Quiz. 1

(Deadline March 07, 2024)

Problem 1

Given the ciphertext:

C UYGHARMZ IUWMPRWIR GAIR YVRMP

MBHMZWMPUM C VMMXWPE YV PYR VCZ

ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM

RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN

KMCZ LZWPEI SWRN WR

a) Please write a program to find out the frequencies of letters in the ciphertext.

b) Use the plaintext frequency count information below as a reference to break this encrypted messages.

Table 1: Ciphertext letter frequency count: (times)

A	B	C	D	E	F	G	H	I	J	K	L	M
2	2	12	6	4	0	5	3	4	0	2	1	19
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	1	12	2	9	3	1	6	7	9	6	12	9

Table 2: Common frequency of letters appearance: (%)

E	A	R	I	O	T	N	S	L	C	U	D	P
11.16	8.5	7.58	7.54	7.16	6.95	6.65	5.74	5.49	4.54	3.63	3.38	3.17
M	H	G	B	F	Y	W	K	V	X	Z	J	Q
3.01	3.0	2.47	2.07	1.81	1.78	1.29	1.10	1.01	0.29	0.27	0.20	0.20

Table 3: Ciphertext to plaintext mapping

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
Plaintext	U	X	A	D	G	J	M	P	S	Q	Y	B	E
	20	23	0	3	6	9	12	15	18	16	24	1	4
Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	H	K	N	V	T	W	Z	C	F	I	L	O	R
	7	10	13	21	19	22	25	2	5	8	11	14	17

c) Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?

d) Suppose "$f(x) = ax + b \bmod 26$", where x is plaintext, please solve the value of a and b.

e) What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult?

f) (Bonus) Please try to see if it is possible to decipher this problem with ChatGPT or another tool.

Problem 2

Plaintext is encrypted using an affine cipher. A plaintext symbol, x, is drawn from $\mathbb{Z}_{30}$ and, hence, encryption is defined as "$y = ax + b \bmod 30$", where y is the resulting ciphertext and the encryption key is given by $k_{\text{enc}} = (a, b)$.

a) Determine the size of the key space (that is, the total number of keys).

b) Determine all values in $\mathbb{Z}_{30}$ that have inverses and, by trail-and-error, determine the inverses.

c) An attacker intercepts the following plaintext/ciphertext pairs:

x	y
4	8
10	26
27	7

Determine the encryption key $k_{\text{enc}} = (a, b)$.

d) Determine the decryption key $k_{\text{dec}} = (c, d)$, where "$x = cy + d \bmod 30$".