(Ch-10) CRYPTOGRAPHY

(10.1) Transforming messages to secret form, then convert it to plain text.

Text — Cipher text (Coding text)
— plain text (message to convey)

① The process of converting from plain text (main message) to cipher text is said to be encrypting. (or encipherment)

② The process of changing from cipher text (coded msg) back to plain text is called decrypting. (or decipherment)

Caesar Cipher -

Plain text 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 text 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

(Example) The plain text message (plain text message)

CAESAR WAS GREAT — (1)

ciphertext FDHVDU ZDV JUHDW.

* The Caesar Cipher described using Congruence theory
[The plain text is first expressed numerically by translating the characters of the text into digits as following:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

P → plaintext letter
C → ciphertext letter

Relation in Congruence form $C \equiv P + 3 \pmod{26}$ adding 3 to each letter of plain text.

Scanned with CamScanner

Formula eq^n ① in congruence relation

Plaintext C A E S A R W A S G R E A T
02 00 04 18 00 17 22 00 18 06 17 04 00 19

then Ciphertext using Congruence

$C \equiv P + 3 \pmod{26}$

(02+3) (00+03) (04+3)

05 03 07 21 03 20 25 03 21 09 20 07 03 22

Now, recover the plaintext

Plaintext $P \equiv C - 3 \equiv C + 23 \pmod{26}$

(Example) ATTACK AT ONCE ... so on

00 19 19 00 02 10 00 19 14 13 02 04

Use Keyword READY

numerical version 17 04 00 03 24

+ Repetitions of this sequence are arrayed, add numerical version, then

17 04 00 03 24 17 04 00 03 24 17 04
(repeat until digits finish of main msg.)

Now, Add columns modulo 26, the plaintext is encrypted as

00+17 19+4 19+00 (26≡0) (27≡1)

17 23 19 03 00 01 04 19 17 11 19 08

we get (by using cater cipher, congruence

R X T D A B E T R L T I

Scanned with CamScanner

General form

Encryption $C_i \equiv P_i + b_i \pmod{26}$; $1 \le i \le n$

where plain message is expressed as successive blocks $P_1 P_2 \cdots P_n$ of in two digits integers P_i

Ciphertext blocks $C_1 C_2 \cdots C_n$

and $b_1 b_2 \cdots b_n$ $(00 \le b_i \le 25)$ will serve as keyword.

Decryption $P_i \equiv C_i - b_i \pmod{26}$ $1 \le i \le n$.

Note: Keyword — seed or primer (generally a single letter)

(Example (10.1)) Assume that the message

ONE IF BY DAWN

is to be encrypted. Taking the letter K as the seed,

(Plain to Cipher)

(Sol^n) By taking letter K as the seed, (shift by single letter K)

Keyword becomes

KONEIFBYDAWN

When Both plaintext and Keyword are converted numerical form, we obtain

O	N	E		I	F		B	Y		D	A	W	N	
14	13	04		08	05		01	24		03	00	22	13	
10	14	13		04	08		05	01		24	03	00	22	
K	O	N		E	I		F	B		Y	D	A	W	

Adding these integers under modulo 26

$(27 \equiv 1) \pmod{26}$

24 01 17 12 13 06 25 01 03 22 09

Now, changing back to letters, By Caesar Cipher Congruence

Y B R M N G Z B D W J. (Ans)

Scanned with CamScanner

Note: Recovering the main MSJ ONE IF BY DAY-UN, By using Formig, Congruence Relation with seed (key word)

* Plaintext (digits equivalent) $P_1 P_2 - P_n$
* Ciphertext $C_1 C_2 - C_n$
* S indicates the seed

$P_1 = C_1 - S = 24 - 10 \equiv 14 \pmod{26}$
(use previous example) $Y - K = O$ (letter)
P_1 (first alphabet)

$P_2 = C_2 - S = 01 - 14 \equiv -13 \equiv 13 \pmod{26}$
$B \quad O \equiv N$

$P_3 = C_3 - S = 17 - 13 \equiv 4 \pmod{26}$
$R \quad N \quad E$

In general, form

$P_K \equiv C_K - P_{K-1} \pmod{26}$

(maintain two digit format. 4 is written as 04)

Hill-Ciphes Method:

In this method, message is divided into blocks of 2 letters.

In congruence form,

$C_1 = a P_1 + b P_2 \pmod{26}$

$C_2 \equiv c P_1 + d P_2 \pmod{26}$

where four coefficient a, b, c, d must be such that

$\gcd(ad - bc, 26) = 1$

(Ex/p. 10.2) Use, Hill's Cipher, method.

let us use the congruence

$C_1 \equiv 2P_1 + 3P_2 \pmod{26}$ — (1)

$C_2 \equiv 5P_1 + 8P_2 \pmod{26}$ — (2)

to encrypt the message BUY NOW.

(Soln) We divide in blocks of 2 letters.

BU YN OW

Numerically For BU (block) 01 20
$\downarrow P_1$ $\downarrow P_2$

Scanned with CamScanner

$P_1 = 01$, $P_2 = 20$ (doing for first block BU) (3)

From (1) & (2), we get

$2P_1 + 3P_2 \pmod{26}$

i.e $2(01) + 3(20) \pmod{26}$

$= 62 \pmod{26}$

$\equiv 10 \pmod{26}$

$\Rightarrow C_1 = 10 = K$

$C_2 \equiv 5P_1 + 8P_2 \pmod{26}$

$= 5(01) + 8(20)$

$= 165 \pmod{26}$

$\equiv 09$

$C_2 = 09 = JJ$

(2) YN (1block) $P_1 = Y = 24$, $P_2 = N = 13$

$2(24) + 3(13) = 48 + 39 \equiv 87 \equiv 9 \pmod{26}$

$5(24) + 8(13) = 120 + 104 \equiv 204 \equiv 16 \pmod{26}$

$C_1 = 9 = J$, $C_2 = 16 \equiv Q$

(5) OW (1block) $P_1 = O = 14$, $P_2 = 22 = W$

$2(14) + 3(22) = 28 + 66 = 94 \equiv 16 \pmod{26}$

$5(14) + 8(22) = 70 + 176 = 246 \equiv 12 \pmod{26}$

$C_1 = 16$, $C_2 = 12$

$= Q$ $= M$

∴ Complete cipher text is

10 09 09 16 16 12

(10 09 — first block)

K J J Q Q M

Now, to find (Decryption) the plain text

$P_1 \equiv 8C_1 - 3C_1 \pmod{26}$

$P_2 \equiv -5C_1 + 2C_2 \pmod{26}$

K J J Q Q M

(K J — first block)

(1) K J $C_1 = K = 10$, $C_2 = J = 09$

$P_1 = 8(10) - 3(09) = 80 - 27 = 53 \equiv 01 \pmod{26}$

$P_2 = -5(10) + 2(09) = -50 + 18 = -32 \equiv 20 \pmod{26}$

Scanned with CamScanner

$P_1 = 01 = B$, $P_2 = 20 = U$. (same obtained Plain msg)

② JQ $C_1 = J = 09$, $C_2 = Q = 16$

$P_1 = 8(09) - 3(16) = 72 - 48 = 24 \pmod{26}$

$P_2 = -5(09) + 2(16) = -45 + 32 = -13 \equiv 13 \pmod{26}$

$P_1 = 24 = Y$

$P_2 = N = 13$

③ QM

$C_1 = Q = 16$, $C_2 = M = 12$

$P_1 = 8(16) - 3(12) = 92 \equiv 14 \pmod{26}$

$P_2 = -5(16) + 2(12) = -80 + 24 \equiv -56 \equiv 22 \pmod{26}$

$P_1 = 14 = O$, $P_2 = 22 = W$

Complete Plain Text is

01	20	24	13	14	22
B	U	Y	N	O	W

Exr. 1, 2, 3, 7, 8, 12, 13

(Exr. ①) RETURN HOME using Caesar Cipher

RETURN HOME

$C \equiv P + 3 \pmod{26}$

R	E	T	U	R	N	H	O	M	E
17	04	19	20	17	13	07	14	12	04
20	07	22	23	20	16	10	17	15	07
U	H	W	X	U	Q	K	P	R	H

(Addii +3) → 20 07 22 23 20 16 10 17 15 07

we set ↓

U H W X U Q K P R H

(0.3) ...

Scanned with CamScanner

(Ex 8.7) (a) Use Hill cipher $C_1 = 5P_1 + 2P_2 \pmod{26}$
$C_2 = 3P_1 + 4P_2 \pmod{26}$

to encipher the message GIVE THEM TIME

(Soln) GI VE TH EM TI ME

(1) GI $P_1 = G = 06$, $P_2 = I = 08$

$C_1 = 5(6) + 2(8) = 30 + 16 = 46 = 20 \pmod{26}$
$C_2 = 3(6) + 4(8) = 18 + 32 = 50 = 24 \pmod{26}$

$C_1 = 20 = U$, $C_2 = 24 = Y$

(2) VE $P_1 = V = 21$, $P_2 = E = 04$

$C_1 = 5(21) + 2(04) = 105 + 8 = 113 \equiv 9 \pmod{26} = C_1$
$C_2 = 3(21) + 4(04) = 63 + 16 = 79 \equiv 1 \pmod{26} = C_2$

$C_1 = 09 = J$, $C_2 = 01 = B$

(3) TH $\longrightarrow$ $C_1 = 05 = F$, $C_2 = 07 = H$

(4) EM $\longrightarrow$ $C_1 = S$, $C_2 = I$

(5) TI $\longrightarrow$ $C_1 = 7 = H$, $C_2 = 11 = L$

(6) ME $\longrightarrow$ $C_1 = 16 = Q$, $C_2 = 0 = A$

Complete Cipher Text (pairs)

20 24 09 01 05 07 18 8 7 11

16 0

$\Rightarrow$ U Y J B F H S I H L

Q A

(b) Cipher text ALXWU VADCOJO

AL XW UV AD CO JO

$C_1 \equiv 4P_1 + 11P_2 \pmod{26}$
$C_2 \equiv 3P_1 + 8P_2 \pmod{26}$

Here we know, C_1, C_2 (by coding)
to find P_1 & P_2 (simplify equation)

Scanned with CamScanner

i.e $4P_1 + 11P_2 = C_1$ — ①
$3P_1 + 8P_2 = C_2$ — ②

eq^n ② × 11 then subtract eq^n ① × 8

we get
$33P_1 + 88P_2 = 11C_2$
$32P_1 + 88P_2 = 8C_1$
$P_1 = 11C_2 - 8C_1$
i.e $\boxed{P_1 = -8C_1 + 11C_2}$

Now eq^n ② × 4 − eq^n ① × 3
$12P_1 + 32P_2 = 4C_2$
$12P_1 + 33P_2 = 3C_1$
$-P_2 = 4C_2 - 3C_1$
$\boxed{P_2 = 3C_1 - 4C_2}$

$P_1 = -8C_1 + 11C_2$
$P_2 = 3C_1 - 4C_2$

① AL $C_1 = A = 00$
$C_2 = L = 11$
$P_1 = 11(11) - 8(0) \overset{\text{zero}}{=} 121 \equiv 17 \pmod{26}$
$P_2 = 3(0) - 4(11) = -44 \equiv 8 \pmod{26}$
$P_1 = 17 = R$, $P_2 = 08 = I$

② XW $P_1 = G$, $P_2 = H$

③ UV $P_1 = T$, $P_2 = C$

④ AD $P_1 = H$, $P_2 = 0$

⑤ CO $P_1 = 24 = X$, $P_2 = 2 = C$

⑥ JO $P_1 = E$, $P_2 = X$

So, we get
RIGHT CHOICE X

i.e RIGHT CHOICEX.

Scanned with CamScanner

Ch-10

Public key Cryptosystem

(Conventional cryptographic system)

(1) In Caesar's cipher method, the sender & receiver jointly have a Secret key.

The sender uses the key to encrypt the plaintext to be sent
The receiver uses the same key to decrypt the cipher text.

(2) Public key Cryptography differs from Conventional cryptography in that it uses two keys, an encryption key and decryption key.

(3) A major advantage of public-key cryptosystem is that it is unnecessary for senders & receiver to exchange key in advance of their decision to communicate with each other.

RSA algorithm (Rivest, Shamir, Adleman)

2 keys — Private key
Public key.

M (message)

(1) choose two different large prime numbers p & q

(2) It is assumed that plaintext number (message) M < n where n = p·q (n is called enciphering modulus)

(3) If message is too long, then message is divide in blocks of digits say $M_1, M_2, \ldots M_s$ of appropriate size.
Each block is encrypted separately.

(4) calculate $\phi(n) = (p-1)(q-1)$

(5) Choose integer K such that gcd $(K, \phi(n)) = 1$

(6) calculate j, such that $Kj \equiv 1 \pmod{\phi(n)}$
(j is called recovery exponent)
(& K is called enciphering exponent)

Scanned with CamScanner

Encryption

$M^k \pmod n = r$ (say) → bbbbbb
(Ciphertext) (r is ciphertext number)

Decryption

$r^j \pmod n = M$ → (plaintext)
(main msg)

(Note) (n, k) → public key

(n, j) → private key

(Exp 10.3) Use RSA public key algorithm To encrypt message

NO WAY

$n = 1537$

(Soln) plain text NO WAY

1314 (99) 220024

(space)

(Next page proper solution)

Encryption process begin with M (message). Convert into numerical form, in which each letter, number or punctuation mark of plain text is replaced by two digit integer.

ie

A = 00	K = 10	U = 20	1 = 30
B = 01	L = 11	V = 21	2 = 31
C = 02	M = 12	W = 22	3 = 32
D = 03	N = 13	X = 23	4 = 33
E = 04	O = 14	Y = 24	5 = 34
F = 05	P = 15	Z = 25	6 = 35
G = 06	Q = 16	? = 26	7 = 36
H = 07	R = 17	. = 27	8 = 37
I = 08	S = 18	, = 28	9 = 38
J = 09	T = 19	0 = 29	! = 39

with 99 indicating a space between words.

(space) = 99

Scanned with CamScanner

10.3) Use RSA public key algorithm to encrypt message NO WAY
n = 1537

(Sol^n) plaintext NO WAY
13 14 99 22 00 24
coding for space

$n = 1537 = 29 \times 53$
$= p \times q$

$\phi(n) = (p-1)\times(q-1) = 28 \times 52 = 1456$

$\phi(n) = 1456$

131499220024 (too large so, blocks)

Each block is $< n = 1537$

131499220024 (as 1314 9922 0024 $\rightarrow$ 1537 so, not possible)

split M into blocks of three digit each.

first block 131

Now, choose K such $gcd(K, \phi(n)) = 1$
$gcd(K, 1456) = 1$

choose $K = 47$ so, $(n, K) = (1537, 47)$ is publickey $(1 < K < \phi(n))$

Now, Calculate j,

$Kj \equiv 1 \pmod{\phi(n)}$
$47j \equiv 1 \pmod{1456}$
$\Rightarrow j = 31$ (By chinese remainder thm.)

$(n, j) = (1537, 31)$ private key

first block 131

$M_1^K \pmod n$ i.e $131^{47} \pmod{1537}$

calculate $131^{47} \pmod{1537}$

i.e $131^{47} \equiv \underbrace{570}_{r} \pmod{1537}$

Second block $499^{47} \equiv 1222 \pmod{1537}$

we get 0570 1222 0708 1341

as n = 1537 (four digit)

Scanned with CamScanner

M = 1314992200 24 Encryption

↓ secret transmission

0570122207081341

→ r (for first block)

Decryption

$r^d \pmod n$ ie $570^{(\text{first block})/31} = 131 \pmod{1537}$

(Exam 10.1) (Q-12, 13)

(try as exercise)

Scanned with CamScanner