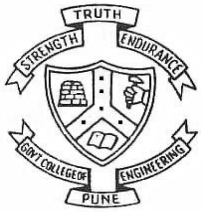
Cryptography and Network Security

Session 6

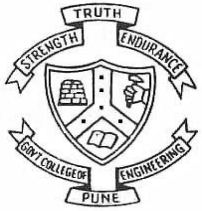
Dr. V. K. Pachghare



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

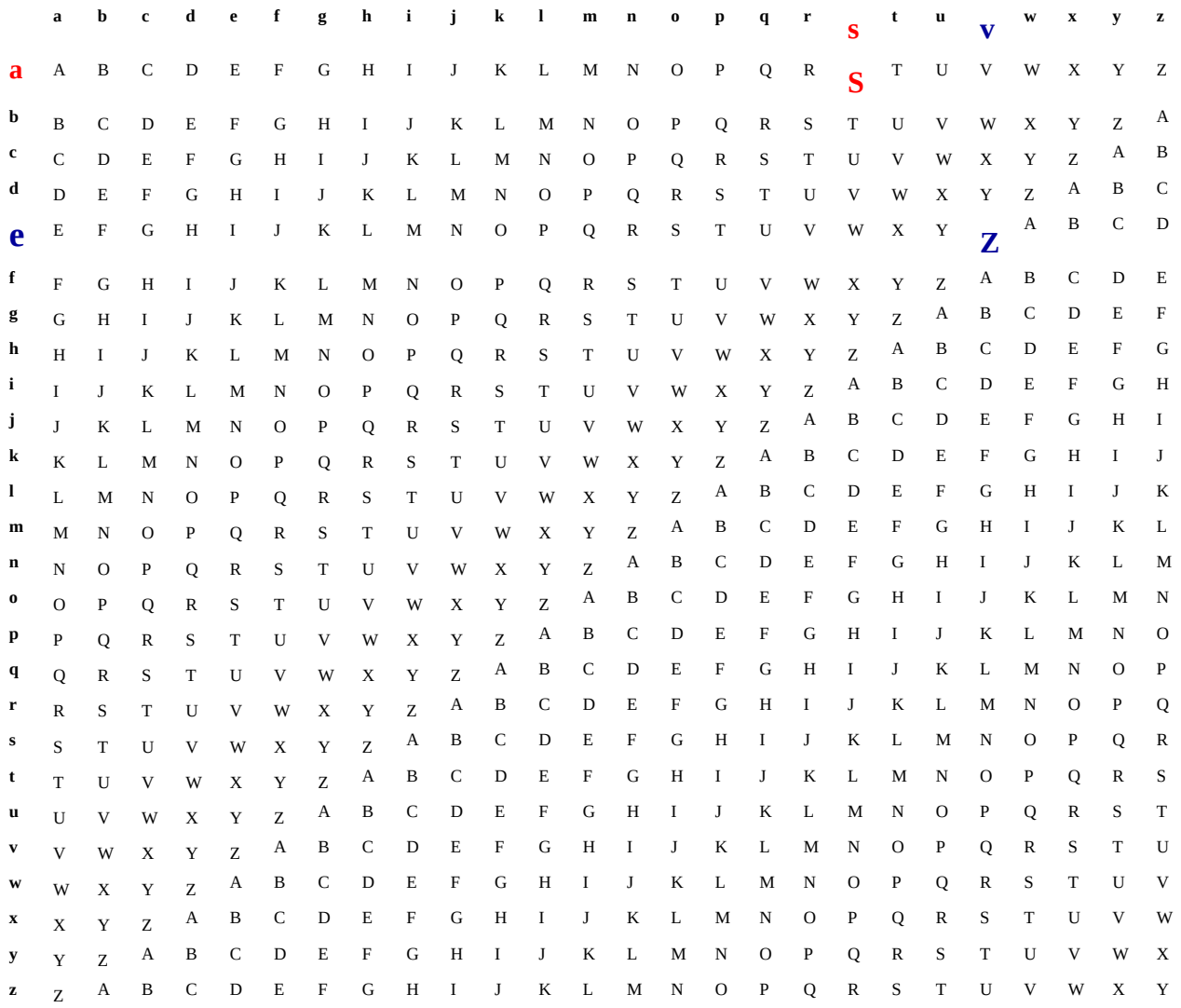
Classical Encryption Techniques

- Polyalphabetic Ciphers
- Transposition ciphers



Polyalphabetic Ciphers

- The keyspace consists of all ordered permutations of the alphabet called a Vigenere square.
- There are 26 rows that can be used as keys, each numbered with the amount they are shifted.


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
a 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
S
V
Z

- Create a master-key that specifies which order the keys (or rows) are to be used in. This does not have to include all rows.
- For example we could use k = (5, 2, 16) and then cycle through these three keys. This would mean every third letter is encrypted with the same key.
- For each single letter, you are using only 1 key and encryption and decryption works as with monoalphabetic ciphers.

- One finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the ciphertext letter.

Key: ant

Plaintext: technology

a n t a n t a n t a (Row)

t e c h n o l o g y (Column)

T R V H A H L B Z Y

		Plaintext								
		c	e	g	h	l	n	o	t	y
KEY	a	C	E	G	H	L	N	O	T	Y
	n	P	R	T	U	Y	A	B	G	L
	t	V	X	Z	A	E	G	H	M	R

Ciphertext is TRVHAHLBZY

- **Plaintext:** She is very happy and beautiful girl
- **Keyword:** ‘another’

Keyword:	anoth				erano				thera			nothe			ranot			heran						
Plaintext:	sheis				veryh				appya			ndbea			utifu			lgirl						
CT:	SUSBZ				ZVRLV				TWTPA			ARULE			LTVTN			SKZRY						

	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
a	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
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Decryption

Keyword:	a	n	o	t	h	e	r	a	n	o	t	h	e	r	a	n	o	t	h	e	r	a	n	
Ciphertext:	S	U	S	B	Z	Z	V	R	L	V	T	W	T	P	A	A	R	U	L	E	L	T	V	T
PT:	s	h	e	i	s	v	e	r	y	h	a	p	p	y	a	n	d	b	e	a	u	t	i	f

	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
a	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
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Advantages

- For the same plaintext letter, there are multiple ciphertext.
- This helps to avoid the frequency analysis of the cipher.
- For example, in the above plaintext there are 3 e's that they have been encrypted by 'S,' 'V,' 'L', respectively.
- Plaintext: sh**e**is v**e**ryh appya ndb**e**a utifu lgirl
  CT: SU**S**BZ Z**V**RLV TWTPA ARU**L**E LTVTN SKZRY

- This helps to hide the count of occurrence of e in the plaintext.
- So, it makes frequency analysis of the letters in the plaintext difficult.
- The implementation of this cipher is easy.

Disadvantages

- If the attacker is able to find out the **length of the key**, then frequency analysis is possible.
- The chosen-plaintext attack is possible against this cipher.

Transposition ciphers

Transposition ciphers

- Letters are written in a row under the key
- Arrange the column as per alphabetical order.
- Transposition ciphers encrypt plaintext by moving small pieces of the message around
- There are two types of transposition ciphers:
  - single columnar and
  - double columnar transposition ciphers

Single columnar transposition

- The total encryption process is divided into three parts:
  - Preparing the Key
  - Preparing the Plaintext
  - Encryption

Preparing the Key

- Suppose the key is '**another'.**
- We can assign the number to each letter in this key
- The first letter 'a' is numbered **1**.
- There are no 'B', 'C' or 'D', so the next letter to be numbered is the 'e'. So e is numbered 2, followed by h, and so on.

a n o t h e r 1

a n o t h e r

1 2

a n o t h e r

1 3 2

a n o t h e r

1 4 3 2

a n o t h e r

1 4 5 3 2

a n o t h e r

1 4 5 3 2 6

a n o t h e r

1 4 5 7 3 2 6

- In the key word if the same letter is occurred more than one time, it should be numbered 1, 2, 3 etc. from left to write for ex. Key word is **heaven**

h	**e**	a	v	**e**	n
4	**2**	1	6	**3**	5

Preparing the Plaintext

- The letters from the message is written in rows under the numbered letters of the key.
- One letter from message is to be written under each letter of the key.
- Suppose the message is

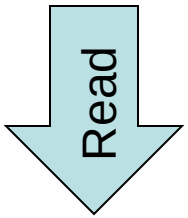
“we are the best”

- Next the plaintext "We are the best" is written in rows under the numbered keyword

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A	R	E	T
H	E	B	E	S	T

Encryption

- Now, arrange the above message written in rows under the numbered letters of the key as per ascending order of the numbers at the top of the plaintext letters.



a	e	e	h	n	v
1	2	3	4	5	6
A	E	E	W	T	R
B	E	S	H	T	E

- Then the letters are copied down column wise from top to bottom. The result is ciphertext, i.e.,

AB EE ES WH TT RE

- The ciphertext is

AB EE ES WH TT RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5
		A			
		B			

- The ciphertext is

AB EE ES WH TT RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5
	E	**A**			
	E	**B**			

- The ciphertext is

AB EE **ES** WH TT RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5
	E	A		**E**	
	E	B		**S**	

- The ciphertext is

AB EE ES **WH** TT RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A		E	
H	E	B		S	

- The ciphertext is

AB EE ES WH **TT** RE

Decryption-

h	e	a	v	e	n
4	2	1	6	3	5
W	E	A		E	**T**
H	E	B		S	**T**

- The ciphertext is

AB EE ES WH TT **RE**

Decryption-

	h	e	a	v	e	n
	4	2	1	6	3	5
Read	W	E	A	**R**	E	T
	H	E	B	**E**	S	T

Plaintext: WEARETHEBEST

WE ARE THE BEST

Double Columnar Transposition

- Double columnar transposition is similar to single columnar transposition, but the process is repeated twice.
- One either uses the same keyword both times or, preferably, a different one on the second occasion.

- Let's encrypt the text
- “we are the best”
- using the keywords **“heaven” and “another”**

h e a v e n

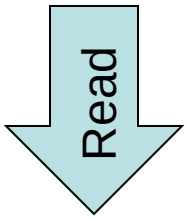
4 2 1 6 3 5

W E A R E T

H E B E S T

Encryption

- Now, arrange the above message written in rows under the numbered letters of the key as per ascending order of the numbers at the top of the plaintext letters.



a	e	e	h	n	v
1	2	3	4	5	6
A	E	E	W	T	R
B	E	S	H	T	E

- Then the letters are copied down column wise from top to bottom. The result is ciphertext, i.e.,

AB EE ES WH TT RE

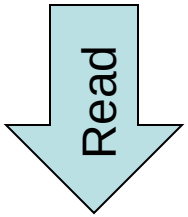
a n o t h e r

1 4 5 7 3 2 6

A B E E E S W

H T T R E

- If the last row like the above example, having less letters than the first row, then we can add some more letters to complete the row.
- But this reduces the security of the cipher.
- So, one can encrypt the plaintext by not adding any dummy letters in the last row.
- Rearrange the columns in ascending order.



a	e	h	n	o	r	t
1	2	3	4	5	6	7
A	S	E	B	E	W	E
H		E	T	T		R

Ciphertext: AHSEEBTETWER

Cryptanalysis

- Ciphertext:

GSMOEVMTEFMTPYPEIRSPIOEVIEEOMP

- Count the number of letters in the ciphertext. There are 30 letters in the ciphertext.
- Assuming the possible dimension of an array. The array could have any of the following dimensions:

6 x 5, 5 x 6, 10 x 3 or 3 x 10. Suppose that we first try a 6 x *5* array. This helps us to guess the key length. For this array, the key length is 6. Then the ciphertext array is as shown in Table

1	2	3	4	5	6
G	V	M	E	I	E
S	M	T	I	O	E
M	T	P	R	E	O
O	E	Y	S	V	M
E	F	P	P	I	P

- Now observe the top row of the array in Table and try to find the meaningful word. As per this word identify the column and permute these columns. After permutation, we observe the word GIVE in the first row. Also there are words or partial words in the other rows. If this gives meaning statement then, the key is almost recovered.

1	5	2	6	3	4
G	I	V	E	M	E
S	O	M	E	T	I
M	E	T	O	P	R
O	V	E	M	Y	S
E	L	F	P	P	P

- Plaintext is

"GIVEMESOMETIMETOPROVEMYSELFPPP"

GIVE ME SOME TIME TO PROVE MYSELF".

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message.

This can be achieve by concealing the existence of **information** within seemingly harmless **carriers or cover**

- **Carrier:** text, image, video, audio, etc

Question

Salutations, Mr. Robertson of CIS 5371. The Florida Society of Math and Cryptography is proud to present you with an small exam for qualification into our society. The key for passing is studying. Cryptography is rigorous and only those with patience in themselves pass. We have an exam PO Box in Tallahassee. But please submit by 12/12.

Answer

Salutations, Mr. Robertson of CIS 5371. **The** Florida Society of Math and **Cryptography** is proud to present you with an small **exam** for qualification into our society. The **key** for passing is studying. Cryptography **is** rigorous and only those with patience **in** themselves pass. We have an exam **PO Box** in Tallahassee. But please submit by **12/12**.

The Cryptography exam key is in PO Box 1212.

Thanks!!!