#### **Conventional Encryption Techniques**

Computer Science and Engineering Indian Institute of Information Technology Sri City, India

January 21, 2021

1/33

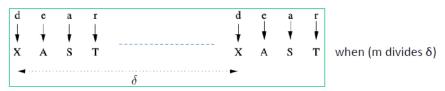
(IIIT Sri City) January 21, 2021

## **Objectives**

- Vigenere Cipher
- Kasiski Analysis

## Kasiski Analysis

- Kasiski test by Friedrich Kasiski in 1863
- Let m be the size of the key
- observation: two identical plaintext segments will encrypt to the same ciphertext when they are  $\delta$  apart and  $(m \mid \delta)$



- If several such  $\delta s$  are found (i.e.  $\delta_1$ ,  $\delta_2$ ,  $\delta_3$ , ....) then
  - $-m|\delta_1, m|\delta_2, m|\delta_3, ....$
  - Thus m divides the gcd of  $(\delta_1, \delta_2, \delta_3, ....)$



January 21, 2021

U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

```
6
                                 9
                                     10
                                          11
                                              12
U
        F
            В
                    G
                         M
                             Р
                                 F
                                     Χ
                                          Α
                                               V
U
                    Р
                             R
                                 W
                                              K
                         Α
Н
                         U
                                     F
                                               Ρ
    M
        11
                В
                    G
                             U
                    W
                         F
                                     Ρ
                                              Ν
        W
                Κ
                                          Ω
Х
                         F
        G
                    G
                             Р
                                 W
                                              C
Ε
                         U
                                               Р
    G
                    G
Р
                    Ν
                         Ν
Ρ
```

U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Ε	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	I	Ρ
P	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram No.of Occ Dist

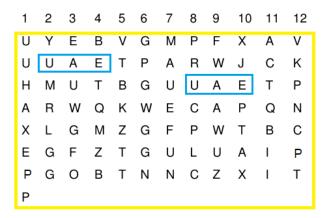
4/33

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Ρ
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	T
Р											

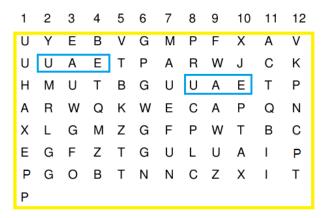
Trigram No.of Occ Dist

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Ε	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18



Trigram	No.of Occ	Dist
UUA	2	18



Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	V	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	T	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	T	Р
Α	R	W	Q	K	W	Ε	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	V	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	T	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	T	Р
Α	R	W	Q	K	W	Ε	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Ε	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Ε	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Ε	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Ε	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	I	Ρ
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	V	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Ρ
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	T
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Ε	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Ε	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	V	G	М	Р	F	Χ	Α	V
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Е	В	٧	G	М	Р	F	Χ	Α	V
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Ε	С	Α	Р	Q	N
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	T
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18
PAR	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Ε	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Ε	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Е	G	F	Z	Т	G	U	L	U	Α	1	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18
PAR	2	18
ARW	2	18

1	2	3	4	5	6	7	8	9	10	11	12
U	Υ	Ε	В	٧	G	М	Р	F	Χ	Α	٧
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	Ν
Х	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	1	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	1	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18
PAR	2	18
ARW	2	18

Key word length may be any one of the factor of 18, that is, 2, 3, 6, or 9

- 4 ロ > 4 個 > 4 差 > 4 差 > - 差 - 夕久で

11/33

(IIIT Sri City) January 21, 2021

1	2	3	4	5	6	7	8	9	10	11	12
									Χ		
U	U	Α	Е	Т	Р	Α	R	W	J	С	K
Н	М	U	Т	В	G	U	U	Α	Е	Т	Р
Α	R	W	Q	K	W	Е	С	Α	Р	Q	Ν
Χ	L	G	М	Z	G	F	Р	W	Т	В	С
Ε	G	F	Z	Т	G	U	L	U	Α	I	Р
Р	G	0	В	Т	Ν	Ν	С	Z	Χ	I	Т
Р											

Trigram	No.of Occ	Dist
UUA	2	18
UAE	2	18
AET	2	18
ETP	2	18
TPA	2	18
PAR	2	18
ARW	2	18

Key word length may be any one of the factor of 18, that is, 2, 3, 6, or 9 Suppose, adversary guesses key length as 6

(IIIT Sri City) January 21, 2021 11/33

### Adversary Attempt to Recover the Plaintext



U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

### Adversary Attempt to Recover the Plaintext



U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

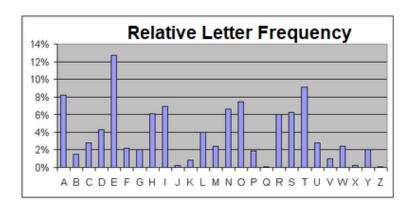
List the most repeated letters in each column.

Keyword						
	U	Υ	Е	В	٧	G
	М	Р	F	Χ	Α	V
	U	U	Α	Е	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	G
	U	U	Α	E	Т	G P
	Α	R	W	Q	K	W
	E	С	Α	Р	Q	N
	E X	L	G	М	Q Z	G
	F	Р	W	Т	В	С
	Е	G	F	Z	Т	G P
	U	L	U	Α	ı	Р
	Р	G C	O Z	В	Т	N
	N	С	Ζ	Х	ı	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

U YE BV GMPFXAVU UAET PAR WJCKHMUTBG U UAET PAR WQKWEC APQNX LGM ZGFPWTB C EGFZTG ULUA IPP G OBTN NC ZXITP

 List the most repeated letters in each column.

### Letter Frequency



Most common letter is E.

Keyword						
	U	Υ	Е	В	٧	G
	М	Р	F	Χ	Α	V
	U	U	Α	Ε	Т	Р
	Α	R	W	J	С	P K
	Н	М	U	Т	В	G
	U	U	Α	Ε	Т	Р
	Α	R	W	Q	K	W
	E	С	Α	Р	Q	
	Х	L	G W	М	Z	G
	F	Р	W	Т	В	N G C G P
	E	G	F	Z	Т	G
	U		U	Α	ı	Р
	Р	L G C	0	В	Т	N
	N	С	O Z	Χ	1	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

 Adversary assumes that G is the ciphertext letter for E.

Keyword						
	U	Υ	Е	В	٧	Е
	М	Р	F	Χ	Α	V
	U	U	Α	Е	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	Е
	U	U	Α	Е	Т	E P
	Α	R	W	Q	K	W
	Е	С	Α	Р	Q	N
	Χ	L P	G	М	Z	Е
	F	Р	W	Т	В	С
	E	G	F	Z	Т	E C E P
	U	L	U	Α	1	
	Р	G C	U O Z	В	Т	N
	N	С	Ζ	Χ	1	Т
	Р					
Most	U	?	W A	?	Т	G
repeated			Α			

- Adversary assumes that G is the ciphertext letter for E.
- Adversary replaces G with plaintext letter E in the sixth column.

Keyword						
	U	Υ	Е	В	V	Е
	М	Р	F	Χ	Α	V
	U	U	Α	Е	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	Е
	U	U	Α	Е	Т	Р
	Α	R	W	Q	K	W
	E X	С	Α	Р	Q	N
	Х	L	G	М	Z	E C
	F	L P	W	Т	В	С
	E	G	F	Ζ	Т	E P
	U		U	Α	ı	Р
	Р	L G C	U O Z	В	Т	N
	N	С	Ζ	Х	ı	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

- Adversary assumes that G is the ciphertext letter for E.
- Adversary replaces G with plaintext letter E in the sixth column.
- We can see,
   G = E + keywordLetter

$$G=6$$
 
$$E=4$$
 
$$6-4=2\pmod{26}$$

Hence keyword letter is C.

Keyword						С
	U	Υ	Е	В	V	Е
	М	Р	F	Χ	Α	V
	U	U	Α	Ε	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	Е
	U	U	Α	Е	Т	Р
	Α	R	W	Q	K	W
	E X	С	Α	Р	Q	N
	Х	L	G	М	Z	N E C
	F	L P	W	Т	В	С
	Е	G	F	Z	Т	E P
	U		U	Α	1	Р
	Р	L G C	U O Z	В	Т	N
	N	С	Z	Χ	1	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

- Adversary assumes that G is the ciphertext letter for E.
- Adversary replaces G with plaintext letter E in the sixth column.
- We can see,G = E + keywordLetter

$$G=6$$
 
$$E=4$$
 
$$6-4=2\pmod{26}$$

Hence keyword letter is C.

17/33

Keyword						С
	U	Υ	Е	В	V	Е
	М	Р	F	Χ	Α	٧
	U	U	Α	Е	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	Е
	U	U	Α	Е	Т	E P
	Α	R	W	Q	K	W
	A E X F E	RCLPGLGC	Α	Р	Q Z	N
	Х	L	G	M	Z	Е
	F	Р	W	Т	В	С
		G	F	Ζ	Т	C E P
	U	L	U	Α	1	
	Р	G	O Z	В	Т	N
	N	С	Ζ	Χ	1	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

- [	а	t	ы	С	П	d	е	f	g	h	i	j	k		m	n
Ì	0	1		2	!	3	4	5	6	7	8	9	10	11	12	13
- [	0	Τ	р		q		r	s	t	П	u	٧	w	Х	у	Z
- [	14	Т	15	П	1	6	17	18	19	9	20	21	22	23	24	25

Decrypt the remaining letters in the column.

• 
$$V - C = 21 - 2 = 19 = T$$

Keyword						С
	U	Υ	Е	В	V	Е
	М	Р	F	Χ	Α	V
	U	U	Α	Е	Т	Р
	Α	R	W	J	С	K
	Н	М	U	Т	В	Е
	U	U	Α	Е	Т	E P
	Α	R	W	Q	K	W
	E	С	Α	Р	Q Z	N
	E X F	L	G	M	Z	E C E P
	F	Р	W	Т	В	С
	E	G	F	Z	Т	Е
	U	L	U	Α	ı	Р
	Р	L G C	O Z	В	Т	N
	N	С	Ζ	Х	ı	Т
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

a	b	С	d	е	f	g	h	i	j	k	1	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р		q	r	s	t	Т	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	<del>∍</del> ⊤	20	21	22	23	24	25

Decrypt the remaining letters in the column.

• 
$$V - C = 21 - 2 = 19 = T$$

- Similarly, P as N, K as I, W as U, N as L, C as A, P as N, T as R.
- Replace all of them in the column.

Keyword						С
	U	Υ	Е	В	V	Ε
	M	Р	F	Х	Α	Т
	U	U	Α	E	T	Ν
	Α	R	W	J	T C	1
	Н	М	U	Т	В	Ε
	U	U	Α	T E	Т	Ν
	Α	R	W	Q P	T K	U
	A E X F	С	Α		Q Z	L
	Χ	C L P G	G	М	Z	L E A E
		Р	W	T Z	В	Α
	Ε	G	F	Z	Т	
	U	L	U	Α	1	Ν
	Р	L G C	O Z	В	Т	L R
	Ν	С	Ζ	Х	1	R
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

ſ	а	b	С	d	е	f	g	h	i	j	k	1	m	n
ſ	0	1	2	3	4	5	6	7	8	9	10	11	12	13
ſ	0	р	Т	q	r	s	t	П	u	٧	w	Х	у	Z
ĺ	14	15	5	16	17	18	1	9	20	21	22	23	24	25

- V C = 21 2 = 19 = T
- Similarly, P as N, K as I, W as U, N as L, C as A, O as M, T as R.
- Replace all of them in the column.

Keyword						С
	U	Υ	Е	В	V	Ε
	M	Р	F	X E	Α	Т
	U	U	Α		T	Ν
	Α	R	W	J	T C	1
	Н	М	U	Т	l B	Ε
	U	U	Α	T E	Т	Ν
	Α	R	W	Q	T K	U
	A E X F E	RCLPGLGC	Α	P	Q Z	L
	Χ	L	G	М	Z	L E A
	F	Р	W	Т	В	Α
	E	G	F	T Z	Т	Е
	U	L	U	Α	1	Ν
	Р	G	O Z	В	Т	L R
	Ν	С	Z	Х	1	R
	Р					
Most	U	?	W A	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	p		r	s	t	Т	u	٧	w	х	у	Z
14	15	5	16	17	18	1:	9	20	21	22	23	24	25

 Observe that first letter in the text is U.

Keyword						С
	U	Υ	Е	В	V	Е
	M	Р	F	Х	Α	Т
	U	U	Α	E	T	N
	Α	R	W	J	T C	1
	Н	М	U	Т	В	Ε
	U	U	Α	Е	Т	N
	Α	R	W	Q	K	U
	A E X F	С	Α	Р	Q	L
	Х	CLPGLGC	G	М	Q Z	L E A E
	F	Р	W	Т	В	Α
	Ε	G	F	T Z	Т	Е
	U	L	U	Α	1	N
	Р	G		В	Т	L
	Ν	С	O Z	Х	1	L R
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

а	b		,	d	е	f	g	h	1	i	j	k		m	n
0	1	1 2	2	3	4	5	6	7		8	9	10	11	12	13
0	Tp	,	7	7	r	s	t		ū	П	٧	W	Х	у	Z
14	1	5	-	16	17	18	1	9	2	0.	21	22	23	24	25

- Observe that first letter in the text is U.
- Which could be either A or I.

Keyword						С
	U	Υ	Е	В	V	Е
	M	Р	F	Х	Α	Т
	U	U	Α	E	T	N
	Α	R	W	J	T C	1
	Н	М	U	Т	В	Ε
	U	U	Α	Е	Т	N
	Α	R	W	Q	K	U
	A E X F	С	Α	Р	Q	L
	Х	CLPGLGC	G	М	Q Z	L E A E
	F	Р	W	Т	В	Α
	Ε	G	F	T Z	Т	Е
	U	L	U	Α	1	N
	Р	G		В	Т	L
	Ν	С	O Z	Х	1	L R
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

а	b		2	d	е	f	g	h	i	j	k		m	n
0	1	1	2	3	4	5	6	7	8	9	10	11	12	13
0	T	5	7	a	r	s	t	П	u	٧	W	Х	У	z
14	1	15	1	16	17	18	1	9	20	21	22	23	24	25

- Observe that first letter in the text is U.
- Which could be either A or I.
- Adversary guesses it as ciphertext U is a plaintext I.

20/33

Keyword						С
	U	Υ	Е	В	V	Е
	M	Р	F	X E	Α	Т
	U	U	Α	E	T	Ν
	Α	R	W	J	T C	1
	Н	М	U	Т	В	Ε
	U	U	Α	T E	Т	Ν
	Α	R	W	Q P	T K	U
	A E X F	С	Α	Р	Q Z	
	Х	L	G	М	Z	Ε
	F	Р	W	Т	В	Α
	Ε	L P G	F	T Z	Т	L E A E
	U	L	U	Α	1	Ν
	Р	L G C	O Z	В	Т	L R
	Ν	С	Z	Х	1	R
	Р					
Most	U	?	W	?	Т	G
repeated			Α			

а	b		,	d	е	f	g	h	i	j	k		m	n
0	1	1	2	3	4	5	6	7	8	9	10	11	12	13
0	T		7	7	r	s	t	П	u	٧	w	Х	У	Z
14	1	5	•	16	17	18	1	9	20	21	22	23	24	25

- Observe that first letter in the text is U.
- Which could be either A or I.
- Adversary guesses it as ciphertext U is a plaintext I.
- Replaces *U* by *I* in the first column.

Keyword						С
	I	Υ	Е	В	V	E T
	M	Р	F	Х	Α	
	1	U	Α	E	Т	Ν
	Α	R	W	J	T C	1
	Н	М	U	Т	l B	Ε
	1	U	Α	Е	Т	Ν
	Α	R	W	Q	T K	U
	Е	С	Α	Р	Q Z	L
	E X F	L	G	М	Z	L E A
	F	Р	W	Т	В	Α
	Ε	CLPGLGC	F	T Z	Т	Ε
	1	L	U	Α	1	Ν
	Р	G	0	В	Т	L R
	Ν	С	O Z	Х	1	R
	Р					
Most	U	?	W	?	Т	G
repeated			W A			

а	b	С	d	е	f	g	h	i	j	k	1	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	Т	q	r	S	t	П	u	٧	W	Х	у	Z
14	15	5	16	17	18	15	9	20	21	22	23	24	25

- Observe that first letter in the text is U.
- Which could be either A or I.
- Adversary guesses it as ciphertext U is a plaintext I.
- Replaces *U* by *I* in the first column.

KeywordLetter:

$$U - I = 20 - 8 = 12 = M$$



Keyword	М					С
	I	Υ	Е	В	٧	Е
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	Ν
	O V	R	W	J	T C	1
	V	М	U	Т .	В	Ε
	1	U	Α	T E	Т	Ν
	0 S	R	W	Q	K	U
	S	С	Α	Р	Q Z	L
	L	L	G	М	Z	Е
	L T S	Р	W	Т	В	Α
	S	CLPGLGC	F	Z	Т	LEAENLR
	1	L	U	Α	1	Ν
	D	G	O Z	В	Т	L
	В	С	Ζ	Х	1	R
	D					
Most	U	?	W A	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	П	q	r	s	t	Т	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

Adversary decrypts all the ciphertext letters in the first column.

 M as A, A as O, H as V, A as O, E as S, X as L, F as T, E as S, P as D, N as B, P as D.

Keyword	М					С
	1	Υ	Е	В	V	Ε
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	N
	0 V	R	W	J	С	1
	V	М	U	Т	В	Е
	1	U	Α	E	T	N
	O S	R	W	Q	K	U
	S	С	Α	Р	Q Z	L E
		L	G	М	Z	Ε
	L T S	Р	W	Т	В	Α
	S	L P G	F	Z	T	Ε
	1	L	U	Α	1	N
	D	L G C	O Z	В	T	L R
	В	С	Ζ	Х	1	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

ĺ	а	b	С	d	е	f	g	h	i	j	k		m	n
ĺ	0	1	2	3	4	5	6	7	8	9	10	11	12	13
ĺ	0	р	Т	q	r	s	t	Т	u	٧	W	Х	У	Z
ĺ	14	15	5	16	17	18	19	9	20	21	22	23	24	25

 You cannot get the message now.

I YE BV EAPFXAT I UAET NOR WJCIVMUTBE I UAET NOR WQKUSC A PQLL LGM ZETPWTB A SGFZTE ILUA IND G OBTL BC ZXIRD

Keyword	М					С
	I	Υ	Е	В	V	E T
	Α	Р	F	Х	Α	
	1	U	Α	E	Т	Ν
	O V	R	W	J	T C	1
	V	М	U	Т	l B	Ε
	1	U	Α	Е	Т	Ν
	0	R	W	Q	T K	U
	O S	С	Α	Р	Q Z	L
		L	G	М	Z	L E A
	L T S	Р	W	Т	В	Α
	S	CLPGLGC	F	T Z	Т	Ε
	1	L	U	Α	1	Ν
	D	G	O Z	В	Т	L R
	В	С	Ζ	Х	1	R
	D					
Most	U	?	W A	?	Т	G
repeated			Α			

I YE BV EAPFXAT I UAET NOR
WJCIVMUTBE I UAET NOR
WQKUSC A PQLL LGM
ZETPWTB A SGFZTE ILUA IND G
OBTL BC ZXIRD

 Adversary notices the 3-letter word IND.

Keyword	М					С
	I	Υ	Е	В	٧	Е
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	Ν
	0	R	W	J	С	1
	V	М	U	Т	В	E N
	1	U	Α	Е	Т	Ν
	0 S	R	W	Q	K	U
	S	С	Α	Р	Q Z	L
	L	L	G	М	Z	Ε
	T S	Р	W	T Z	В	Α
	S	P G L G C	F	Z	Т	LEAEN
	1	L	U	Α	1	
	D	G	O Z	В	Т	L R
	В	С	Ζ	Х	1	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

I YE BV EAPFXAT I UAET NOR
WJCIVMUTBE I UAET NOR
WQKUSC A PQLL LGM
ZETPWTB A SGFZTE ILUA IND G
OBTL BC ZXIRD

- Adversary notices the 3-letter word IND.
- He guess it as AND

Keyword	М					С
	I	Υ	Е	В	V	Е
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	Ν
	O V	R	W	J	С	1
	V	М	U	Т	В	E N
	1	U	Α	E	Т	Ν
	0	R	W	Q P	T K	U
	O S	RCLPGLGC	Α	Р	Q Z	L
		L	G W	М	Z	LEAE
	L T	Р	W	Т	В	Α
	S	G	F	Z	Т	Ε
	1	L	U	Α	1	N
	D	G	O Z	В	Т	L R
	В	С	Ζ	Х	1	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

I YE BV EAPFXAT I UAET NOR
WJCIVMUTBE I UAET NOR
WQKUSC A PQLL LGM
ZETPWTB A SGFZTE ILUA IND G
OBTL BC ZXIRD

- Adversary notices the 3-letter word IND.
- He guess it as AND
- The ciphertext letter I can decrypt as A in column 5.

Keyword	М					С
	I	Υ	Е	В	٧	Е
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	Ν
	0	R	W	J	С	1
	V	М	U	T E	В	E N
	1	U	Α	E	Т	Ν
	0	R	W	Q	K	U
	0 S	С	Α	Р	Q Z	L
		L	G	М	Z	Ε
	L T S	Р	W	T	В	Α
	S	P G L G C	F	T Z	Т	LEAEN
	1	L	U	Α	Α	Ν
	D	G	O Z	В	Т	L R
	В	С	Z	Х	1	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

I YE BV EAPFXAT I UAET NOR
WJCIVMUTBE I UAET NOR
WQKUSC A PQLL LGM
ZETPWTB A SGFZTE ILUA IND
OBTL BC ZXIRD

Keyword	М				Ι	С
	I	Υ	Е	В	٧	Е
	Α	Р	F	Х	Α	Т
	1	U	Α	E	Т	N
	0	R	W	J	С	1
	V	М	U	Т	В	E N
	1	U	Α	E	Т	N
	0	R	W	Q	K	U
	0 S	С	Α	Р	Q Z	L
	L	C L	G	М	Z	LEAE
	Т	Р	W	Т	В	Α
	S	P G	F	Z	Т	Ε
	1	L	U	Α	Α	Ν
	D	L G C	O Z	В	Т	L
	В	С	Ζ	Х	1	L R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

I YE BV EAPFXAT I UAET NOR
WJCIVMUTBE I UAET NOR
WQKUSC A PQLL LGM
ZETPWTB A SGFZTE ILUA IND G
OBTL BC ZXIRD

Now, the keyword letter is

$$I - A = 8 - 0 = 8 = I$$

Keyword	М				П	С
	I	Υ	Е	В	N	Е
	Α	Р	F	Х	S	Т
	1	U	Α	E	L	Ν
	0 V	R	W	J	U	1
	V	М	U	T E	Т	Ε
	1	U	Α	E	L C	Ν
	0 S	R	W	Q P	С	U
	S	С	Α		1	L
	L T	L	G	М	R	Е
		L P G	W	Т	Т	Α
	S	G	F	T Z	L	LEAEZ
	1	L	U	Α	Α	Ν
	D	L G C	O Z	В	L	L R
	В	С	Z	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	Т	q	r	s	t	Т	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

I YE BN EAPFXST I UAEL NOR
WJUIVMUTTE I UAEL NOR
WQCUSC A PILL LGM RETPWT
TA SGFZLE ILUA AND G OBLL
BC ZXARD

Keyword	М				I	С
	I	Υ	Е	В	N	Е
	Α	Р	F	Х	S	Т
	1	U	Α	E	L	N
	0 V	R	W	J	U	1
	V	М	U	T E	Т	E N
	1	U	Α	E	L C	N
	0 S	R	W	Q P	С	U
	S	С	Α		1	L
	L T	L	G	М	R	Е
		Р	W	Т	Т	Α
	S	L P G L G C	F	Z	L	LEAEZ
	1	L	U	Α	Α	Ν
	D	G	O Z	В	L	L R
	В	С	Ζ	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	Т	q	r	s	t	П	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

I YE BN EAPFXST I UAEL NOR WJUIVMUTTE I UAEL NOR WQCUSC A PILL LGM RETPWT TA SGFZLE ILUA AND G OBLL

- Two letter word BC.
- It could be BE or BY.
- Adversary guesses it as BE.

Ciphertext C encrypted as E

January 21, 2021

Keyword	М				I	С
	I	Υ	Е	В	N	Е
	Α	Р	F	Х	S	Т
	1	U	Α	E	L	N
	0 V	R	W	J	U	1
	V	М	U	T E	Т	E N
	1	U	Α	E	L C	N
	0 S	R	W	Q P	С	U
	S	С	Α		1	L
	L T	L	G	М	R	Е
		L P G	W	Т	Т	Α
	S	G	F	Z	L	LEAEZ
	1	L	U	Α	Α	Ν
	D	L G E	O Z	В	L	L R
	В	Ε	Ζ	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	Т	q	r	s	t	П	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

I YE BN EAPFXST I UAEL NOR
WJUIVMUTTE I UAEL NOR
WQCUSC A PILL LGM RETPWT
TA SGFZLE ILUA AND G OBLL
BC ZXARD

- Two letter word BC.
- It could be BE or BY.
- Adversary guesses it as BE.

Ciphertext C encrypted as E

Keyword	М	Υ			I	С
	I	Υ	Е	В	N	Е
	Α	Р	F	Х	S	Т
	1	U	Α	E	L	Ν
	0	R	W	J	U	1
	٧	М	U	T E	Т	Ε
	1	U	Α	E	L C	Ν
	0 S	R	W	Q P	С	U
	S	С	Α		1	L
	L	L	G	М	R	Ε
	L T	L P G	W	Т	Т	Α
	S	G	F	T Z	L	LEAEZ
	1	L	U	Α	Α	Ν
	D	L G E	O Z	В	L	L R
	В	Ε	Z	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	Тр	Т	q	r	s	t	Т	u	٧	W	Х	у	Z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

#### Keyword letter is

• 
$$C - E = 2 - 4 = -2$$
  
 $(\text{mod } 26) = 24 = Y$ 



Keyword	М	Υ			ı	С
	1	Α	E F	В	N	Е
	Α	R	F	Х	S	Т
	1	W	Α	E	L	N
	0 V	Т	W	E J	L U	1
	V	O W	U	Т	Т	E N
	1	W	Α	E	L C	N
	O S	T E	W	T E Q P	С	U
	S	Е	Α		I	ULEAEN
		N	A G	М	R	Е
	L T S	R	W	Т	Т	Α
	S	1	F	Ζ	L	Е
	1	N	U	Α	Α	
	D	1	O Z	T Z A B	L	L R
	В	Е	Z	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

а	b	С	d	е	f	g	h	i	j	k		m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	р	Т	q	r	s	t	П	u	٧	w	Х	у	z
14	15	5	16	17	18	19	9	20	21	22	23	24	25

I AE BN EARFXST I WAEL NOT WJUIVOUTTE I WAEL NOT WQCUSE A PILL NGM RETRWT TA SIFZLE INUA AND I OBLL BE ZXARD

Keyword	М	Υ			I	С
	I	Α	Е	В	N	Е
	Α	R	F	Х	S	Т
	1	W	Α	Е	L	N
	0 V	Т	W	J	L U	1
	V	O W	U	T E	Т	E N
	1		Α	E	L C	N
	0 S	T E	W	Q P	С	U
	S	Е	Α		ı	L
	L	N	G	М	R	$\square$ $\square$ $\square$ $\square$
	L T	R	W	Т	Т	Α
	S	1	F	T Z	L	Е
	1	N	U	Α	Α	N
	D	1	O Z	В	L A	L R
	В	Е	Z	Х	Α	R
	D					
Most	U	?	W	?	Т	G
repeated			Α			

ſ	а	b	С	d	е	f	g	h	i	j	k	1	m	n
Ī	0	1	2	3	4	5	6	7	8	9	10	11	12	13
ſ	0	р		q	r	S	t		u	٧	W	Х	у	Z
Γ	14	15	5	16	17	18	15	9	20	21	22	23	24	25

I AE BNEARFXST I WAEL NOT WJUIVOUTTE I WAEL NOT WQCUSE A PILL NGM RETRWT TA SIFZLE INUA AND I OBLL BE ZXARD

- Adversary looks for words
- He can see the word EARFXST
- Guesses as EARNEST

Keyword	М	Υ	S	Т	I	С
	Ι	Α	Е	В	N	Е
	Α	R	N	Е	S	Т
	1	W	Α	E	L	Ν
	0 V	Т	W	J	L U	1
	V	O W	U	Т	Т	E N
	1	W	Α	E	T L C	N
	0 S	T E	W	T E Q P	С	U
	S	E	Α	Р	1	L
	L	N	G	М	R	Е
	L T	R	W	T	Т	Α
	S	1	F	Z A	L	Е
	1	N	U	Α	L A	N
	D	1	O Z	В	L A	ULEAENLR
	В	Е	Ζ	Х	Α	R
	B D					
Most	U	?	W	?	Т	G
repeated			Α			

I AE BNEARFXST I WAEL NOT WJUIVOUTTE I WAEL NOT WQCUSE A PILL NGM RETRWT TA SIFZLE INUA AND I OBLL BE ZXARD

#### Keyword Letters are

Column2:

$$F - N = 5 - 13 = -8$$
  
(mod 26) =  $18 = S$ 

Column3:

$$X - E = 23 - 4 = 19 = T$$



Keyword	М	Υ	S	Т	П	С
	Τ	Α	М	Τ	N	Е
	Α	R	N	Е	S	Τ
	1	W	1	L	L	N
	0	Т	Ε	Q	U	1
	V	0	С	Α	Т	E
	1	W	1	L	L	N
	0	Т	Е	X W	С	U
	O S	Е	1	W	1	L
	L T S	N	0	Т	R	L E
	Т	R	Е	Α	Т	Α
	S	1	N	G	L	A E N
	1	N	С	Н	Α	N
	D	1	W	1	L	L
	В	Е	Н	Е	Α	R
	D					

I AM IN EARNEST I WILL NOT EQUIVOCATE I WILL NOT EXCUSE I WILL NOT RETREAT A SINGLE INCH AND I WILL BE HEARD

- Now, it is readable text.
- The keyword is MYSTIC

- Used to determine *m* (keyword length)
- To confirm m, determined by Kasiski test

#### **Definition**

Suppose  $X = x_1 x_2, ..., x_n$  is a string of length n. Then index of coincidence of X, denoted by  $I_c(X)$ , is defined to be the probability that two random elements of X are identical.

• Denoted the frequencies of  $A, B, \ldots, Z$  in X by  $f_0, f_1, \ldots, f_{25}$ 

$$I_c(X) = \frac{\sum_{i=0}^{25} {f_i \choose 2}}{{n \choose 2}} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}$$



33/33

(IIIT Sri City) January 21, 2021

If X is a string of English Language text, then

$$I_C(X) \approx \sum_{i=0}^{25} p_i^2 = 0.065$$

where occurrences of  $A, B, \ldots, Z$  are  $p_0, p_1, \ldots, p_{25}$ , respectively.

- The probability that two random elements both are A is  $p_0^2$ , both are B is  $p_1^2$ , and so on.
- The same reasoning applies if X is a ciphertext string obtained using any monoalphabetic cipher.



#### Shift Cipher (Monoalphabetic Cipher)

plaintext : classical encryptions

cipher : FODVVLFDO HQFUBSWLRQV

#### Shift Cipher (Monoalphabetic Cipher)

plaintext : classical encryptions cipher : FODVVLFDO HQFUBSWLRQV

#### Polyalphabetic Cipher (Vigenere Cipher)

#### Vigenere Cipher

#### Shift Cipher (Monoalphabetic Cipher)

plaintext : classical encryptions

cipher : FODVVLFDO HQFUBSWLRQV

#### Polyalphabetic Cipher (Vigenere Cipher)

#### Vigenere Cipher

#### Frequencies of individual letters

Frequencies of individual le											
a	.	b	(	)	d		е		f	g	
7		4	4	4	0		5		3	7	
h		i	j		k				m	n	٦
1		2	1		2		2		3	3	
0		р	(	7	r		S		t	u	
1		8	2	2	2		0		7	8	
\	/	W	· >		Κ		у		z		
2	2	4	4 3		3		1		3		

#### Polyalphabetic Cipher (Vigenere Cipher)



#### Polyalphabetic Cipher (Vigenere Cipher)



Frequencies of individual letters in column-wise:

#### Polyalphabetic Cipher (Vigenere Cipher)



Frequencies of individual letters in column-wise:

Keyword is MYSTIC

# Thank You