Ch-3

CRYPTOGRAPHY

→ Cryptography is the study of sending messages in disguished form so that only intended recipients can remove disguise and read message.

→ Message we want to send → Plain text
disguished Message → Eg Ciphertext

→ We use 'letter' (or character) which includes A-Z, numericals, blanks etc. to write the message.

→ Process of converting plaintext to ciphertext is called enciphering or Encryption.
and Reverse process is deciphering or decryption.

→ Plaintext and ciphertext are broken into Message units.
A message units might be → a single letter
→ a pair of letter (digraph)
→ triplet of letter (trigraph)
→ block of 50 letters

→ Encryption works as → it is a map f from the set $\mathcal{P}$ of all possible plaintext message units to set $\mathcal{C}$ of all possible ciphertext message unit.

→ decryption is basically f^{-1}.

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P$$

Such a set up is called cryptosystem.

→ First step of cryptosystem is to 'label' all message units.

Example → if our plaintext or ciphertext are single letters from A-Z, then we can label them using integers $0, 1, \ldots, 25$.

Ex-2 if our message units are digraphs in 27 letter alphabet consisting A-Z & blank, first consider blank as numerical equivalent 26 and then label the digraph whose 2 letter corresponds to $x, y \in \{0, 1, 2, \ldots, 26\}$ —

$$27x + y \in \{0, 1, \ldots, 728\}$$

Thus, we view individual letters as digits in base 27 and we view digraph as 2 digit integer in that base.

Ex → "NO" ⟶ $27 \cdot 13 + 14 = 365$

N O

→ Example – Suppose we are using 26 letter alphabet A-Z with numerical equivalent A-Z. Let letter $P \in \{0, 1, \ldots, 25\}$ as plaintext. function f is defined as

$$f(P) = \begin{cases} P+3 & x < 23 \\ P-23 & x \geq 23 \end{cases}$$

In other words, f simply adds 3 modulo 26.

$f(P) = P + 3 \bmod 26$.

→ The definition using Modular Arithmatic is easier to work with.

Thus, if Plaintext is "YES" then first convert to numbers 24 4 18,

then add 3 modulo 26 : 1 7 21 (P → 25 0 1 → 26)

translate back "BHV".

To decipher, we subtracts 3 modulo 26.

– Generalising this Example we get,

$$C \equiv P + b \bmod N \qquad , P = C - b \bmod N$$

⇒ Here b is called a key or enciphering key. (Parameter)

Ex ⇒ Suppose their is enciphered Message ex: "FQOCVDEM". we know that is was enciphered using shift transformation on single letters of 26 letters alphabet.
But we have to find b.
To we do that using 'frequency Analysis'.

→ Suppose we intercepted a long string of ciphertext we know that 'E' is most frequently occurring letter in English language. So it is reasonable to assume that most frequently Occurring letter in ciphertext is E.
Suppose that we find 'V' is most freq. occurring character.

That means the shift takes, 'E'=4 to 'V'=20
i.e., $20 = 4 + b \bmod 26$

$$\boxed{b = 16}$$

To diCipher Subtract b mod 26

FQOCVDEM' = 5 16 14 2 20 3 4 12 ⟷
15 0 24 12 4 13 14 22
= "PAYMENOW"

DRAWBACK :- We know that,
- there are only 26 possibilities for b, one can simply run through all of them. most likely only one will give Message that makes sense. and that 5 is encrypting key.
Thus it is so much easy to break.

→ A improvement is to use more general type of transformation of $\mathbb{Z}/N\mathbb{Z}$, called an affine map

$$C \equiv aP + b \bmod N$$

where a and b are fixed integers
(together they form enciphering key)

→ To decipher message which was enciphered by affine map method,

$C \equiv aP + b \bmod N$, $P \equiv a'C + b' \bmod N$

where a' is inverse of a modulo N

$b' = -a^{-1}b$.

Note, this works only if $\gcd(a, N) = 1$

Otherwise we will not get map to be 1-1 which was our basic definition.

→ Special Case when $b = 0$:

$P \equiv a \pmod N$, $C \equiv a^{-1}P \bmod N$

this case is called linear transformation meaning that map takes sum to a sum. i.e.

$C_1 \longrightarrow P_1$, $C_2 \longrightarrow P_2$

$C_1 + C_2 \longrightarrow P_1 + P_2$

Ex-3 Still working in 26 letter Alphabet, Suppose we know that 'X' → Most frequent character
'D' → 2nd most " "
It is reasonable to assume that these are the encryption of 'E' and 'T'.
Thus, replacing P and C in deciphering formula we obtain,

$$10a' + b' \equiv 4 \bmod 26$$
$$3a' + b' \equiv 19 \bmod 26$$

Subtracting them we get,

$$7a' \equiv 11 \bmod 26$$
$$\rightarrow a' \equiv 7^{-1} 11 \equiv 9 \bmod 26.$$

For b', $b' \equiv 4 - 10a' \equiv 18 \bmod 26$

So we get, $P \equiv 9C + 18 \bmod 26$

⇒ Sometimes after solving we can get Multiple values of a' and b' and they all can possible affine deciphering.
In that case we have to continue our frequency analysis and find out which one is correct.

Digraph transformation

→ Now, Our plaintext and ciphertext are 2-letter block, called digraph.

→ If Plaintext has odd number of letters. Then, we add extra letter at end as.
if P has blank in it then add blank.
else add 26 letter alphabet

→ As we seen before, we write digraph as
$x\ N + y$
where $x \rightarrow$ numerical Equivalent of 1st letter
$y \rightarrow$ " " " 2nd "
$N \rightarrow$ number of letters in alphabet

We think of digraph as 2-digit base-N integer

→ We define encryption of P to be non-negative integer less than N^2,

$$C = aP + b \bmod N^2$$

where $\gcd(a, N) = 1$

$$P = a'C' + b' \bmod N^2$$

where $a' \equiv a^{-1} \bmod N^2$
$b' \equiv -a^{-1} b \bmod N^2$

class notes
DATE
PAGE

Ex-5 → Suppose we are working in 26-letter alphabet and using digraph enciphering,

$C \equiv 159P + 580 \bmod 676$ ——(i)

$676 = N^2 \rightarrow N = 26$

Then digraph 'No' has

$13 \cdot 26 + 14 = 352$ ——(ii)

(numerical Equivalent)

Put (ii) in (i)

$C \equiv 159 \cdot 352 + 580$

$\equiv 440 \bmod 676$

$\rightarrow$ "84"

Ex-6 → Suppose 2 letters have numerical Equivalent as x and y, then digraph has numerical Equivalent as $27x + y$ (as before).
Suppose study of certain cipher tells that "ZA", "IA", 'IW' are most frequently occuring digraphs.
And in English most frequently occuring digraphs are 'E_', 'S_', '_T'. Then find deciphering key, and read "NDX BHo".

→ We know that, $C \equiv aP + b \bmod 729$ → enciphering key

for Enciphering,

for Deciphering, $P \equiv a'C + b' \bmod 729$ → deciphering key

After doing shifts from "G" → "ZA"
"S" → "IA"
"T" → "IW"

We get,

$675a' + b' \equiv 134 \mod 729$ — (i)
$216a' + b' \equiv 512 \mod 729$ — (ii)
$238a' + b' \equiv 721 \mod 729$ — (iii)

Now (i) − (iii)
$437a' \equiv 142 \mod 729$

To solve this we must find inverse of 437 mod 729,

By Euclidean Algorithm in detail,

$729 = 437 + 292$
$437 = 292 + 145$
$292 = 2 \cdot 145 + 2$
$145 = 72 \cdot 2 + 1$

and then

$1 = 145 - 72 \cdot 2$
$1 = 145 - 72(292 - 2 \cdot 145)$
$= 145 \cdot 145 - 72 \cdot 292$
$= 145(437 - 292) - 72 \cdot 292$
$= 145 \cdot 437 - 217 \cdot 292$
$= 145 \cdot 437 - 217(729 - 437)$
$= 362 \cdot 437 \mod 729$

Thus, $a' = 362 \cdot 142 \equiv 374 \mod 729$
then $b' = 647 \mod 729$

→ To read "ND XB HO"

Applying deciphering transformation,

→ 354 622 203

We obtain $365 = 13 \cdot 27 + 14$

$724 = 26 \cdot 27 + 22$

$24 = 0 \cdot 27 + 24$

We get "NO WAY"

⇒

2) Enciphering Matrices

→ In this section, we are using Vectors to send digraphs as our message unit.

Ex → if A-Z corresponds to 0-25

then digraph NO corresponds to Vector $\begin{pmatrix} 13 \\ 14 \end{pmatrix}$.

→ digraph P as a point on an $N \times N$ square array.

→ ~~hhh~~

→ We interpret an 'enciphering transformation' as a rearrangement of $N \times N$ array of points, an enciphering map is a 1-to-1 function from $(\mathbb{Z}/N\mathbb{Z})^2$ to itself.

→ Review of Linear Algebra

→ We now review how one works with vectors in real x-y plane & with 2×2 Matrices.

Given 2×2 array of numbers $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ★

a vector in plane $\begin{pmatrix} x \\ y \end{pmatrix}$

→ We can get new vector as,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

for a fixed matrix, this function from one vector to another vector is called linear transformation.

We can write it as, $AX = B$ —— (i)

where A is $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

X is vector of unknowns $\begin{pmatrix} x \\ y \end{pmatrix}$

B is vector of constants $\begin{pmatrix} e \\ f \end{pmatrix}$ → $e = ax+by$, → $f = cx+dy$

→ We can find X, by multiplying A^{-1} to both sides of eq (i)

$$X = A^{-1}B$$

→ Matrix A has inverse if and only if $D = ad-bc$ is nonzero, and

$$A^{-1} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$$

Linear Algebra Modulo N

→ The Difference when we work with $(\mathbb{Z}/N\mathbb{Z})^2$ rather than $\mathbb{Z}/N\mathbb{Z}$ is that now instead of an integer a we need 2×2 Matrix, denoted by A.

→ (in which order doesn't effect result)

→ Let R be any Commutative Ring, i.e., set with multiplication and addition satisfying same rules as in a field, except we do not require that any non zero element have multiplicative inverse

Ex → $\mathbb{Z}/N\mathbb{Z}$ is always a ring but it is not field unless N is prime

→ If R is Commutative Ring, we let $M_2(R)$ denote the set of all 2×2-matrices with entries in R.

We call $M_2(R)$ a "matrix ring over R";

↓

it is itself a ring but not commutative because in matrix multiplication order of factors makes difference

Now, we already know that, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has inverse if and only if $D \neq 0$,

$$A^{-1} = \begin{pmatrix} D^{-1}d & D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$$

→ We have similar situation when we work over an arbitary Ring R, suppose,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$$

and $D = det(A) = ad - bc$

Let D^{-1} denote the Multiplicative inverse of D then,

$$\begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} D^{-1}(ad-bc) & 0 \\ 0 & D^{-1}(ad-bc) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We obtain same result,

Thus A has an inverse matrix given by same formula as in real number,

$$A^{-1} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}$$

Ex→ Find inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\mathbb{Z}/26\mathbb{Z})$

→ $D = 2 \cdot 8 - 3 \cdot 7$

$= -5$

$\equiv$ which is 21 in $\mathbb{Z}/26\mathbb{Z}$ Since $\gcd(21, 26) = 1$,

D has an inverse, $D^{-1} = 21^{-1} = 5$,

$\therefore A^{-1} = \begin{pmatrix} 5 \cdot 8 & -5 \cdot 3 \\ -5 \cdot 7 & 5 \cdot 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -36 & 10 \end{pmatrix}$

$= \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}$

→ To solve Equations (when Matrix is not invertible) is to eliminate one of variables by Subtracting.

→ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $D = ad - bc$ $\gcd(D, N) = 1$

each of plaintext message unit $P = \begin{pmatrix} x \\ y \end{pmatrix}$ is taken to ciphertext $\begin{pmatrix} x' \\ y' \end{pmatrix}$ by rule

$C = AP$ i.e. $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

To decipher, take inverse Matrix

$P = A^{-1} AP = A^{-1} C$

i.e., $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$

Ex→ Given 26 letter alphabet, use matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$, to encipher Message 'NO'.

→ $C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix}$

$= \begin{pmatrix} 68 \\ 203 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix}$

⇒ Suppose if we are not given the "key" → i.e., Matrix A and A^{-1} (deciphering). But we were able to determine $C_1 = AP_1$ and $C_2 = AP_2$.

To solve for A and A^{-1}, we put 2 columns of P_1 and P_2 together into 2×2 matrix P similarly for ciphertext columns.

$$C = AP$$

multiplying P^{-1} both sides

$$APP^{-1} = A = CP^{-1}.$$

Similarly, $A^{-1} = PC^{-1}$

Ex⇒ Suppose we have 2×2 enciphering matrix with 29 letter Alphabet as A-Z → 0, 1, 2 - -, 25
blank = 26, ? = 27, ! = 28
We receive message as

GFPYJP_X?UYXSTLADPLW

Suppose we know last 5 letters of plaintext as 'KARLA'. We use 4 letters of this plaintext because we don't have 6th letter.
Thus,

DP → AR
LW → LA

→ We know; $C = A^{-1}B$

$$P = A^{-1}C$$

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} = A^{-1} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 13 \\ 23 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}$$

→ full plain text,

$$P = A^{-1}C$$

$$P = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15 & 9 & 26 & 27 & 24 & 18 & 11 & 3 & 11 \\ 5 & 24 & 15 & 23 & 30 & 23 & 19 & 0 & 15 & 12 \end{pmatrix}$$

$$= \begin{pmatrix} 18 & 17 & 10 & 26 & 19 & 13 & 14 & 28 & 0 & 11 \\ 19 & 8 & 4 & 0 & 26 & 14 & 13 & 10 & 17 & 0 \end{pmatrix}$$

= "STRIKE AT NOONI[illegible]AKLA"

xxx xxx