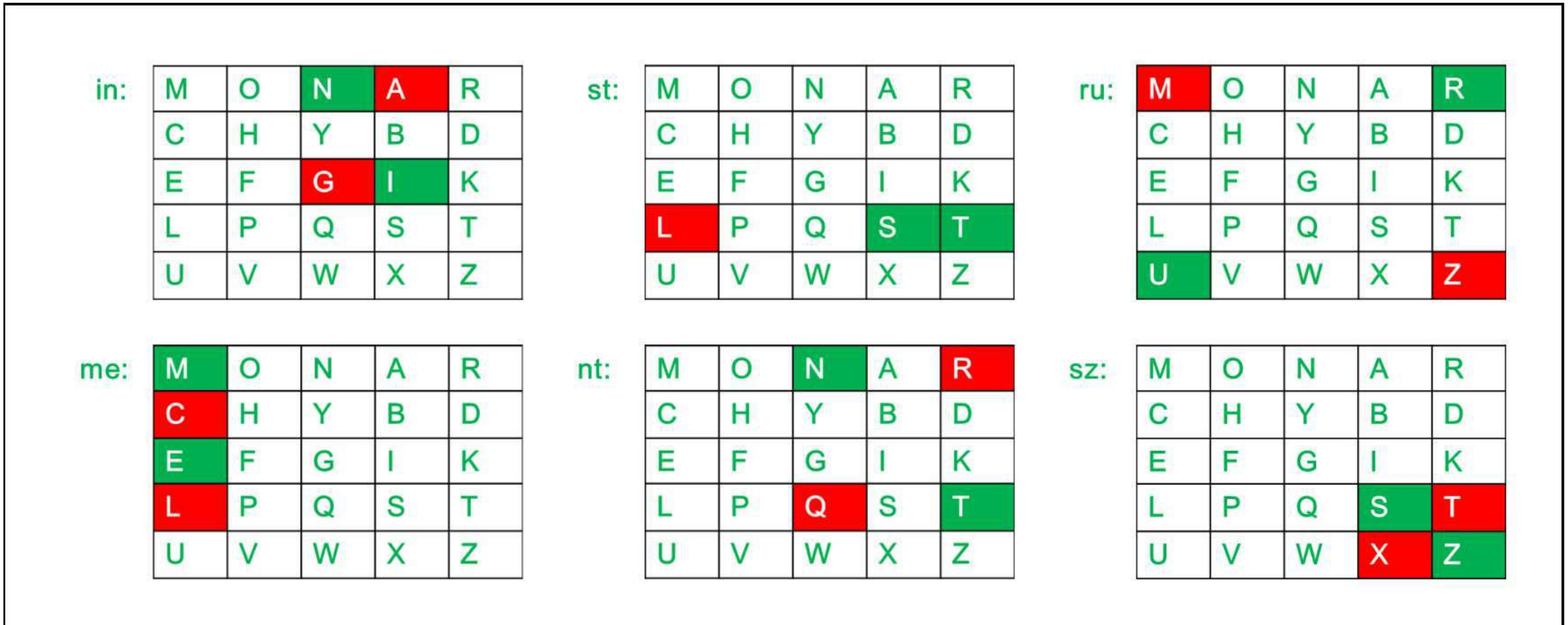
# Playfair Cipher…

- To encrypt a message, one would break the message into groups of 2 letters. If there is a dangling letter at the end, we add an X. For example. "Secret Message" becomes "SE CR ET ME SS AG EX". We now take each group and find them out on the table. Noticing the location of the two letters in the table, we apply the following rules, in order.
    1. If both letters are the same, add an X between them. Encrypt the new pair, re-pair the remining letters and continue.
    2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively, wrapping around to the left side of the row if necessary. For example, using the table above, the letter pair GJ would be encoded as HF.
    3. If the letters appear on the same column of your table, replace them with the letters immediately below, wrapping around to the top if necessary. For example, using the table above, the letter pair MD would be encoded as UG.
    4. If the letters are on different rows and columns, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first letter of the pair should be replaced first. For example, using the table above, the letter pair EB would be encoded as WD.

- To decipher, ignore rule 1. In rules 2 and 3 shift up and left instead of down and right. Rule 4 remains the same. Once you are done, drop any extra Xs that don't make sense in the final message and locate any missing Qs or any Is that should be Js.

# Playfair Cipher example

- Key: MONARCHY Message: instruments
- After Split: 'in' 'st' 'ru' 'me' 'nt' ‘sz‘
- Here z is padded to make even number of characters
- Cipher text: gatlmzclrqtx



## Example

Plaintext: attack

Digrams: at ta ck

Plaintext: neso academy

Digrams: ne so ac ad em yx

Plaintext: balloon

Digrams: ba ll oo n

Digrams: ba lx lo on

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