Assignment 1

Q.1) Encrypt "The key is hidden under the door" using playfair ciphers with key word "domestic"

So Ans)

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

Plain text: ["TH", "EK", "EY", "IS", "HI" "DX", "DE", "NX"]

↑ dogus character

ENCRYPTION: "TH" → "CF"

"EK" → "SJ"; "EY" → "SX"

"IS" → "BO"; ~~"HI" → "CG"~~

"HI" → "GC"; "DX" → "EU"

~~"DE" → "EU"; "NX" → "QV"~~

~~Encypted text: CFSJSX BOGCEUEUQV~~

"DE" → "OS"; "NX" → "QV"

Cipher text: CFSJSXBOGCEUOSQV

Q.2) Encrypt the given message using Autokey cipher, Key = 7 & the Message is: "The house is being sold tonight".

Ans)

Plain text	T	H	E	H	O	U	S	E	T	S	B	E	I	N	G
~~Key Stream~~															
P's values	19	07	04	07	14	20	18	04	08	18	01	04	08	13	6
Key Stream	07	19	07	04	07	14	20	18	04	08	18	01	04	08	13
C's values	00	00	11	11	21	08	12	22	12	00	19	05	12	21	20
Cipher text	A	A	L	L	V	I	M	W	M	A	T	F	M	V	U

Plain text	S	O	L	D	T	O	N	I	G	H	T
P's values	18	14	11	03	19	14	13	08	06	07	19
Key Stream	26	18	14	11	03	19	14	13	08	06	07
Cipher text Values	24	6	25	14	22	07	01	21	14	13	00
Cipher text	Y	G	Z	O	W	H	B	V	O	N	A

Cipher text: AALLVIMWMATFMVTYGZO
WHBVONA

Q.3) Use the Playfair cipher with the keyword: "HEALTH" to encipher the message "Life is full of Surprises".

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

Plain text = {"Li", "fe", "is", "fu", "ll"}

Plain text = ["LI", "FE", "IS", "FO", "X", "LO", "FS", "UR", "PR", "IS", "ES"]

Encryption: "LI" → "HN", "FE" → "CL"
"IS" → "NP", "FO" → "GS"
"LX" → "AY", "LO" → "IN"
"FS" → "NY", "UR" → "PS"
"RR" → "QS", "IS" → "NP"
"ES" → "LQ"

Cipher text: HNCLNPGSAYINNYPSQSNP
LQ.

Q.4) Encrypt the plain text message "SECURITY" using affine ciphex with the key pair (3, 7). Decrypt to get back original plaintext.

Ans) $K_1 = 3$; $K_2 = 7$ $\Rightarrow C(K_1, K_2) = (PK_1 + K_2) \bmod 26$

multiplicative, Additive

$$\boxed{K_2^{-1} = -K_2 = -7}$$

$$K_1 \cdot K_1^{-1} \equiv 1 \pmod{26}$$

i.e $K_1 \cdot (K_1^{-1}) + n(-9) = 1$

$\Rightarrow$ G.C.D $(K_1, n) = 1$

G.C.D $(3, 26) \Rightarrow$ $26 = 3(8) + 2$

$3 = 2(1) + 1$

$2 = 1(2)$

$\therefore$ G.C.D $(3, 26)$

$26 + 3(-8) = 2$

$\therefore 3 + 2(-1) = 1$

$3 + (-1)[26 + 3[-8]] = 1$

$26[-1] + 3[+9] = 1$

$\therefore \boxed{K_1^{-1} = +9}$; $\boxed{K_2^{-1} = -7}$

$$P(K_1^{-1}, K_2^{-1}) = [(C + K_2^{-1}) K_1^{-1}] \pmod{26}$$

Plain text = "SECURITY"

Encryption:

S → 18 → C(3,7)

∴ S ⇒ 18 ⇒ (18×3 + 7)(mod 26) = 9 ⇒ J

E ⇒ 04 ⇒ (04×3+7)(mod26) = 19 ⇒ T

C ⇒ 02 ⇒ (02×3+7)(mod26) = 13 ⇒ N

U ⇒ 20 ⇒ (20×3+7)(mod26) = 15 ⇒ P

R ⇒ 17 ⇒ (17×3+7)(mod26) = 6 ⇒ G

I ⇒ 08 ⇒ (08×3+7)(mod26) = 5 ⇒ F

T ⇒ 19 ⇒ (19×3+7)(mod26) = 12 ⇒ M

Y ⇒ 24 ⇒ (24×3+7)(mod26) = 01 ⇒ B

Cipher text: JTNPGFMB

Decryption:

Character → Value → P(9,7)...

J ⇒ 9 ⇒ [(9-7)×9](mod26) = 18 ⇒ S

T ⇒ 19 ⇒ [(19-7)×9](mod26) = 04 ⇒ E

N ⇒ 13 ⇒ [(13-7)×9](mod26) = 02 ⇒ C

P ⇒ 15 ⇒ [(15-7)×9](mod26) = 20 ⇒ U

G ⇒ 6 ⇒ [(6-7)×9](mod26) = 17 ⇒ R

F ⇒ 5 ⇒ [(5-7)×9](mod26) = 08 ⇒ I

M ⇒ 12 ⇒ [(12-7)×9](mod26) = 19 ⇒ T

B ⇒ 01 ⇒ [(1-7)×9](mod26) = 24 ⇒ Y

Plain text: SECURITY.

Q.5) Use hill cipher to encrypt the text "short" the key to be used is "hill"

Ans) Key = [[K1 = h = 07 , K2 = i = 08] [K3 = i = 11, K4 = i = 11]]

$$K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} ; |K| = 77 - 88 = -11$$

Plain text = [[P1 = s = 18 , P2 = h = 07]
[P3 = o = 14 , P4 = r = 17]
[P5 = t = 19 , P6 = x = 23]]
↑ Bogus character.

$$\therefore P = \begin{bmatrix} 18 & 7 \\ 14 & 17 \\ 19 & 23 \end{bmatrix}$$

Encryption:

$$C = (P \cdot K) \bmod 26 = \left(\begin{bmatrix} 18 & 7 \\ 14 & 17 \\ 19 & 23 \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \right) \bmod 26$$

$$C = \begin{bmatrix} 18\times7 + 7\times11 & 18\times8 + 7\times11 \\ 14\times7 + 17\times11 & 14\times8 + 17\times11 \\ 19\times7 + 23\times11 & 19\times8 + 23\times11 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 21 & 13 \\ 25 & 13 \\ 22 & 15 \end{bmatrix} \Rightarrow \begin{bmatrix} [21 \Rightarrow V, & 13 \Rightarrow N] \\ [25 \Rightarrow Z, & 13 \Rightarrow N] \\ [22 \Rightarrow W, & 15 \Rightarrow P] \end{bmatrix}$$

∴ Ciphere text = VNZNWP.

Q.6) In an RSA System the Public Key(e,n) of user A is defined as (7,119). Calculate totient(n) and Private key d. What is the cipher text when you encrypt message m=10 using the Public key.

Ans) $\phi(n) = \phi(119)$

Prime factorization of $119 = 7^1 \times 17^1$

$\therefore \phi(119) = \phi(7^1 \times 17^1) \Leftrightarrow \phi(7) \times \phi(17)$

$$\boxed{\phi(119) = 6 \times 16 = 96}$$

$e \cdot d \equiv 1 \pmod{\phi(n)}$

$\therefore e \cdot (d) + \phi(n)(-9) = 1$

$\therefore GCD(e, \phi(n)) = GCD(7, 96)$

$96 = 7(13) + 5 \Leftrightarrow 5 = 96 + 7(-13)$
$7 = 5(1) + 2 \Leftrightarrow 2 = 7 + 5(-1)$
$5 = 2(2) + 1 \Leftrightarrow 1 = 5 + 2(-2)$
$2 = 1(2)$
$\therefore GCD(7, 96) = 1$

$\therefore 2 = 7 + (-1)[96 + 7(-13)]$
$2 = 96(-1) + 7(14)$

$1 = [96 + 7(-13)] + (-2)[96(-1) + 7(14)]$
$\therefore 1 = 96(+3) + 7(-41)$

$d = -41 \pmod{96} \Leftrightarrow 55$

$m = 10$

Encrypted message $= m^e \pmod{n}$

$C = 10^7 \pmod{119}$

$C \equiv [(10^3)^2 \cdot 10] \pmod{119}$

$C = [(48)^2 \cdot 10] \pmod{119}$

$C = [48 \cdot 480] \pmod{119}$

$C = [48 \cdot 4] \pmod{119}$

$C = 73$

Q.7) If A and B wish to use RSA to communicate securly. A chooses public key (e,n) as $(7, 247)$ and B chooses Public key (e,n) as $(5, 221)$

i) Calculate A's Private key:

A of $(e,n) = (7, 247)$

$\therefore \phi(n) = \phi(247)$

$247 = 13^1 \times 19^1$

$\therefore \phi(247) = \phi(13 \times 19) = \phi(13) \times \phi(19)$

$\phi(247) = 12 \times 18 = 216$

$\therefore d = -41 \pmod{96} = 55$

$d = e^{-1} \bmod \phi(n)$

$e \cdot (e^{-1}) + \phi(n)(-q) = 1$

$\therefore G.C.D(e, \phi(n)) \Rightarrow G.C.D(7, 216)$

$216 = 7(30) + 6 \Rightarrow 6 = 216 + 7(-30)$

$7 = 6(1) + 1 \Rightarrow 1 = 7 + 6(-1)$

$6 = 1(6) + 0$

$\therefore 1 = 7 + (-1)[216 + 7(-30)]$

$7(31) + 216(-1) = 1$

$\therefore e^{-1} = 31$

$d = 31 \bmod 216 = 31$

$\therefore \boxed{d = 31}$

ii) Calculate Private key of B:

B of $(e, n) = (5, 221)$

$\phi(221) = \phi(13 \times 17) = \phi(13) \times \phi(17)$

$\therefore \phi(221) = 12 \times 16 = 192$

$d = e^{-1} \bmod \phi(n)$

$e \cdot (e^{-1}) + \phi(n)(-q) = 1$

G.C.D(5, 192) ⇒

$$192 = 5(38) + 2$$
$$5 = 2(2) + 1$$
$$2 = 1(2) + 0$$

$$2 = 192 + 5(-38)$$

$$1 = 5 + 2(-2)$$

$$\therefore 1 = 5 + (-2)[192 + 5(-38)]$$

$$192(-2) + 5(77) = 1$$

$$\therefore d = e^{-1} 77 \pmod{192} = \boxed{77}$$

$$\therefore \boxed{d = 77}$$

(iii) What will be the cipher text sent by to B, if A wishes to send M = 8 to B

Ans) If A wish to send some text to B
A will use publickey of B (e, n)
i.e. (5, 221)
M = 8.

$$\therefore \text{Ciphertext} \Rightarrow C = M^e \pmod{n}$$

$$\therefore C = 8^5 \pmod{221} = 3125 \pmod{221}$$

$$\therefore \boxed{C = 31}$$