Network and Computer Security.
CSE 437

Booki

12.07.25 — Class no.: 1

Cryptography and Network Security.
—3rd edition (Behrouz A. Forouzan) — (752 page total)

★ 3 principle to secure information: (Security goals) — Page 28
→ confidentiality.
→ integrity
→ availability.

★ Security attacks (figure 1.2; page-29)

confidentiality →
⇒ Snooping (unauthorized user getting access to confidential info)
⇒ Traffic analysis

★ Attacks threatening integrity:
kinds of attacks
→ modification
→ mas-querading (ছদ্মবেশ ধারণ)
→ replaying.
→ repudiation (deny)

★ Availability:
Denial of Service (harms system)

Table 1.1 (Page-31) — Categorization of Passive-active attacks.
→ Passive-attack
→ Active-attack

1.3 Service and Mechanisms. (Page 32)

Security services:

→ Data confidentiality

→ Data integrity.

→ Authentication.

→ Nonrepudiation.

→ Access control.

Figure 1.4 Security mechanism (Page 32) (total-8)

Authentication Exchange.

Traffic padding.

Routing control.

Notarization.

★ Table 1.2 (Page 35)
Relation between security services and security mechanisms.

Cryptography } Encipherment
Steganography } technique.

Cryptography
- Encryption
- Decryption.

Symmetric key
Asymmetric key
Hashing.

Chapter 1 (1.1–1.3)

Symmetric key cipher:

Figure 3.1 (General idea of symmetric key cipher) — page 82

$E_k(x)$
- → encryption algo.
- → plain text
- → key

$D_k(c)$

$\frac{n(n-1)}{2}$ key required

- Kirckhoff's principle (Page-83):
  (hide key, not algorithm)
- Cryptoanalysis (Page-84):
  measures how vulnerable cryptosystem is.

Cryptoanalysis attacks:

- ✱ ↳ Ciphertext only attack: (ciphertext — key, plaintext)
  - ↳ Brute-force attack:
  - ↳ Statistical attack
  - ↳ Pattern attack.

- ✱ Known plaintext attack: (previous text)
- ✱ Chosen-plaintext attack (hardware access)
- ✱ Chosen-ciphertext attack

Figure important.

3.2 Substitution ciphers:

→ Monoalphabetic ciphers (One to one)
→ Polyalphabetic ciphers. (One to many)

Additive cipher (Page-88)

Example 3.3.

plain-text = hello
key = 15

WTAAD

CWTAAD

22 19 00 00 03

22 − 15 = 7 mod 26

19 − 15 = 4 "

00 − 15 = −15 "

00 − 15 = −15 "

03 − 15 = −12 "

★ Shift cipher: } Additive cipher

★ Caesar cipher: }

Example 3.5

Multiplicative cipher

Page-88

Additive cipher

Page-91

Multiplicative cipher

$9 \equiv 3 \pmod 6$
modular inverse

Figure 3.10

Example 3.8

If K=7

h — 7
e — 9
l — 11
l —
o — 19

$C = (P * K) \bmod 26$

h ⟶ 49 mod 26 = 23
e ⟶ 28 mod 26 = 2
l ⟶ 77 mod 26 = 25
l ⟶ 77 mod 26 = 25
o ⟶ 98 mod 26 = 20

Affine cipher (page 92) + Figure 3.11

combines (additive + multiplicative cipher)

$(P \times K_1 + K_2) \bmod 26$

$P = ((C - K_2) \times K_1^{-1}) \bmod 26$

↳ modulu inverse.

Example 3.10

Example 3.11

{Cryptoanalysis for Affine cipher.}

$K_1 = 7$

$K_2 = 2$

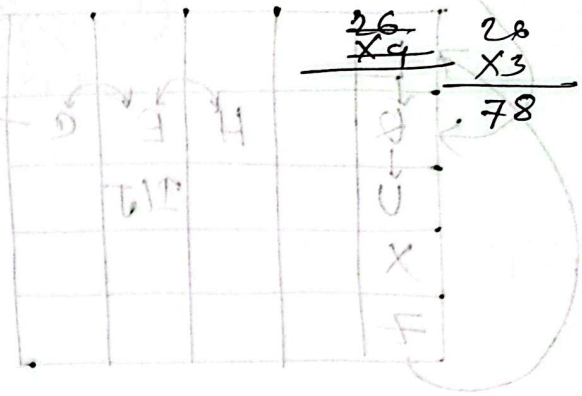
$h \longrightarrow 51 \bmod 26 = 25$

$e \longrightarrow 30 \bmod 26 = (4)$

$l \longrightarrow 79 \bmod 26 = 01$

$l \longrightarrow 79 \bmod 26 = 01$

$o \longrightarrow 100 \bmod 26 = 22$



$((4-2) \times 7^{-1}) \bmod 26$

* Monoalphabetic
* Multiplicative Substitution Cipher (Page 94) + figure 3.12

↓

→ diff. key
→ makes difficult for brute-force attack.

till now Hello → same cipher value. advantageous for attacker.

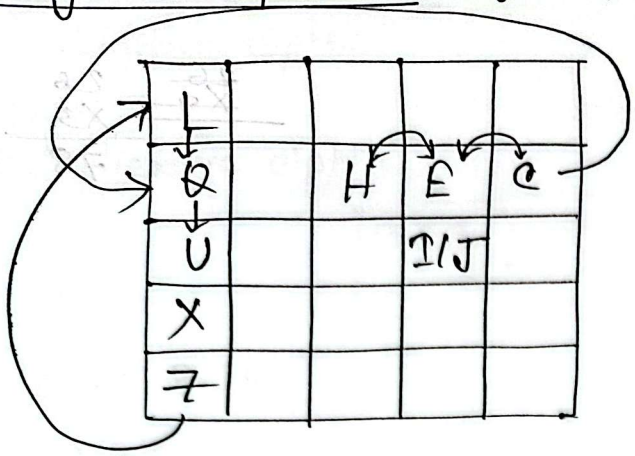
* Polyalphabetic cipher (Page 95)
* Autokey cipher (Page 95)

$K = (K_1, P_1, P_2, \ldots\ldots)$

Example 3.19

⇒ additive
polyalphabetic – key different.
additive – key same.

Playfair cipher: (Page 96)



* same letter একসাথে e.g. hello
  l. bogus letter x

Example 3.15

* same row ⟶ wrap with next character.

~~Playfair (Cryptoanalysis)~~
বুঝবার চেষ্টা.

* diff. row — diff. column.
  (row ও column দুইই change)

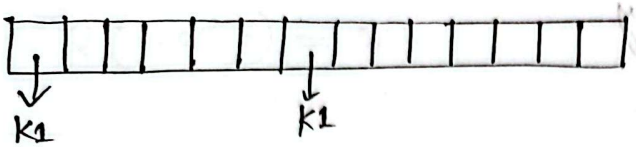
L (1,1) —— L এর cipher (L এর row, O এর col) =
O (4,4) —— O " " (O এর row, L এর col) =

{ Linear congruence.
  modular inverse

Vigenere Cipher (Page-98) 20.07.25

(Key repeats) e.g. $K_1 - K_6$ (Pascal)

K_1 K_2 K_3 .....



→ ~~Cryptoanalysis~~ (Vigenere)

→ Hill cipher ~~+~~ বা sub-division (বিভাগ)

Transposition ciphers (Page-107)

- Keyless
- Keyed

Keyless — Row by Row → সারিভিত্তিক row, সারিভিত্তিক col.

Column by Column → সারিভিত্তিক col, সারিভিত্তিক rowwise.
wise

Example - 3.23

Column by Column

→ row no given
→ organize column wise
→ row by row sending.

Row by row

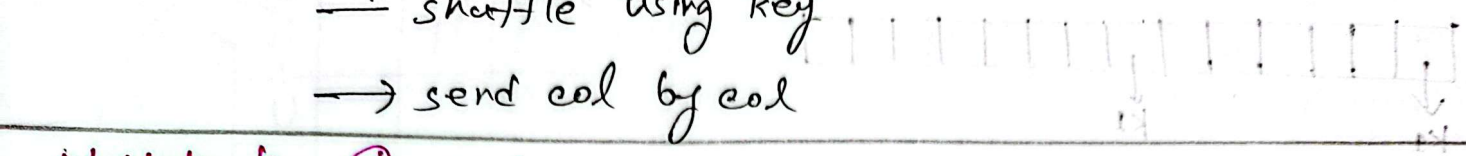
→ col. no will be given
→ organize row wise
→ col by col sending.

meet me at the park.

m	e	e
t	m	e
a	t	t
h	e	p
a	r	k

Keyed transposition cipher (Page 108)

— row by row organize.
— shuffle using key
⟶ send col by col



Multiplicative Inverse:

- Wheather there exist a MI for a number under (mod n) or not.

$5 \times 5^{-1} = 1$ $\quad$ $A \times A^{-1} = 1$

↳ MI of (5)

Under mod n:

$A \times A^{-1} = 1 \pmod n$

When this value is divided by (n), we get the remainder as 1

Q. $3 \times ? = 1 \bmod 5$ (What is the M.I. of 3 (mod 5)?)

↳ $3 \times 2 = 1 \bmod 5$

relatively prime to each other and modular arithmetic.

Q. $2 \times ? = 1 \bmod 11$

↳ $2 \times 6 = 1 \bmod 11$

Q. $4 \times ? = 1 \bmod 5$.

↳ $4 \times 4 = 1 \bmod 5$

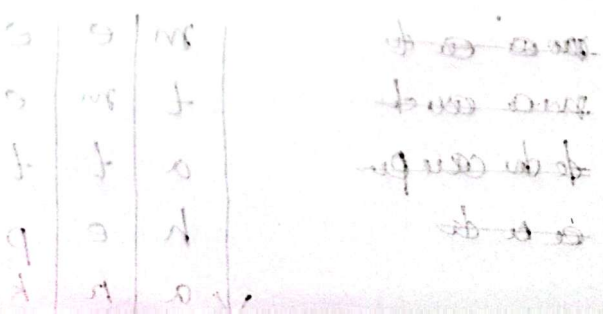
Q. $5 \times ? = 1 \bmod 10$

will never get.

Relatively prime:

$GCD(x, y) = 1$

(In such cases, we will never have a multiplicative inverse if they are not relatively prime).



The M.I. for 2(mod 5) is 3

The M.I. for 2(mod 7) is 4

$2 \pmod 5 = 3$

(remainder; divided by)

Extended Euclidean Algorithm:
(when number is very big)

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	2	-5	X

A > B

$B \overline{)A}$

R

$T_1 = 0$ and $T_2 = 1$

$T = T_1 - T_2 \times Q$

T_1 is the M.I.

Continue the iteration:

Stop when

$0 \overline{)1}$

situation arises.

What is the multiplicative inverse of 3 mod 5?

→ Cryptoanalytis attacks of transposition ciphers. (no so important)
page: 111
→ Stream cipher — additive, monoalphabetic, vigenere
→ Block cipher.

Steam cipher Vs Block cipher:

Confusion and Diffusion: (property should owned by encryption technique)

Confusion → making the relationship between the encryption key and ciphertext as complex as possible.
→ Relationship between plaintext and ciphertext is obscured.

Diffution → Making each plaintext bit affect as many ciphertext bit as possible.
e.g. 1 bit change in PT, significant effect on CT.
Example: Transposition / permutation.

Stream cipher:

Each plaintext digit is encrypted one at a time with the corresponding digit of the keystream.

Block cipher:

A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks.

Sunday – CT (Chapter-3) -
03.08.25

Monoalphabetic	Polyalphabetic	Transposition
Additive	Autokey	Keyed
Multiplicative	Playfair	Keyless
Affine	× Vigenere	

4 types of attack:

Chapter 6:

Data Encryption Standard

⇒ Figure 6.1 (Page 186) —
56 bit key

⇒ Figure 6.2 (General Structure of DES — ~~Page~~ page 187)
From 56 bit, 16 48 bit key will be generated.

Page – 188
Table 6.1 (Initial and final Permutation table)

Page – 188
example 6.2

Figure 6.5 (DES function)

Page 189

DES Function
- → Expansion P-box
- → XOR
- → S-box
- → Straight P-box

Figure 6.8 S-box rule. (Page 190)

row — bit(1,6)
col — bit(2,3,4,5)

Linear congruence
Modular inverse
— required in multiplicative + affine

DES

64 bit — plaintext ↔ ciphertext
56 bit — Key size

From page no. — 187

Key generation (196 page)

64 —8→ 56 (parity bit discarded) (8 16 32 64)

↓

48 bit gererated (16)

64 32 16 8 4 2 1
63

197 bit

Key with parity bit (64 bit)

↓

Parity drop

↓

cipher key (56 bit)

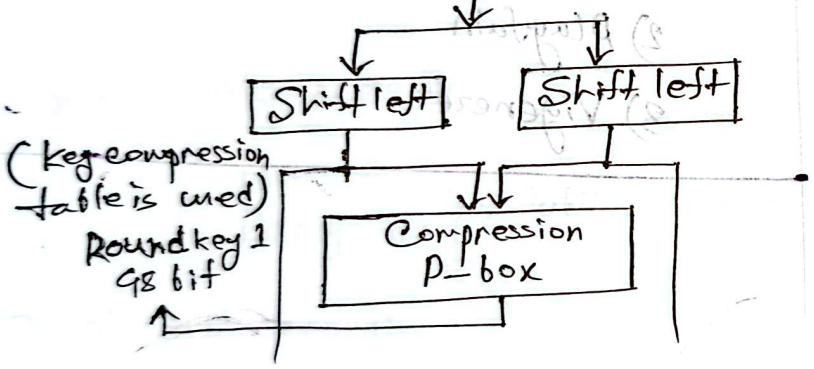


Table 6.14

1-56 — 6 bit each

48

Figure 6.5

6.3 DES Analysis (Page 201)

DES weakness (Page-203)

Table 6.18 (Weak keys)