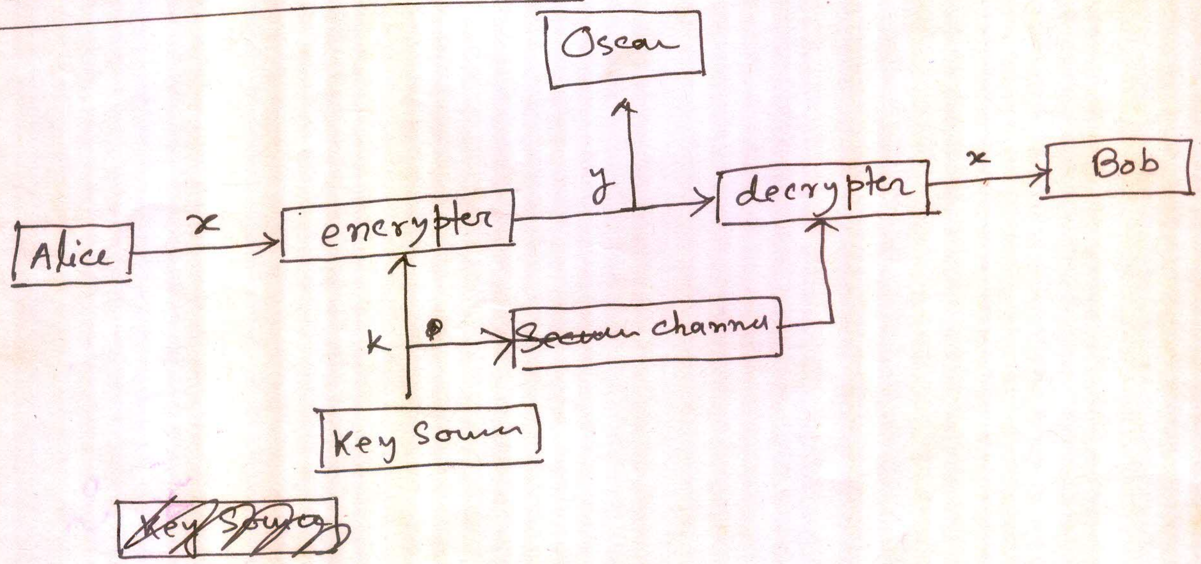
Introduction to classical cryptography

- Cryptography is the science or art of secret writing
- The fundamental objective of cryptography is to enable two people (Alice & Bob) to communicate over an insecure channel in such a way that an opponent (Oscar) cannot understand what is being said.

- Plaintext → the information that alice wants to send to Bob
- Alice encrypts the plaintext, using a predetermined key, & send the resulting ciphertext to Bob over the public channel.

- Upon receiving the ciphertext
  - Oscar cannot determine what the plaintext was
  - But Bob knows the encryption key, can decrypt the ciphertex & get the plaintext.

The communication channel



- Cryptology $\rightarrow$ Cryptography + Cryptanalysis.
  - Cryptography: Art of converting information to a form that will be unintelligible to an unintended receipent; carried out by cryptographer.
  - Cryptanalysis: Art of breaking cryptographic systems; carried out by cryptanalyst.

- Two main types of cryptography in use today:
  - Symmetric key or secret key cryptography
  - Asymmetric key or public key cryptography.

Def^n. A cryptosystem is a five tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

(i) $\mathcal{P}$ is a finite set of possible plaintexts;

(ii) $\mathcal{C}$ is a finite set of possible ciphertexts;

(iii) $\mathcal{K}$, the keyspace, is a finite set of possible keys;

(iv) for each $k \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every plaintext $x \in \mathcal{P}$.

- A practical cryptosystem should satisfy
  - each encryption function e_K & each decryption function d_K should be efficiently computable
  - an opponent, upon seeing the ciphertext string y, should be unable to determine the key K that was used, or the plaintext string x.

- The process of attempting to compute the key K, given a string of ciphertext y, is called cryptanalysis
  - if opponent can determine K, then he can decrypt y just as Bob would, using d_K.
  - determining K should be as difficult as determining the plaintext string x, given the ciphertext string y.

The Caesar Cipher

Shifting each plaintext letter 3 letters down in the alphabet

Example

Plaintex : i came, i saw, i conquered

in lower case

(Omitting spaces and commas)

Ciphertex : LFDPHLVDZLFRQTXHUHG

in upper case

& recycling back to the beginning of the alphabet when we pass Z.

intended ~~receip~~ recipient would simpley need to shift each ciphertext letter backward 3 letters.

The Caesar Cipher

a	b	c	d	e	f	.....	v	w	x	y	z	plaintex
↓	↓	↓	↓	↓	↓		↓	↓	↓	↓	↓	
D	E	F	G	H	I		Y	Z	A	B	C	CIPHERTEXT

Exercise Find the ciphertext for the plaintext message: "Meet the iceman at noon", using Caesar Cipher.

Exercise The following ciphertext was encrypted using the Caesar Cipher:

PHHWPHDIWHUWKHSDUWB

Find the original plaintext message.

The Shift Cipher

- $\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$
- for $K \in \mathcal{K}$, $0 \leq K \leq 25$

$$e_K(x) = x + K \mod 26 \quad \text{for } x \in \mathcal{P}$$

$$d_K(x) = y - K \mod 26 \quad \text{for } y \in \mathcal{C}.$$

- The Caesar cipher is a particular case of the shift cipher with $k = 3$.

Example

- Plaintext → ordinary English text
- Correspondence between alphabetic characters & integers:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	2

- $K = 11$
- Plaintext → we will meet at midnight.

Convert the seq. of int.s to alphabetic characters.

- Corresponding sequence of integers →

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

Subtract 11 from each value (reducing modulo 26)

- Add 11 (key) to each value (reducing modulo 26) →

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

- Convert the sequence of integers to alphabetic characters:

Convert the ciphertext to seq. of int.s

- Ciphertext →

HPHTWWXPPELEXTOYTRSE

- Decryption →

Shift Cipher is not Secure

- Bruit-force cryptanalysis easily performed on the shift cipher by trying all 25 possible keys. (Exhaustive key search)
- Given a ciphertext string, Oscar successively try the decryption process with $k = 0, 1, 2, \ldots$ until get a meaningful text.

- Ciphertext →

JBCRCLQRWCRVNBJENBWRWN

~~K=0 → JBCRCLQRWCRVNBJENBWRWN~~

~~K=1 → KCDSDMRSXDSWOCKFOCXSXO~~

~~K=1 →~~

- k=0 → jbcrclqrwcrvnbjenbwrwn

  k=1 → iabqbkpqvbqumaidmavqvm

  k=2 → hzapajopuaptlzhclzupul

k=0 →	j	b	c	r	c	l	q	r	w	c	r	v	n	b	j	e	n	b	w	r	w	n
k=1 →	i	a	b	q	b	k	p	q	v	b	q	u	m	a	i	d	m	a	v	q	v	m
k=2 →	h	z	a	p	a	j	o	p	u	a	p	t	l	z	h	c	l	z	u	p	u	l
k=3 →	g	y	z	o	z	i	n	o	t	z	o	s	k	y	g	b	k	y	t	o	t	k
k=4 →	f	x	y	n	y	h	m	n	s	y	n	r	j	x	f	a	j	x	s	n	s	j
k=5 →	e	w	x	m	x	g	l	m	r	x	m	q	i	w	e	z	i	w	r	m	r	i
k=6 →	d	v	w	l	w	f	k	l	q	w	d	p	h	v	d	y	h	v	q	l	q	h
k=7 →	c	u	v	k	v	e	j	k	p	v	k	o	g	u	c	x	g	u	p	k	p	g
k=8 →	b	t	u	j	u	d	i	j	o	u	j	n	f	t	b	w	f	t	o	j	o	f
$\boxed{k=9}$ →	a	s	t	i	t	c	h	i	n	t	i	m	e	s	a	v	e	s	n	i	n	e

- The key is $k = 9$

7

Exercise (a) Find the ciphertext for the plaintext message "Meet the iceman at noon", using the shift cipher with a shift of 12 letters down the alphabet.

(b) The following ciphertext was encrypted using the shift cipher of part (a):

VQZWUZEUEMFGDZOAMF

Find the original plaintext message.

The Affine Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
- $\mathcal{K} = \{ (a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a,26) = 1 \}$.

  required for $a \in \mathbb{Z}_{26}$ to have its multiplicative inverse a^{-1}.
- for $k = (a,b) \in \mathcal{K}$,

$$e_K(x) = ax + b \mod 26 \quad , \quad x \in \mathbb{Z}_{26}$$

affine functions

$$d_K(x) = a^{-1}(y-b) \mod 26 \quad , \quad y \in \mathbb{Z}_{26}.$$

- Note: we want the congruence

$$ax + b \equiv y \pmod{26} \quad \text{or} \quad ax \equiv y - b \pmod{26}$$

to have unique soln. for x.

$$y \in \mathbb{Z}_{26} \Rightarrow y - b \in \mathbb{Z}_{26}$$

So it is sufficient to study the congruence

$$ax \equiv y \pmod{26} \quad , \quad y \in \mathbb{Z}_{26}.$$

- Theorem: The congruence $ax \equiv b \pmod m$ has a unique soln. $x \in \mathbb{Z}_m$ for every $b \in \mathbb{Z}_m$ iff $\gcd(a,m) = 1$.

- Defn. $\phi(m)$ = # of integers in $\mathbb{Z}_m$ that are relatively prime to m.

  ($\phi \to$ Euler's phi function)

  a, m relatively prime if $\gcd(a,m) = 1$ when $a \geq 1$ & $m \geq 2$ are integers.

<u>Theorem</u>: Suppose $m = \prod_{i=1}^{n} p_i^{e_i}$

when p_i's are distinct primes & $e_i > 0, 1 \le i \le$

Then $\phi(m) = m \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)$

<u>$m = 26$</u> $\phi(m) = \phi(26) = \phi(13 \times 2)$

$= 26\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{2}\right)$

$= \cancel{26}^{2} \times \frac{12}{\cancel{13}} \times \frac{1}{\cancel{2}} = 12.$

$\left| \{ a \in \mathbb{Z}_{26} \text{ s.t. } \gcd(a, 26) = 1 \} \right| = \phi(26) = 12.$

$a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$

exclude multiples of 2 & multiples of 13.

$e_K(x) = ax + b \mod 26.$

$a, b \in \mathbb{Z}_{26}$

$\gcd(a, 26) = 1$

12 26.

$K = (a, b) \in \mathcal{K}$

$\therefore |\mathcal{K}| = 12 \times 26 = 312$ possible keys.

too small to be secure.

<u>Note</u>

# of keys in the Affine Cipher over $\mathbb{Z}_m$ is $m\phi(m)$.

$K = (a, b) \in \mathcal{K} = \mathbb{Z}_m$, $a, b \in \mathbb{Z}_m$

$\gcd(a, m) = 1$

$\phi(m)$ m $\boxed{\text{Need to find } a^{-1} \bmod m}$

$60 = 3 \times 2^2 \times 5$

$|\mathcal{K}| = m\phi(m).$

<u>Example</u> <u>$m = 60$</u> $\longrightarrow \phi(60) = 60\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = \cancel{60}^{2} \times \frac{2}{\cancel{3}} \times \frac{1}{\cancel{2}} \times \frac{4}{\cancel{5}} = 16$

$|\mathcal{K}| = 60 \times 16 = 960$

Example $\quad K = (7,3) \quad \gcd(7,26) = 1.$

$7^{-1} \bmod 26 = 15$

$y = e_K(x) = 7x+3 \quad , x \in \mathbb{Z}_{26}$

$d_K(y) = 7^{-1}(y-3) = 15y - 19$

$\frac{45}{26}$
19

$= 7^{-1}(7x+3-3)$

$= 15$

$d_K(e_K(x)) = d_K(7x+3)$

105

$= 15(7x+3) - 19 = x + 45 - 19 = x \bmod 26$

$= \cancel{x + 45 - 19}$

Plaintext:

hot

a	b	c	d	...
0	1	2	3	...

$\downarrow$

7 14 19

Encryption

$7 \times 7 + 3 \bmod 26 = 52 \bmod 26 = 0 \to t$

$14 \times 7 + 3 \bmod 26 = 101 \bmod 26 = 23$

$19 \times 7 + 3 \bmod 26 = 136 \bmod 26 = 6.$

0 23 6

$G \to 15 \times 6 - 19 \bmod 26$
$= 12 - 19 \bmod 26$
$= -7 \bmod 26$
$= 19 \bmod 26$

3×59, 52, 17; 90, 78, 12

34, 26, 8

5×69, 52, 17; 85, 78, 7

$312 - 26 \cdot 306$

Ciphertext:

A X G.

Exhaustive search

$26 \phi(26) = 26 \times 12 = 312$

Decryption

$A \to 15 \times 0 - 19 \bmod 26 = -19 \bmod 26 = 7 \bmod 26 \to h$

$X \to 15 \times 23 - 19 \bmod 26 = 67 \bmod 26 = -12 \bmod 26 = 14 \bmod 26 \to 0$

~~$6 \times 23 - 19 \bmod 26 = (-17)(-19) \bmod 26 = \ldots \bmod 26 =$~~

The Substitution Cipher

- $\mathcal{P} = \mathcal{C}$ = Set of 26-letter English alphabet

  $\mathcal{P} = \{a, b, c, \cdots, y, z\}$

  $\mathcal{C} = \{A, B, C, \cdots, Y, Z\}$.

- $\mathcal{K}$ = set of all possible permutations of 26 alphabetic characters.
- for each permutation $\Phi \in Z$,

  $e_{\Phi}(x) = \Phi(x)$ for $x \in \mathcal{P}$

  $d_{\Phi}(y) = \Phi^{-1}(y)$ for $y \in \mathcal{C}$, where Φ^{-1} is the inverse permutation of Φ.

__Example:__

- Encryption function is the permutation Φ:

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

$e_{\Phi}(a) = X$, $e_{\Phi}(b) = N$, etc.

- Decryption function is the inverse permutation Φ^{-1}:

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
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

- Key: $K = \Phi$
- Ciphertext: MGZVYZLGHCMHJMYXSNHAHYCDLM HA
- Plaintext: find the plaintex???

this ciphertext can be decrypted.

- Monoalphabetic cipher : Each alphabetic character is mapped to a unique alphabetic character.

- We use arbitrary monoalphabetic substitution, ~~so~~ in the substitution cipher, so there are $\lfloor 26 = 4 \times 10^{26} \approx 2^{88}$ possible permutations, which is a very large number.

- Thus Bruit force is infeasible

- However, we will see later that a substitution Cipher is insecure against frequency analysis.

- Note : The Shift cipher is a special case of the substitution cipher which includes only 26 of the $\lfloor 26$ possible permutations of 26 elements.

(*)

- Polyalphabetic cipher : Uses different monoalphabetic substitutions while moving through the plaintext.

- The vigenere Cipher is polyalphabetic as explained next.

(*) Note : The Affine Cipher is a special case of the Substitution cipher which include ~~only~~ only $\phi(26) \times 26 = 12 \times 26 = 312$ possible ~~keys~~ permutations of the $\lfloor 26$ possible permutation of 26 elements

$ax+b$

possible choices of a

possible choice of b

$\underline{ax+b}$

The Vigenere Cipher

- $m \to$ a fixed positive integer
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
- for $K = (k_1, k_2, \ldots, k_m) \in \mathcal{K}$,

$|\mathcal{K}| = 26^m$
exhaustive search requires long time.
$m=5$
$|\mathcal{K}| > 1.1 \times 10^7$
ES by hand impractical (but not by computer)

$$e_K(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

$$d_K(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$$

- all operations are performed modulo $\mathbb{Z}_{26}$.

Example:

- Correspondence between alphabetic characters and integers:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- $m = 5$
- Keyword is 'money', this corresponds to the numerical equivalent $K = (12, 14, 13, 4, 24)$
- Plaintext : vive la france
- Keyword : mone ym oneymo
- Encryption : add modulo 26.

Plaintext :	21	8	21	4	11	0	5	17	0	13	2	4
Keyword :	12	14	13	4	24	12	14	13	4	24	12	14
Add modulo 26	$\cancel{33}$ 7	22	$\cancel{34}$ 8	8	$\cancel{35}$ 9	12	19	$\cancel{30}$ 4	4	$\cancel{37}$ 11	14	18
Ciphertext :	H	W	I	I	J	M	T	E	E	L	O	S

- Decryption : Use the same keyword, but now subtract modulo 26 instead of adding.

- <u>Note</u> : In a vigenere Cipher having keyword length m, an alphabetic character can be mapped to one of m possible alphabetic characters (assuming that the keyword contains m distinct characters).

- The Vigenere Cipher is thus polyalphabetic
- Cryptanalysis is more difficult for polyalphabetic than monoalphabetic cryptosystems.

- The Hill cipher is another polyalphabetic cipher that we will discuss next.

The Hill cipher

- m some fixed positive integer
- $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
- $\mathcal{K} = \{ m \times m$ invertible matrices over $\mathbb{Z}_{26} \}$.
- for a key K, we define

$$e_K(x) = xK$$

$$d_K(y) = yK^{-1}$$

where all operations are performed in $\mathbb{Z}_{26}$.

~~Example~~:

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

a	b	c	d	u	v	w	x	y	z
0	1	2	3	20	21	22	23	24	25

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

$26 \,|\, 193 \,|\, 7 \ldots$, 188, $11 \ldots$

- Plaintext: july

$26 \,|\, 212 \,|\, 8$, 208, 4 $\qquad$ $26 \,|\, 159 \,|\, 6$, 156, 3

ju $\quad$ ly

9 20 $\quad$ 11 24

$26 \,|\, 256 \,|\, 9 \ldots$, 234, 22 $\qquad$ $26 \,|\, 86 \,|\, 3$, 78, 8

- Encryption:

$$(9, 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99+60 \quad 72+140) = (159, 86) = (3, 8)$$

$\downarrow$

~~CD~~ DE

$$(11 \ 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121+72 \quad 88+168) = (193 \quad 256)$$

$= (11, 22) \to$ LW

- ciphertext: DELW

Example: Use the Hill cryptosystem with encoding matrix $K = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ to encrypt the message 'code blue alert'.

Note that $\det K = 1 \equiv 1 \pmod{26}$; so the matrix K is invertible $\pmod{26}$ & is thus a legitimate matrix.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

code blue alert → plaintext

↓ corresponding $\mathbb{Z}_{26}$ vector

2 14 3 4 1 11 20 4 0 11 4 17 19 13 → padded

46 − 26 = 20; 52 − 52; 77 − 52 = 25

mod 26

1×2, 2×2, $=1\times 2$

2+28, 2+42; 30, 44; 4, 18.

2+14=16. 4+42=46.

$$(2\ 14)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (2+14 \quad 4+42) = (16 \quad 46) = (16 \quad 20) \to QU$$

$$(3\ 4)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (3+4 \quad 6+12) = (7 \quad 18) \Rightarrow HS$$

$$(1\ 11)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (1+11 \quad 2+33) = (12 \quad 35) = (12 \quad 9) \to MJ$$

$$(20\ 4)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (20+4 \quad 40+12) = (24 \quad 52) = (24 \quad 0) \to YA$$

$$(0\ 11)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (11 \quad 33) = (11 \quad 7) \to LH$$

$$(4\ 17)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (4+17 \quad 8+51) = (21 \quad 59) = (21 \quad 7) \to VH$$

$$(19\ 13)\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = (19+13 \quad 38+39) = (32 \quad 77) = (6 \quad 25) \to GZ$$

QU HS MJ YA LH VH GZ

plaintext :	c	o	d	e	b	l	u	e	a	l	e	r	t	n
plaintext in $\mathbb{Z}_{26}$:	2	14	3	4	1	11	20	4	0	11	4	17	19	13
Ciphertext in $\mathbb{Z}_{26}$:	16	20	7	18	12	9	24	0	11	7	21	7	6	25
ciphertext :	Q	U	H	S	M	J	Y	A	L	H	V	H	G	Z

$\Rightarrow$ polyalphabetic cipher.

Exercise

The following ciphertext was encrypted using the Hill cipher using the encoding matrix

$$K = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

TARIDW XGXWNUANFHHU

Decode this message.

The Transposition / Permutation cipher

- m a positive integer
- $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
- $\mathcal{K}$ = set of all possible permutations of $\{1, 2, \ldots, m\}$
- For each permutation $\pi \in \mathcal{K}$

$$e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)}), \quad (x_1, \ldots, x_m) \in \mathcal{P}$$

$$d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}), \quad (y_1, \ldots, y_m) \in \mathcal{C}.$$

where π^{-1} is the inverse permutation of π.

Example

- $m = 6$
- key is the following permutation π:

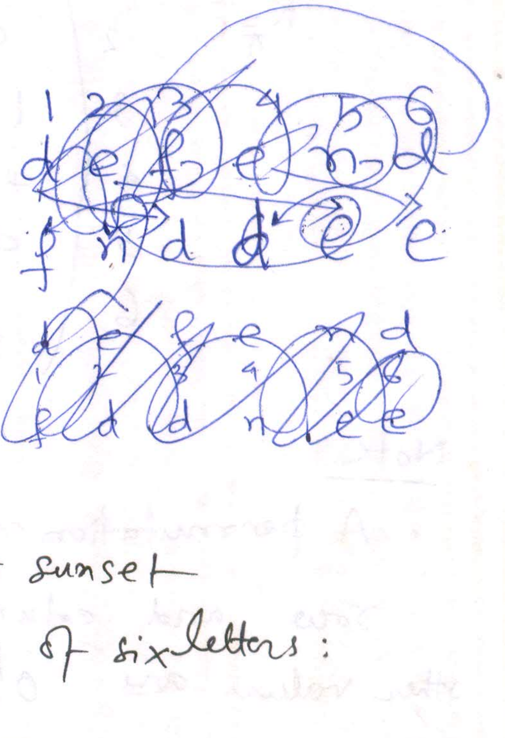
x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

$x \to$ d e f e n d (1 2 3 4 5 6)

f n d d e e (3 5 1 6 4 2)

- inverse permutation π^{-1}

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4



- plaintext: defend the hilltop at sunset

  partition the plaintext into groups of six letters:

  defend thehil ltopat sunset

- rearrange according to π:

  fnddee eitlhh oaltpt nestsu

- Ciphertext: FNDDEEEITLHHOALTPTNESTSU

• Decryption can be done using π^{-1}

- The Permutation Cipher is a special case of the Hill cipher.

- Given a permutation π of the set $\{1, 2, \ldots, m\}$, we can define an associated $m \times m$ permutation matrix $K_\pi = (k_{ij})$ as:

$$k_{ij} = \begin{cases} 1 & \text{if } i = \pi(j) \\ 0 & \text{otherwise} \end{cases}$$

$$K_\pi = \begin{array}{c|cccccc} j \downarrow \; i \rightarrow & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$

π :

1	2	3	4	5	6
3	5	1	6	4	2

π^{-1}

1	2	3	4	5	6
3	6	1	5	2	4

$$K_{\pi^{-1}} = \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 & 0 \\ 6 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}$$

<u>Note</u>

- A permutation matrix is a matrix in which every row and column contains exactly one '1' and all other values are '0'.
- A permutation matrix can be obtained from an identity matrix by permuting rows or columns.
- $K_\pi^{-1} = K_{\pi^{-1}}$

Playfair

Cryptanalysis

- Bruit-force cryptanalysis easily performed on the shift cipher by trying all 25 possible keys.
- Three characteristics of the problem facilitate the successful use of the bruit force approach
  - (i) the encryption scheme is known
  - (ii) there are only a limitted number of keys
  - (iii) the plaintext is easily recognisable.
- Most cases, key size tends to be the main problem for bruit-force attacks.

~~Monoalphabetic ciphers~~ :

- If instead of using only the 25 possible keys, arbitrary substitution is used as in the substitution cipher (monoalphabetic), then there are $\lfloor 26$ or $4 \times 10^{26} \approx 2^{88}$ possible keys & hence bruit-force is infeasible.
- We now show the frequency analysis on the substitution cipher.

Frequency Analysis

- Suppose we have a long ciphertext, the challenge is to decipher it
- let we know the text is in English and has been encrypted using a monoalphabetic substitution cipher.
- searching all possible keys is impractical as the keyspace is of size 26!.
- In English, e is the most common letter, followed by t, then a, and so on

	P
e →	.127
t →	.091
a →	.082
o →	.075
i →	.070
n →	.067
s →	.063
h →	.061
r →	.060
⋮	
v →	.01
k →	.008
J →	.002
x, Q, z →	.001

- Examine the ciphertext in question, and work out the frequency of each letter
- If most common letter in the ciphertext is, for example, J, then it would seem likely that this is a substitution for e.
- If the second most common letter in the ciphertext is P, then this is probably a substitution for t, & so on.
- However, regularities of the language may be exploited, e.g. relative frequency.
- frequency analysis requires logical thinking, intution, flexibility and guesswork.

- Homophones : Assigning more than one ciphertext symbol to each plaintext.

- Still flawed because of digraphs

- Two methods are used in substitution cipher to lessen the extent to which the structure of the plaintext survives in the ciphertext.

  (i) Multiple letter encryption : (e.g. The Playfair Cipher)

  (ii) Polyalphabetic ciphers : Using different monoalphabetic substitutions while moving through the plaintext. (e.g. The Vigenere Cipher)

The Playfair Cipher (Multiple letter encryption)

- Use the keyword CHARLES (Charles Wheatstone invented the cipher)
- Draw up a 5×5 matrix with the keyword first, removing any repeating letters as follows:

c	h	a	r	l
e	s	b	d	f
g	i/j	k	m	n
o	p	q	t	u
v	w	x	y	z

- Plaintext : → meet me at the bridge
  - split the sentence into digrams removing spaces, 'x' used to make even number of letters :

    → me et me at th eb ri dg ex

  - Repeating plaintext letters that are in the same pair are seperated with a filler letter, such as 'x':

    ~~balloon → ba lx ox ox~~

    'balloon' would be treated as

    ↓

    ba lx lo on

- Two plaintext letters in the same row are each replaced by the letter to the right, with the first element of the row circularly following the last.

eb is replaced by sd

ng is replaced by gi (or gj as preferred)

- Two plaintext letters that fall in the same column are each replaced by letters beneath, with the top element of the column circularly following the last.

dt would be replaced by my

ty would be replaced by yr.

- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

me becomes gd

me et me at th eb ri dg ex

- Ciphertext therefore is:

GD DO GD RQ ~~AR~~ PR SD HM EM BV

Exercise The playfair cipher is used with keyword 'basketball' to encrypt the message 'the iceman will arrive at midnight'. Find the ciphertext.

(Ans: LGSNFSHKHZHCHLQYQMZBBLNMFMMHGL)

- The playfair cipher is more secure that the Substitution cipher
- However the playfair cipher is also ~~s~~ susceptible to ciphertext-only ~~ciphertext - only attacks~~ attacks by doing statistical frequency counts of pair of letters
- each pair of letters will always get encrypted in the same fashion.
- ~~small~~ short keywords make the Playfair cipher much easier to crack
- Significantly larger portion of ciphertext would be required for cryptanalysis on the Playfair cipher
- ~~distinction~~ there are $26^2 = 676$ ordered pairs of letters & the distinctions are less pronounced than those for single-letter statistics.

Ref:

- Menezes, Oorschot, Vanstone - Handbook of Applied Cryptography
- Douglas R. Stinson cryptography: Theory & Practice, first/2nd/Third edi, CRC press
- W. Stallings Cryptography & Network Security - Principles & Practice, Prentice Hall 3rd/4th. ed.
- A. Stanoyevitch - Intro. to cryptography with math. foundations & Comp. Imp., CRC press

Transposition Techniques

(*) - For this type of column ~~transp~~ transposition, cryptanalysis is fairly straightforward ~~& involves~~ - laying out the ciphertext in a matrix & playing around with column positions. Digram & trigram frequency table can be useful.

- rail fence technique

<u>Example</u>

meet me after the party (plaintext)

```
m   e   m   a   t   r   h   p   r   y
  e   t   e   f   e   t   e   a   t
```

(rail fence of depth 2
read off rows)

MEMATRHPRYETEFETEAT (ciphertext)

- write message in a rectangle, row by row, read off column by column, but permute the order of the columns.
- order of the columns becomes key

<u>Example</u> (4x7 rectangle)

attack postponed until two am (plaintext)

Key :	4	3	1	2	5	6	7
plaintext :	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

4	3	1	2	5	6	7
T	T	N	A	A	P	T
M	T	S	U	O	A	O
D	W	C	O	I	X	K
N	L	Y	P	E	T	Z

ciphertext : TTNAAPTMTSUOAODWCOIXKNLY PETZ

- Pure Transposition cipher is easily recognized as it has the same letter frequency as the original plaintext. (*)
- To make it significantly more ~~complex~~ secure, one can perform more than one stage of transposition.

Key: 4 3 1 2 5 6 7

Input :

t	t	n	a	a	p	t
m	t	s	u	o	a	o
d	w	c	o	i	x	k
n	l	y	p	e	t	z

Output : NSCYAUOPTTWLTMDNAOIE PAXTTOKZ

Original plaintext → 1 2 3 4 28

Key:	4	3	1	2	5	6	7
	a	t	t	a	c	k	p
	1	2	3	4	5	6	7
	o	s	t	p	o	n	e
	8	9	10	11	12	13	14
	d	u	n	t	i	l	t
	15	16	17	18	19	20	21
	w	o	a	m	x	y	z
	22	23	24	25	26	27	28

3 10 17 24 4 11 18

25 2 9 16 23 18 15

16 23 18 15 ~~23~~

5 12 19 26 6

After first transposition

3 10 17 24 | 4 11 18 25 | 2 9 16 23 | 1 8 15 22

AP → CD. = 7

5 12 19 26 | 6 13 20 27 | 7 14 21 28

→ much more difficult to cryptanalyzed.

After 2nd transposition

Key:	4	3	1	2	5	6	7
	3	10	17	24	4	11	18
	25	2	9	16	23	1	8
	15	22	5	12	19	26	6
	13	20	27	7	19	4	28

less structured permutation ↔ has somewhat regular structure

17 9 5 27 24 16 12

7 10 2 22 20 3 25

15 13 4 23 19 14 11

1 26 9 18 8 6 28

Corresponding Transposition / Permutation Cipher

key → 4 3 1 2 5 6 7

mean

permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 2 & 1 & 5 & 6 & 7 \end{pmatrix}$

permutation matrix

$3 = \pi(1)$

$\rightarrow K_\pi = (k_{ij})_{7 \times 7}, \quad k_{ij} = \begin{cases} 1 & \text{if } i = \pi(j) \\ 0 & \text{o.w.} \end{cases}$

$$K_\pi = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} & & & 1 & & & \\ & & 1 & & & & \\ 1 & & & & & & \\ & 1 & & & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix} \end{array}$$

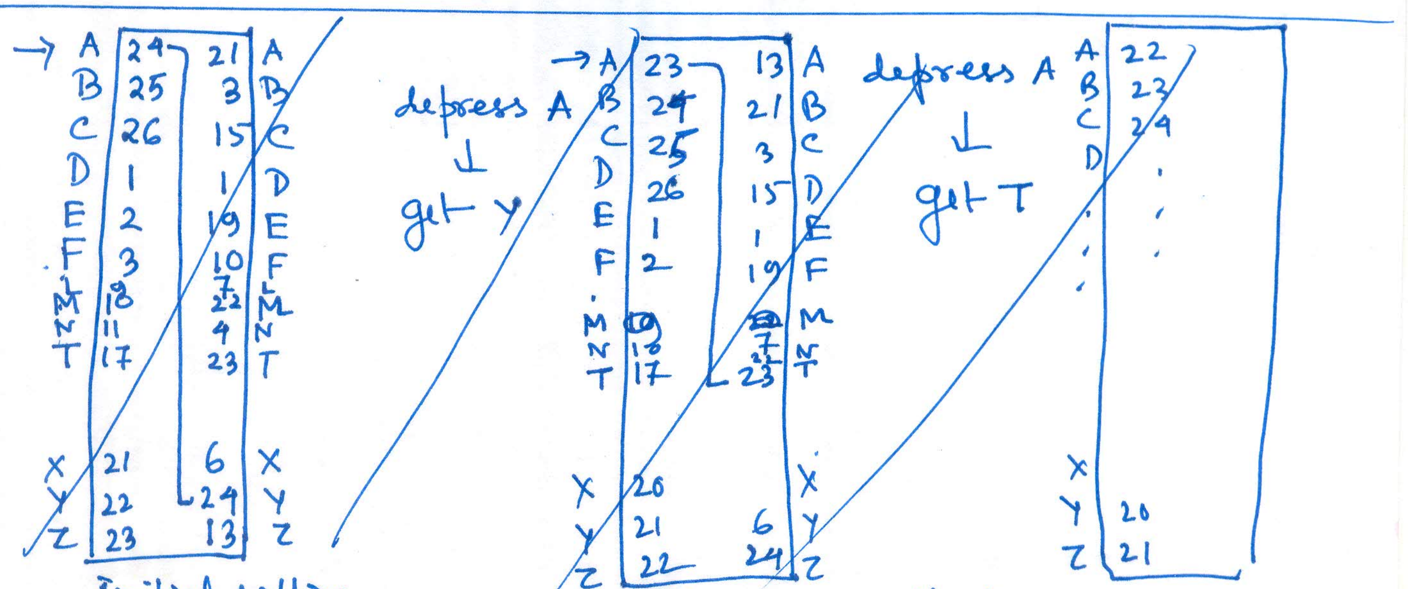
$y = xK$

	3	4	2	1	5	6	7
= row permutation →	t	a	t	a	c	k	p
→	t	p	s	o	o	n	e
→	n	t	u	d	i	l	t
→	a	m	o	w	x	y	z

Read columnwise

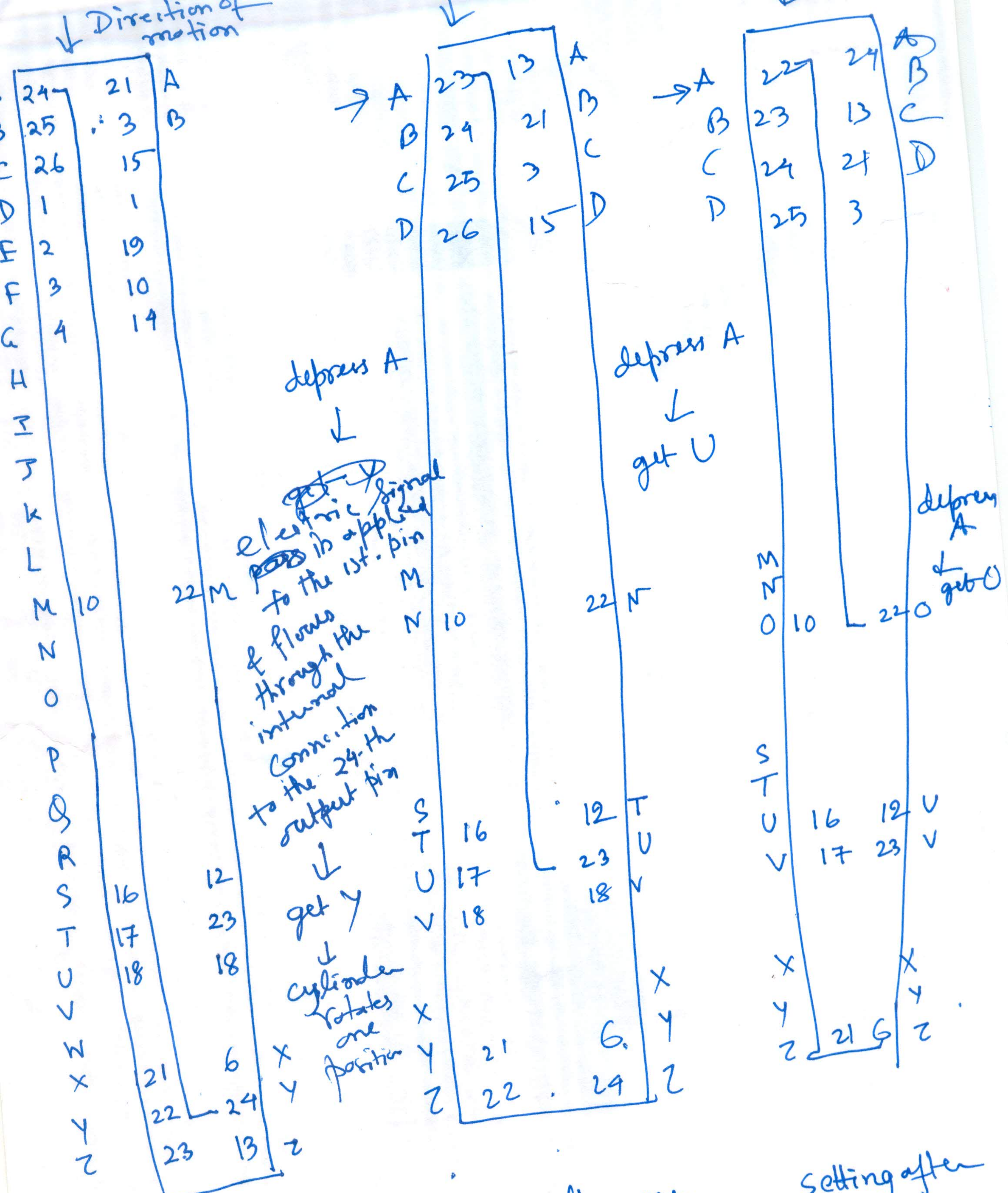
Rotor Machine

- ~~~~ uses multiple stages of encryption
  (thereby, significantly more difficult to cryptanalyze)
- Machines based on rotor principle
  ~~~~ used by both Germany (Enigma) & Japan (Purple) in World War II ~~~~
  ↳ breaking of both ~~~~ has a significant ~~outcome~~ factor of War's outcome
- Machine consists of a set of independent rotating cylinders through which electrical pulses can flow.
- Each cylinder has 26 input pins & 26 output pins with internal wiring that ~~~~ connects each input pin to a unique output pin.
- Each input & output pin is associated with a letter of the alphabet
- Single cylinder defines a monoalphabetic substitution.



Initial setting

after one keystroke
  ~~~~



initial setting

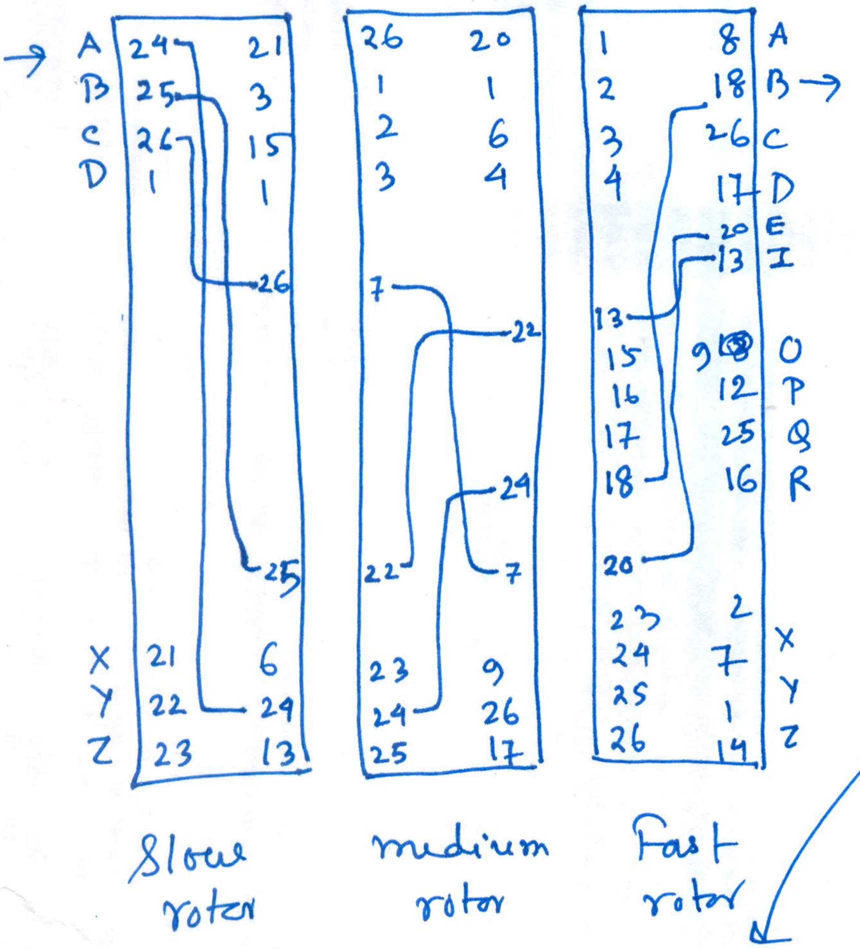
setting after one key stroke

setting after 2nd. keystroke.

- Single cylinder system does not present a formidable cryptanalytic task.

3 rotors

↓ direction of motion

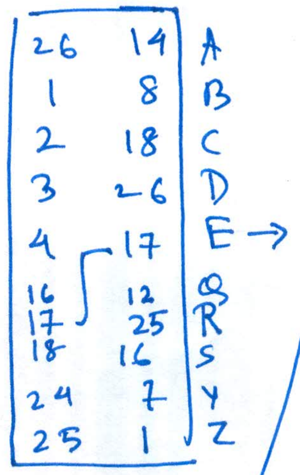


- 4 rotors results in periods of 456,976 letters
- 5 letters results in periods of 11,881,376 letters
- rotor machine points to the way to the most widely used cipher DES (Data Encryption Standard)

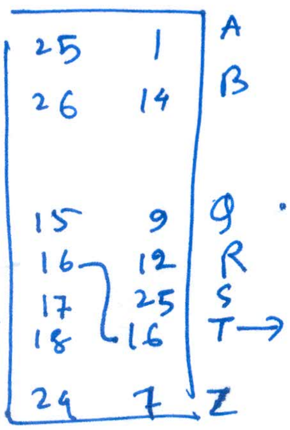
depress A ↓ get B.

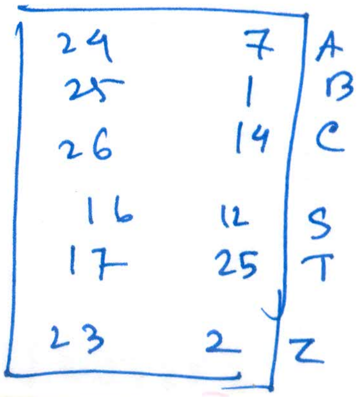
depress A ↓ get E

depress A ↓ get T



- multiple cylinders used with output pins of one cylinder are connected to input pins of the next
- For every complete rotation of the outer cylinder, the middle cylinder rotates one pin position
- For every complete rotation of the middle cylinder, the inner cylinder rotates one pin position.





→ Results $26 \times 26 \times 26 = 17,576$ different substitution ~~ciphers~~ alphabets used before the system repeats.