Recap: · Shift, Hill & Affine ciphers.

Frequency analysis:

Use English language with meaningful words

Then, the frequency of E is the highest

followed by T, A, O N . - - - .

Example:

Ciphertext

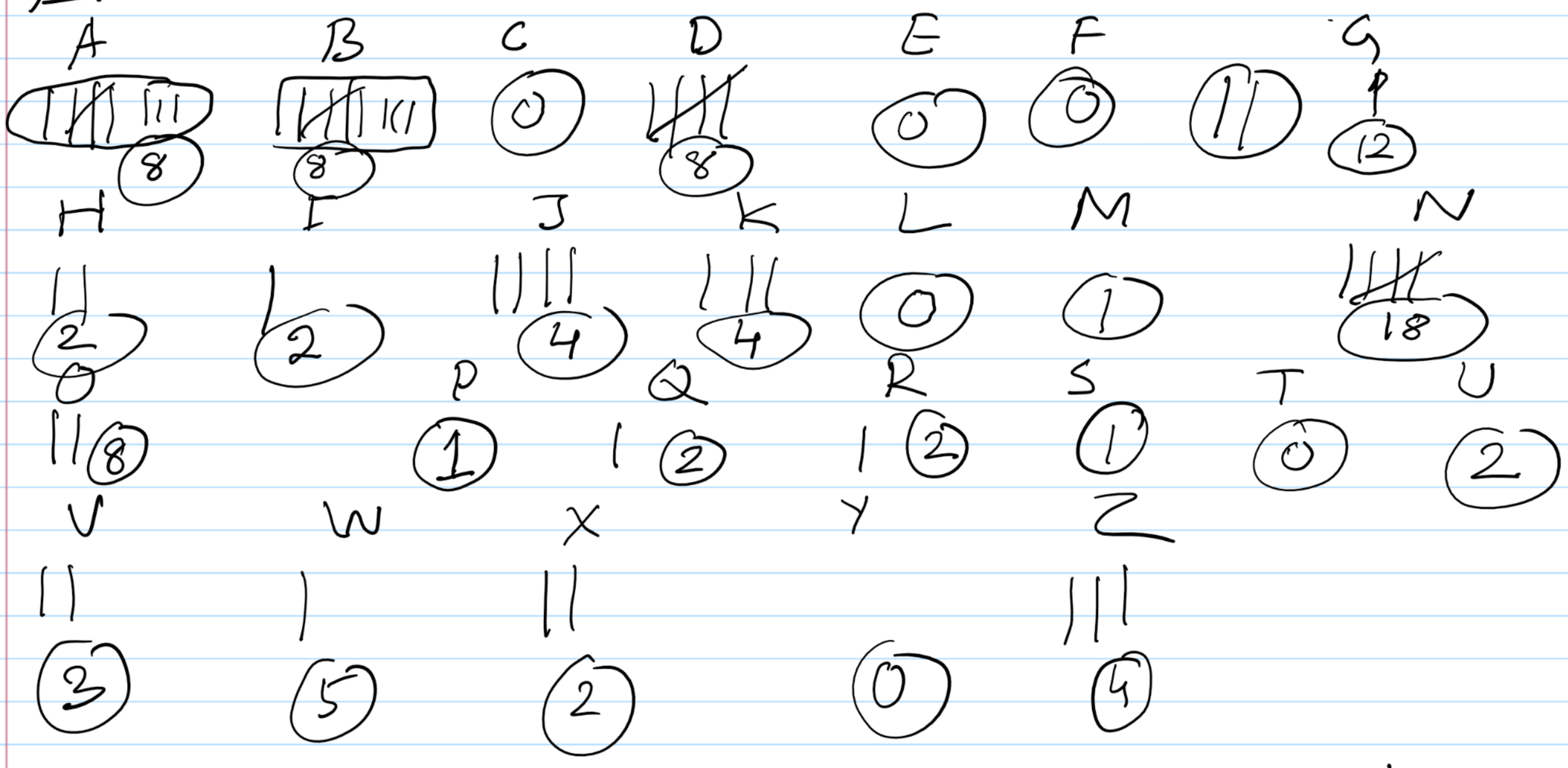
ØAMXJ AOHNB ØBIVD ZDZDB GMHWK

ZXJNJ DMKGR JØKNA GBBOK GWNUB

GGNAO DRQAN UNBGO TNMNO GDPWN

GWNAG WNVBA NINGG NAD2O BGNSG

Frequency:



If we know that encryption was done by affine cipher from $E(x) = kx + b$

$n = 26$,

$$\Sigma(E) = N$$

$$\Sigma(T) = G$$

$$\Sigma(4) = 13 \quad \text{i.e.} \quad \boxed{4k + b = 13}$$

$$\Sigma(19) = 6 \qquad \boxed{19k + b = 6}$$

$$\Rightarrow -15k = 7 \pmod{26}$$

$$\Rightarrow 11k = 7$$

$$\Rightarrow k = 11^{-1}7$$

$$= (-7) \times 7 \pmod{26}$$

$$= -49 = 3 \pmod{26}$$

11×23

$26 \times 3 = 78$

$11 \times 7 = 77 = -1 \pmod{26}$.

$\boxed{3^{-1} = 9 \pmod{26}}$

So $11^{-1} = -7 = 19 \pmod{26}$.

$b = 13 - 4k$

$= 13 - 4 \times 3$

$= 1 \pmod{26}$

$\alpha(y) = k^{-1}y - k^{-1}b$

$= 9y - 9 \times 1$

$= 9y + 17 \pmod{26}$

So

Numerical equivalent of the date

16 - 0 - 13 - 23 - 9 - 0 - 14 - 7 - 21 - 14 - 1 - 8 - 2 1 - . . . .

0

$9 \times 16 + 17 - 17 - 9 \times 13 + 17 \quad 23 \times 9 + 17 \quad 9 \times 9 + 17 \quad 14 \times 9 + 17 \quad 7 \times 9 + 17$

11 11 11 11 11

5 4 16 20 13 2

$2 \times 9 + 17 = 24$

↓

FREQUENCY

Vigenere Cipher.

key word $\bar{k} = k_1 k_2 \cdots k_l$

l is the length of the keyword.

the key word is a common knowledge for Alice & Bob.

Plain text converted to numerical equivalent & arranged in blocks of length l each except for the last block.

$\bar{x}_1 \quad \bar{x}_2 \quad \bar{x}_3 \quad \cdots$

(where $\bar{x}_j = x_{j1} x_{j2} \cdots x_{jl}$
$(x_{j1}, x_{j2} \cdots, x_{jl})$

$E(\bar{x}_i) = \bar{x}_i + \bar{k}$

$= (x_{i1} + k_1, x_{i2} + k_2, \quad , x_{il} + k_l)$

Example: Plain text

THE PASSWORD IS ENGLISH

Use keyword: CABLE

So, $l = 5$ $\quad \bar{k} = (2, 0, 1, 11, 4)$

$A = \{A, B, \cdots, Z, -\}$ $n = 27$

→ THE-PASSWORD-IS-ENGLISH

N ↓

19-7-4-26-15 0-18-18-22-14 16-3-26-8-18

26-4-13-6-11 8-18-7

E $\bar{y} = \bar{x} + \bar{k}$

21-7-5-10-19 2-18-19-5-18 18-3-0-19-22

1-4-14-17-15 10-18-8

N^{-1} ↓

VHFKS CSTFS SDATW B-EORP KSI

↑ P