Conventional Encryption Techniques

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

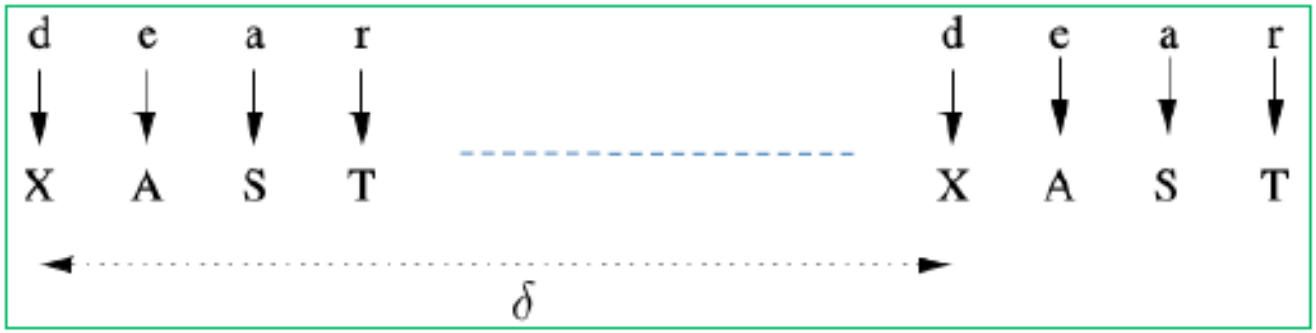
January 21, 2021

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 δ apart and $(m \mid \delta)$



when (m divides δ)

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

Determining Key Length (Kasiski Test)

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

Determining Key Length (Kasiski Test)

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	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Determining Key Length (Kasiski Test)

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	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Trigram	No.of Occ	Dist

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Trigram	No.of Occ	Dist

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Trigram	No.of Occ	Dist
UUA	2	18

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Trigram	No.of Occ	Dist
UUA	2	18

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

1	2	3	4	5	6	7	8	9	10	11	12
U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

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

Determining Key Length (Kasiski Test)

Adversary Attempt to Recover the Plaintext

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

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

Determining Key Length (Kasiski Test)

Adversary Attempt to Recover the Plaintext

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

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.

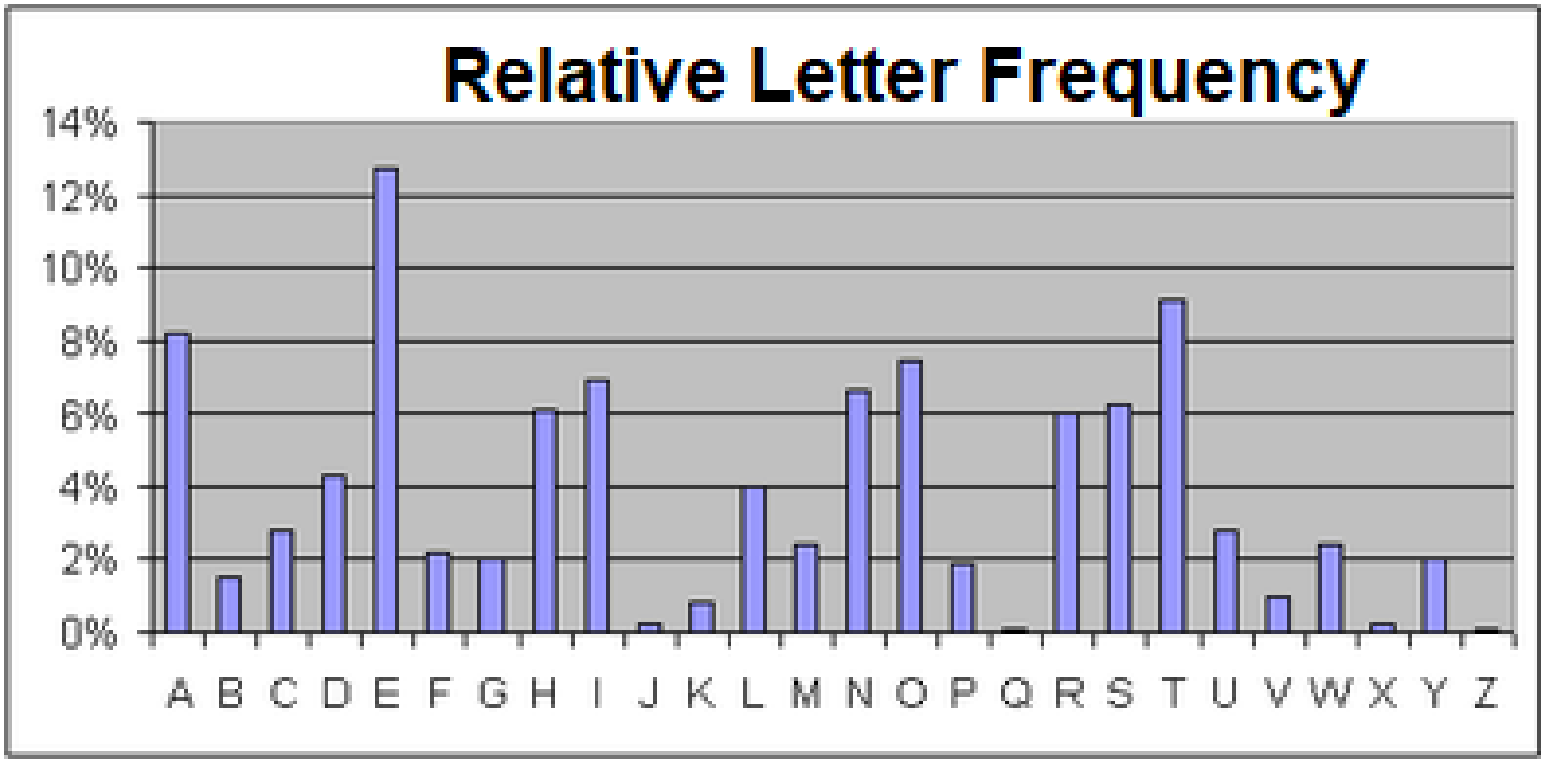
Determining Key Length (Kasiski Test)

Keyword						
	U	Y	E	B	V	G
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	G
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	G
	F	P	W	T	B	C
	E	G	F	Z	T	G
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

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*.

Determining Key Length (Kasiski Test)

Keyword						
	U	Y	E	B	V	G
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	G
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	G
	F	P	W	T	B	C
	E	G	F	Z	T	G
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

- Adversary assumes that G is the ciphertext letter for E.

Determining Key Length (Kasiski Test)

Keyword						
	U M U A H U A E X F E U P N P	Y P U R M U R C L P G L G C	E F A W U A W A G W F U O Z	B X E J T E Q P M T Z A B X	V A T C B T K Q Z B T I T I	E V P K E P W N E C E P N T
Most repeated	U	?	W A	?	T	G

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

Determining Key Length (Kasiski Test)

Keyword						
	U	Y	E	B	V	E
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	E
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	E
	F	P	W	T	B	C
	E	G	F	Z	T	E
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

- 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.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	E
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	E
	F	P	W	T	B	C
	E	G	F	Z	T	E
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

- 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.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	E
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	E
	F	P	W	T	B	C
	E	G	F	Z	T	E
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	20	21	22	23	24	25		

Decrypt the remaining letters in the column.

- $V - C = 21 - 2 = 19 = T$

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	V
	U	U	A	E	T	P
	A	R	W	J	C	K
	H	M	U	T	B	E
	U	U	A	E	T	P
	A	R	W	Q	K	W
	E	C	A	P	Q	N
	X	L	G	M	Z	E
	F	P	W	T	B	C
	E	G	F	Z	T	E
	U	L	U	A	I	P
	P	G	O	B	T	N
	N	C	Z	X	I	T
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	T
	U	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	U	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	U	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	T
	U	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	U	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	U	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	20	21	22	23	24	25		

- Observe that first letter in the text is *U*.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	T
	U	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	U	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	U	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	20	21	22	23	24	25		

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

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	T
	U	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	U	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	U	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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*.

Determining Key Length (Kasiski Test)

Keyword						C
	U	Y	E	B	V	E
	M	P	F	X	A	T
	U	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	U	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	U	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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.

Determining Key Length (Kasiski Test)

Keyword						C
	I	Y	E	B	V	E
	M	P	F	X	A	T
	I	U	A	E	T	N
	A	R	W	J	C	I
	H	M	U	T	B	E
	I	U	A	E	T	N
	A	R	W	Q	K	U
	E	C	A	P	Q	L
	X	L	G	M	Z	E
	F	P	W	T	B	A
	E	G	F	Z	T	E
	I	L	U	A	I	N
	P	G	O	B	T	L
	N	C	Z	X	I	R
	P					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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:

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

Determining Key Length (Kasiski Test)

Keyword	M					C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	I	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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.

Determining Key Length (Kasiski Test)

Keyword	M					C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	I	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

Determining Key Length (Kasiski Test)

Keyword	M					C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	I	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

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.

Determining Key Length (Kasiski Test)

Keyword	M					C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	I	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

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

Determining Key Length (Kasiski Test)

Keyword	M					C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	I	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

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.

Determining Key Length (Kasiski Test)

Keyword	M				I	C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	A	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

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

Determining Key Length (Kasiski Test)

Keyword	M				I	C
	I	Y	E	B	V	E
	A	P	F	X	A	T
	I	U	A	E	T	N
	O	R	W	J	C	I
	V	M	U	T	B	E
	I	U	A	E	T	N
	O	R	W	Q	K	U
	S	C	A	P	Q	L
	L	L	G	M	Z	E
	T	P	W	T	B	A
	S	G	F	Z	T	E
	I	L	U	A	A	N
	D	G	O	B	T	L
	B	C	Z	X	I	R
	D					
Most repeated	U	?	W A	?	T	G

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

Determining Key Length (Kasiski Test)

Keyword	M				I	C
	I	Y	E	B	N	E
	A	P	F	X	S	T
	I	U	A	E	L	N
	O	R	W	J	U	I
	V	M	U	T	T	E
	I	U	A	E	L	N
	O	R	W	Q	C	U
	S	C	A	P	I	L
	L	L	G	M	R	E
	T	P	W	T	T	A
	S	G	F	Z	L	E
	I	L	U	A	A	N
	D	G	O	B	L	L
	B	C	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

Determining Key Length (Kasiski Test)

Keyword	M				I	C
	I	Y	E	B	N	E
	A	P	F	X	S	T
	I	U	A	E	L	N
	O	R	W	J	U	I
	V	M	U	T	T	E
	I	U	A	E	L	N
	O	R	W	Q	C	U
	S	C	A	P	I	L
	L	L	G	M	R	E
	T	P	W	T	T	A
	S	G	F	Z	L	E
	I	L	U	A	A	N
	D	G	O	B	L	L
	B	C	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

Determining Key Length (Kasiski Test)

Keyword	M				I	C
	I	Y	E	B	N	E
	A	P	F	X	S	T
	I	U	A	E	L	N
	O	R	W	J	U	I
	V	M	U	T	T	E
	I	U	A	E	L	N
	O	R	W	Q	C	U
	S	C	A	P	I	L
	L	L	G	M	R	E
	T	P	W	T	T	A
	S	G	F	Z	L	E
	I	L	U	A	A	N
	D	G	O	B	L	L
	B	E	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

Determining Key Length (Kasiski Test)

Keyword	M	Y			I	C
	I	Y	E	B	N	E
	A	P	F	X	S	T
	I	U	A	E	L	N
	O	R	W	J	U	I
	V	M	U	T	T	E
	I	U	A	E	L	N
	O	R	W	Q	C	U
	S	C	A	P	I	L
	L	L	G	M	R	E
	T	P	W	T	T	A
	S	G	F	Z	L	E
	I	L	U	A	A	N
	D	G	O	B	L	L
	B	E	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	20	21	22	23	24	25		

Keyword letter is

- $C - E = 2 - 4 = -2 \pmod{26} = 24 = Y$

Determining Key Length (Kasiski Test)

Keyword	M	Y			I	C
	I	A	E	B	N	E
	A	R	F	X	S	T
	I	W	A	E	L	N
	O	T	W	J	U	I
	V	O	U	T	T	E
	I	W	A	E	L	N
	O	T	W	Q	C	U
	S	E	A	P	I	L
	L	N	G	M	R	E
	T	R	W	T	T	A
	S	I	F	Z	L	E
	I	N	U	A	A	N
	D	I	O	B	L	L
	B	E	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

Determining Key Length (Kasiski Test)

Keyword	M	Y			I	C
	I	A	E	B	N	E
	A	R	F	X	S	T
	I	W	A	E	L	N
	O	T	W	J	U	I
	V	O	U	T	T	E
	I	W	A	E	L	N
	O	T	W	Q	C	U
	S	E	A	P	I	L
	L	N	G	M	R	E
	T	R	W	T	T	A
	S	I	F	Z	L	E
	I	N	U	A	A	N
	D	I	O	B	L	L
	B	E	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	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

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

Determining Key Length (Kasiski Test)

Keyword	M	Y	S	T	I	C
	I	A	E	B	N	E
	A	R	N	E	S	T
	I	W	A	E	L	N
	O	T	W	J	U	I
	V	O	U	T	T	E
	I	W	A	E	L	N
	O	T	W	Q	C	U
	S	E	A	P	I	L
	L	N	G	M	R	E
	T	R	W	T	T	A
	S	I	F	Z	L	E
	I	N	U	A	A	N
	D	I	O	B	L	L
	B	E	Z	X	A	R
	D					
Most repeated	U	?	W A	?	T	G

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 Letters are

- Column2:
  $F - N = 5 - 13 = -8 \pmod{26} = 18 = S$
- Column3:
  $X - E = 23 - 4 = 19 = T$

Determining Key Length (Kasiski Test)

Keyword	M	Y	S	T	I	C
	I	A	M	I	N	E
	A	R	N	E	S	T
	I	W	I	L	L	N
	O	T	E	Q	U	I
	V	O	C	A	T	E
	I	W	I	L	L	N
	O	T	E	X	C	U
	S	E	I	W	I	L
	L	N	O	T	R	E
	T	R	E	A	T	A
	S	I	N	G	L	E
	I	N	C	H	A	N
	D	I	W	I	L	L
	B	E	H	E	A	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

Index of Coincidence (Friedman)

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

Definition

Suppose $X = x_1 x_2, \ldots, x_n$ 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 $f_0, f_1, \ldots, f_{25}$

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

Index of Coincidence (Friedman)

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.

Index of Coincidence (Friedman)

Shift Cipher (Monoalphabetic Cipher)

plaintext	:	classical	encryptions
cipher	:	FODVVLFDO	HQFUBSWLRQV

Index of Coincidence (Friedman)

Shift Cipher (Monoalphabetic Cipher)

plaintext	:	classical encryptions
cipher	:	FODVVLFDO HQFUBSWLRQV

Polyalphabetic Cipher (Vigenere Cipher)

Vigenere Cipher

U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Index of Coincidence (Friedman)

Shift Cipher (Monoalphabetic Cipher)

plaintext : classical encryptions
cipher : FODVVLFDO HQFUBSWLRQV

Polyalphabetic Cipher (Vigenere Cipher)

Vigenere Cipher

U	Y	E	B	V	G	M	P	F	X	A	V
U	U	A	E	T	P	A	R	W	J	C	K
H	M	U	T	B	G	U	U	A	E	T	P
A	R	W	Q	K	W	E	C	A	P	Q	N
X	L	G	M	Z	G	F	P	W	T	B	C
E	G	F	Z	T	G	U	L	U	A	I	P
P	G	O	B	T	N	N	C	Z	X	I	T
P											

Frequencies of individual letters

a	b	c	d	e	f	g
7	4	4	0	5	3	7

h	i	j	k	l	m	n
1	2	1	2	2	3	3

o	p	q	r	s	t	u
1	8	2	2	0	7	8

v	w	x	y	z
2	4	3	1	3

Index of Coincidence (Friedman)

Polyalphabetic Cipher (Vigenere Cipher)

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

Index of Coincidence (Friedman)

Polyalphabetic Cipher (Vigenere Cipher)

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

Frequencies of individual letters in column-wise:

Index of Coincidence (Friedman)

Polyalphabetic Cipher (Vigenere Cipher)

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

Frequencies of individual letters in column-wise:

Keyword is MYSTIC

Thank You