Özge Öneyman
24906

Homework 1

(1) ciphertext: "NKWZ"

13 10 22 25

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

(mod 26)

key=1	12	9	21	24	→ M J V Y
key=2	11	8	20	23	→ L I U X
key=3	10	7	19	22	→ K H T W
=4	9	6	18	21	→ J G S V
=5	8	5	17	20	→ I F R U
=6	7	4	16	19	→ H E Q T
=7	6	3	15	18	→ G D P S
=8	5	2	14	17	→ F C O R
=9	4	1	13	16	→ E B N Q
=10	3	0	12	15	→ **D A M P** → key=10
=11	2	25	11	14	→ C Z L O
=12	1	24	10	13	→ B Y K N
=13	0	23	9	12	→ A X J M
=14	25	22	8	11	→ Z W I L
=15	24	21	7	10	→ Y V H K
=16	23	20	6	9	→ X U G J
=17	22	19	5	8	→ W T F I
=18	21	18	4	7	→ V S E H
=19	20	17	3	6	→ U R D G
=20	19	16	2	5	→ T Q C F
=21	18	15	1	4	→ S P B E
=22	17	14	0	3	→ **R O A D** → key=22
=23	16	13	25	2	→ Q N Z C
=24	15	12	24	1	→ P M Y B
=25	14	11	23	0	→ O L X A
=26	13	10	22	25	→ N K W Z

keys = {10, 22}

(2) most frequent letter is 'A' in plaintext

R → 7
E → 5
Z → 4
A → 1
N → 3
S → 1
J → 2
V → 2
D → 1
B → 3
C → 1
L → 3
X → 1
G → 4
O → 3
M → 1
T → 1
H → 1

A → R

$\gcd(26, \alpha) = 1$

$\alpha \Rightarrow (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25)$

Affine cipher (α, β)

$y = x \cdot \alpha + \beta \pmod{26}$

$17 = 0 \cdot \alpha + \beta \pmod{26}$

$\boxed{\beta = 17}$

There is 12 possibility for α. So, I tried all the 12 combination of α and β with the code which provided to us in hw01_helper.py. And the result is $\boxed{\alpha = 9}$.

Plaintext is ANY BODY CAN MAKE HISTORY. ONLY A GREAT MAN CAN WRITE IT

$\boxed{\gamma \rightarrow 3 \quad \vartheta \rightarrow 1}$

hw1_question2.py

(3) most frequent letter is 'A' in plaintext

C → 149

A → C
↓ ↓
0 2

$y = x \cdot \alpha + \beta \pmod{31}$

$2 = 0 \cdot \alpha + \beta \pmod{31}$

$\beta = 2$

$\gcd(31, \alpha) = 1$

$\rightarrow \alpha \rightarrow 27$

$\gamma \rightarrow 23$

$\vartheta \rightarrow 16$

BERGSON BENİ, GENÇLİĞİMDE HERBİRİ BENİM İÇİN BİRER İŞKENCE OLAN, ÇÖZÜLMESİ OLANAKSIZ, FELSEFE --

(4) Suppose p_a is probability of plaintext letter a, where $a \in \{A, B, \ldots Z\}$ Suppose also that p_β is probability of ciphertext letter β, where $\beta \in \{A, B, \ldots Z\}$

Demonstrate $p_\beta = 1/26$ for every $\beta \in \{A, B, \ldots Z\}$ independent of values of p_a

Example plaintext = 'D' (a) shift by $k = 3$

→ ciphertext = 'G' (β)

Thus, p_β always depends to set of values of p_a

And there are 26 opportunities (sample space = 26) ⇒ Thus, $p_\beta = 1/26$ for every $\beta \in \{A, B, \ldots Z\}$ independent values of p_a

(5) TH $19 \times 28 + 7 = 539$

$27 \cdot 28 + 27 = 783$ (mod)

Key space $= \{ \forall x : 1 < x < 783$ where $\gcd(783, x) = 1 \}$

$\gcd(783, x) = 1 \implies$ 504 relatively prime number

↓

length of key space

(6) Our possible key $|K| = 783$

for recommended security $|K| \geq 2^{100}$

but our key is smaller.

Which said in Lecture2.pptx. Same plaintext letters maps to same ciphertext letters.

So, it should be sufficiently long.

Thus, it is not secure against the letter frequency analysis.

(7) plen $= 2k + 1$

BE → ·X

↓ ↓ ↓ ↓

1 4 26 23

$1 \cdot 28 + 4 = (26 \cdot 28 + 23)\alpha + \beta \pmod{783}$

$32 = 751\alpha + \beta \pmod{783}$