ISS Assignment - 1

Manav Sarkar
2020IIB019

1.) Plaintext = cryptographic secrets

$K = (K_1, P_1, P_2 \ldots)$ $K_1 = 12$

Plain Text: c r y p t o g r a p h i c s e c r e t s

P's value: 2 17 24 15 19 14 6 17 0 13 7 8 2 18 4 2 17 4 19 18

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

Plain Text	c	r	y	p	t	o	g	r	a	p	h	i	c	s	e	c	r	e	t	s
P's value	2	17	24	15	19	14	6	17	0	13	7	8	2	18	4	2	17	4	19	18
Key Stream	12	2	17	24	15	19	14	6	17	0	15	7	8	2	18	4	2	17	4	19
C's Value	14	19	15	13	8	7	20	23	17	15	22	15	10	20	22	6	19	21	23	11
Cipher Text	o	t	p	n	i	h	u	x	r	p	w	p	k	u	w	g	t	v	x	l

Hence encrypted text is

otpnihuxrpwpkuwgtvxl

In polyalphabetic substitution, each occurrence of a character may have different substitutions. In the above example we saw 'r' maps to 't' and 'x', so some characters are having multiple mapping. Hence Autokey Cipher is an example of polyalphabetic cypher.

---

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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

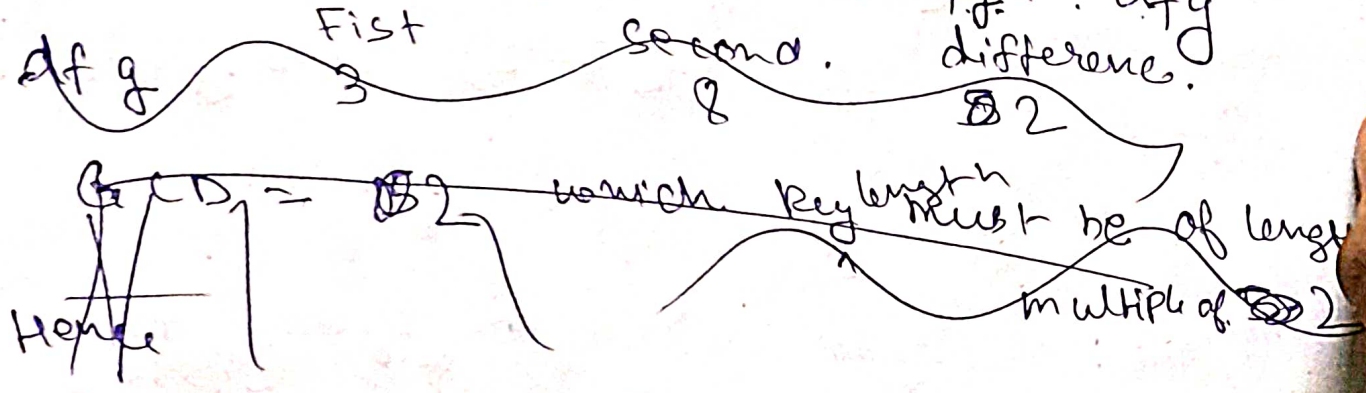
2.) For a shift cipher, the ~~key is~~ key is iterated from 0 to 25. In any of the key, the decrypted cipher makes sense.

For a Auto key cipher, since we are performing $(P_i + K_i) \bmod 26$ which equates to $(P_i \bmod 26 + K_i \bmod 26) \bmod 26$. So K_i can have range of 0 to 25.

So performing exhaustive search for key. Autokey cipher is similar to shift cipher. Hence proved.

3.) 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

any dfg dw dfg ja dmn s c dfg dm dfg



dfg	First	second	third	fourth
	3	8	18	23
	5	10	15	20.

gcd = 5

Hence the key length is 5.

4.) Affine cipher uses multiplicative & additive cyphers.

Hence the size of key domain is $Z^*_{10} \times Z_{10} = 10 \times 5 = 50$

5 a) Cryptography

Keypair (H, C) (7, 2)

2 17 24 15 19 14 6 17 0 15 7 24

16 17 14 3 5 22 18 17 9 3 25 14.

R od

→ q r o d f w s r j d z o

b) Keypair → (H, C)

(7, 2) Encryption

c) decryption (7⁻¹, 2)

= (15, 2)

6).

6) 100 distinct letters. Affine cipher.

For Multiplic (50 - 2) 40.

For 100 distinct letters, there are 50 numbers which have multiplicative inverse.

Hence the Keyspace is 40 × 100 = 4000

using affine cipher.

7)

P:	1 L	2 E	3 T	4 U	5 S
	a	b	t	a	c
	R	E	O	m	O
	r	r	O	W	Z
	u	L	t	e	S

a

Encrypt 4 1 3 2 5 decrypt

1 2 3 4 5

7.)

Plaint Text

l	e	t	u	s
a	t	t	a	c
k	t	o	m	o
w	r	o	w	z

Cipher:

4	1	3	2	5
1	2	3	4	5

u	l	t	e	s
a	a	t	t	c
m	k	o	t	o
w	r	o	r	z

Cipher: uamwlakrttoeettrsco2

The key block size is the block size.

8.) The size of matrix is 5×5

Permutation Matrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Transpose of Permutation matrix = This is the inverse and hence the key

$$K = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

9) $\phi(n)$ [phi function] is the number of non negative integers less than n that are relatively prime to n.

~~So if n>1 then $\phi(n)$~~

$$\phi(p^a) = p^a - p^{a-1} \quad [p \text{ is prime}]$$

$$\phi(2^9) = 2^9 - 2^8$$
$$= 256.$$

10) The key space for a full size key for an n bit transposition cipher is $n!$.

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 1$$

Size of key should be

$$\log_2 n! =$$

12 a) Transposition cipher rearranges the position of characters of plain text. The identity of character is not changed.

b) Vigenere cipher is not a block cipher since it depends on plaintext position as well as key.

c) Playfair cipher is a block cipher with $m = 2$.