part 1: Numerical Exercises

Ex II ⊗ Affine Cipher

a. key(2,9) → a=2, b=9, n=26
GCD(2,26) ≠ 1 → 2 and 26 are no coprime
⟹ key(2,9) un appropriate key to be used

b. a = 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25, 1
→ GCD(a, 26) = 1 → a and 26 are coprime

12 possibilities for a 26 possibilities of b
keys: 12 × 26 = 312 possible keys

c. key(3,5) n=26 E(x) = (ax+b) mod n

a. plaintext: hadi Hakim
E(h) = (3(7)+5) mod 26 = A
E(a) = (3(0)+5) mod 26 = F
E(d) = (3(3)+5) mod 26 = O
E(i) = (3(8)+5) mod 26 = D
E(k) = (3(10)+5) mod 26 = J
E(m) = (3(12)+5) mod 26 = P
⟹ ciphertext: AFOOAFJDP

b. D(x) = a⁻¹(x−b) mod 26

$a^{-1} \times a^3 = 1 \bmod 26$
$a^{-1} = 9$ b = 5

D(x) = $\boxed{9(x-5) \bmod 26}$

$a = 3$, $b = 5$, $a^{-1} = 9$, $n = 26$

c. Ciphertext: LEZYKUXEFUAZ

11 4 25 24 10 20 23 4 5 24 0 25

$D(x) = 9(x - 5) \bmod 26$

$D(L) = 9(11 - 5) \bmod 26 = C$

$D(E) = 9(4 - 5) \bmod 26 = R$

$D(Z) = 9(25 - 5) \bmod 26 = Y$

$D(Y) = 9(24 - 5) \bmod 26 = P$

$D(K) = 9(10 - 5) \bmod 26 = T$

$D(U) = 9(20 - 5) \bmod 26 = O$

$D(X) = 9(23 - 5) \bmod 26 = G$

$D(F) = 9(5 - 5) \bmod 26 = A$

$D(A) = 9(0 - 5) \bmod 26 = H$

plaintext: CRYPTOGRAPHY

Ex III playfair cipher

a. HAKIM → password

key →

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

b. plaintext: Computer Security

Co, mp, ut, er, se, cu, ri, ty

EL, FU, QU, CT, FO, FA, TA, YI

Note: $P_i = (E_i - K_i + 26) \bmod 26$

Ciphertext: ELFUQUCTTOFRTAYI

Ex: V @ Vigenere cipher

Plaintext: "I Love USAL university

Key: HADI

$E_i = (P_i + K_i) \bmod 26$

	I	L	O	U	C	U	S	A	L	
	8	11	14	20	2	20	18	0	11	
E_i = +	H	A	D	I	H	A	D	I	H	mod 26
	7	0	3	8	7	0	3	8	7	
	U	A	I	V	C	I	F	S	Y	

	U	A	I	V	C	I	F	S	Y	
	20	13	8	21	4	17	18	8	19	24
E_i +	A	D	I	H	A	D	I	H	A	D
	0	3	8	7	0	3	8	7	0	3

mod 26

$E_0 = (8+7) \bmod 26 = P$

$E_4 = (11+0) \bmod 26 = L$

Ciphertext: PLYDQBSKTGUIFMDZIOG

Ex: V @ Hill Cipher

a. matrix: $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ Since 2×2 can be used for encryption

b. CDEF is the Encryption key

$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ ← Decryption key is its inverse

Pkey $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}^{-1} = (ad-cb)^{-1}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} =$

$14 \begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}$

C. ciphertext: ZR ZU OW MK AC GM KX
25 17 25 4 14 22 12 10 0 2 6 12 10 23

$\begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} \begin{pmatrix} 25 \\ 17 \end{pmatrix} \bmod 29 = \begin{pmatrix} 21 \\ 4 \end{pmatrix}$ U E

$= \begin{pmatrix} 25 \\ 21 \end{pmatrix} \bmod 29 = \begin{pmatrix} 27 \\ 0 \end{pmatrix}$ - A

$= \begin{pmatrix} 14 \\ 22 \end{pmatrix} \bmod 29 = \begin{pmatrix} 27 \\ 6 \end{pmatrix}$ - G

$= \begin{pmatrix} 12 \\ 10 \end{pmatrix} = \begin{pmatrix} 14 \\ 14 \end{pmatrix}$ O O

$= \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 27 \end{pmatrix}$ D _

$= \begin{pmatrix} 6 \\ 12 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ D A

$= \begin{pmatrix} 10 \\ 23 \end{pmatrix} = \begin{pmatrix} 24 \\ 26 \end{pmatrix}$ Y .

plaintext: VE_A_GOOD_DAY.

Ex: 1

ab. [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]

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

c.d plain text: Hadi Ali Hattim

e Ciphertext: UGC OGW QUGM V

i number of attempts = since plaintext length is 14 and number of characters is 27

27^{14}

ii- Cryptoanalysis better than brute force since it analyse the language (Frequency analysis) but since plaintext is small it is difficult here to find the key.