1- Caser

2- Monoalphabetic

3- Vigenere

4- Rail -fence

5- Playfair

6- ROW Transposition

7- Hill Cipher

8- Geometric

9- One Time Pad

10- Black ciphers modes

11- RSA

Notes

P: Plain text C: Cipher text

K: Key

22 mod 5 → 22/5 = 4.4

= 22-(5x4) = 2

1. Ceaser cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ
FGHIJKLMNOPQRSTUVWXYZABCDE

Ex: P: "Information" Key = 5

Encript using Ceaser

En: "Nsktwrfynts"

2. Mono Alphabic

هو هيبني جدول بالحروف

3. Vigenere cipher

P: wearediscoveredsaveyourself
Encrypt using the Keyword "deceptive"

K: deceptivedeceptivedeceptive
p: wearediscoveredsaveyourself
C: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

4. Rail_fence

P: Computer security K=3

c	p	e	e	r	y
o	u	r	c	i	
m	t	s	u	t	

En: cpeeryourcimtsut

5. Play fair

P; sh|ro|uk| ac|ad|em|y

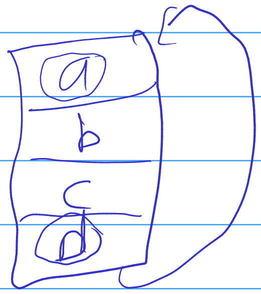
K; security

ud pu rh yu i/jd h t v a i/j Ab~~c~~d~~e~~fghi~~j~~klmnopq~~rstu~~vw ~~x~~yz

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

لو في نفس العمود أخذ التحتها

ba



لو في نفس العمود هاخد الي يمينهم

6. Row Trans Potion

P: Security game

K: 41532 => 5 هذا الـ K

① أرتب الـ K سواء أرقام أو حروف
تصاعدي ascending

1	2	3	4	5
s	e	c	u	r
i	t	y	g	a
m	e	x	x	x

② أكتب الـ K تاني بالأعمدة
بترتيبه

4	1	5	3	2
u	s	r	c	e
g	i	a	y	t
x	m	x	x	e

③ usrcegiaytxmxxe أكتب الإجابة صف صف

7. Hill CiPher

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

P: Hi my friend $\quad K = \begin{matrix} 15 & 15 \\ 20 & 25 \end{matrix}$

$$C = KP \bmod 26$$

① $\begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} H & m \\ i & y \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} 7 & 12 \\ 8 & 24 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} (15\times7)+(15\times8) & (15\times12)+(15\times24) \\ (20\times7)+(25\times8) & (20\times12)+(25\times24) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 225 & 540 \\ 340 & 840 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 17 & 20 \\ 2 & 8 \end{bmatrix} = \text{RCUI}$$

② $\begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} F & i \\ r & e \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 17 & 4 \end{bmatrix} \bmod$

$\begin{bmatrix} 15\times5+15\times17 & 15\times8+15\times4 \\ 20\times5+25\times17 & 20\times8+25\times4 \end{bmatrix} \bmod 26 =$

$\begin{bmatrix} 330 & 180 \\ 525 & 260 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 & 24 \\ 5 & 0 \end{bmatrix} = SFYA$

③ $\begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} n \\ d \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 15 \\ 20 & 25 \end{bmatrix} \begin{bmatrix} 13 \\ 3 \end{bmatrix}$

$\begin{bmatrix} 240 \\ 335 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 23 \end{bmatrix} = GX$

C: RCUISFYAGX

8. Geometric

P: I Came I saw I conquered   key: 6

1	2	3	4	5	6
I	C	A	M	E	I
O	C	I	W	A	S
N	Q	U	E	R	E
					D

IONQCCAIUEWMEARDESI

9 . Vernan/one time pad cipher

P = Come today   K = NCBTZQARX

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

C	o	m	e	T	o	d	a	y
2	14	12	4	19	14	3	0	24
N	C	B	T	Z	Q	A	R	X
13	2	1	19	25	16	0	17	23
15	16	13	23	$\overset{18}{\cancel{44}}$	$\overset{4}{\cancel{30}}$	3	17	$\overset{21}{\cancel{47}}$
P	Q	N	X	S	E	D	R	V

10- Block ciPhermodes

بيديل قواعد تمشي كليها

11- RSA

$n = p \times q$

$\emptyset(n) = (P-1) \times (q-1)$

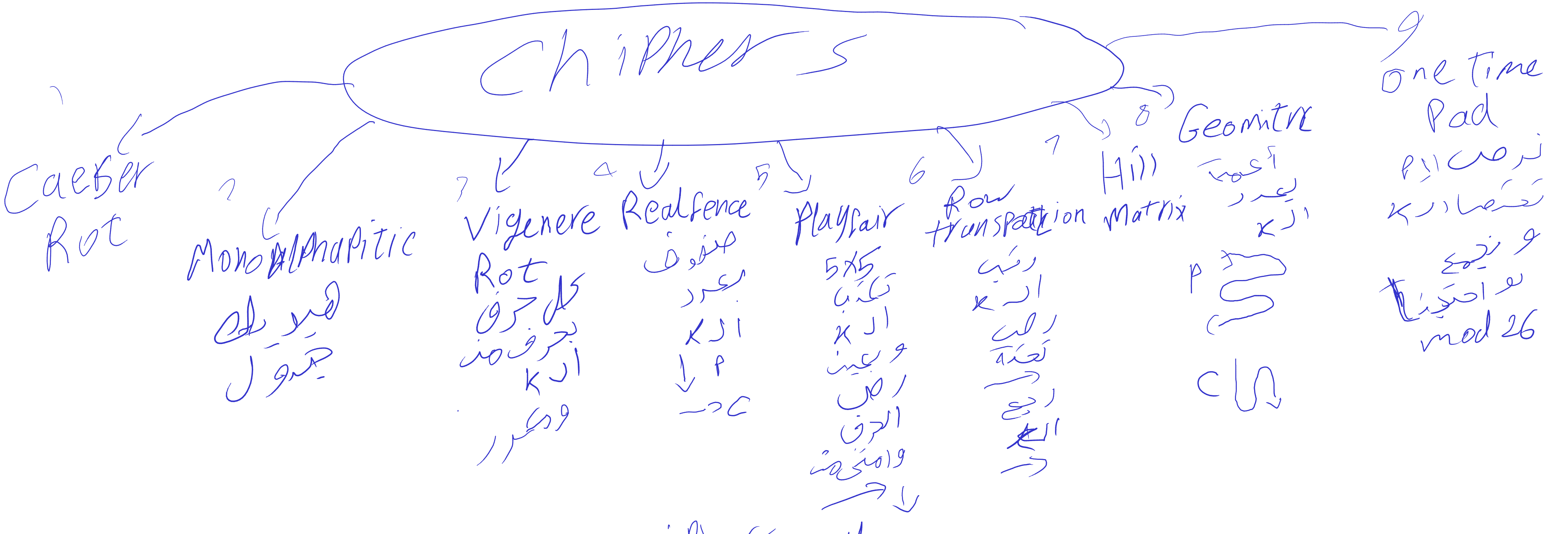
$e \cdot d = K \emptyset(n) + 1$

Public key $= \{e, n\}$

Privet key $= \{d, n\}$

encription: $C = m^e \bmod n$

decriPtion: $M = C^d \bmod n$



Chiphers

1 Caeser Rot

2 Mono~~Al~~Alphapitic
هيديلك جدول

3 Vigenere Rot
كل حرف بحرف من ال K ودحرر

4 Realfence
صفوف بعدد ال K
P ↓ C

5 Playfair
5x5
تكتب ال K وبعين رص الحرف والمتبقي →↓

6 Row transpotion
رتب ال K رأسي تحته → رجع ال ~~K~~ →

7 Hill Matrix

8 Geomitre
أعمدة بعدد ال K
P
C

9 One time Pad
نرص ال P تحت ال K ونجمع ~~h~~ لو احتجنا mod 26

Block chiphers modes

Vely طويل

R SA

$n = p \times q$

$\varnothing(n) = (p-1)(q-1)$

$e \cdot d = k\,\varnothing(n) + 1$

publickey ; $\{e, n\}$

privet ; $\{d, n\}$

$c = M^e \bmod n$

$M = C^d \bmod n$