INFORMATION SECURITY
LECTURE 4
CRYPTANALYSIS OF SYMMETRIC CIPHERS

Khalid Abdullah

MSc computer and Network Security

Computer Science Dept.

University Of Zakho

Last Lecture

- Vernam or one time pad
- Cryptanalysis of symmetric ciphers
- Cryptography Terminology
- Frequency distribution table
- Kasiski method

Outline

- Transposition ciphers (such as Rail Fence cipher)
- Column transposition cipher
- Double Transposition Cipher

TRANSPOSITIONS (PERMUTATIONS)

- Transposition

  An encryption in which the letters of the message are rearranged.

Permutaion

  a transposition is a rearrangement of the symbols of a message

TRANSPOSITION CIPHERS

- A transposition cipher does not substitute one symbol for another, instead the location of the symbols.
- For instant, a symbol in the first position in the plaintext may appear in the tenth position of the ciphertext. We can say, a transposition cipher reorders(transpose) the symbols.
- The simplest such cipher is the rail fence technique.
- in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

TRANSPOSITION CIPHERS

- These hide the message by rearranging the letter order without altering the actual letters used.
- can recognise these since have the same frequency distribution as the original text

Substitution vs. Transposition

– The goal of a substitution: **confusion**

– The goal of a transposition: **diffusion**

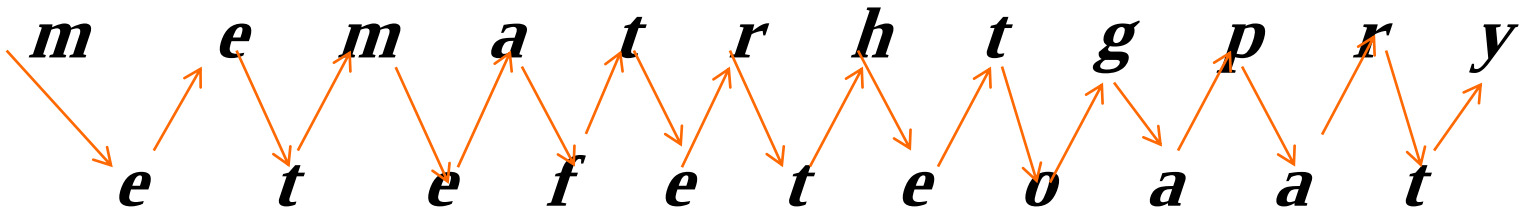
A transposition Cipher reorders symbols

Rail Fence cipher

- The simplest such cipher is the **Rail Fence cipher.**
- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

TRANSPOSITION CIPHERS

- For example, to encipher the Bob message to Alis "***meet me after the toga party***" with a rail fence of depth 2, we write the
- following:



RAIL FENCE CIPHER

- Then creation of encrypted message is:
- M e m a t r h t g p r y e t e f e t e o a a t .

sending the first row followed by the second row.

Does the Rail Fence secure?

All you needs to know that is rail fence had been used

How to decrypt the rail fence

- Decipher (MEMATRHTGPRYETEFETEOAAT)
- In order to decode the message(when depth=2):
  - Splitting the message in half
  - If the message has an odd number of letters, then split the message one letter to the right of the centre .

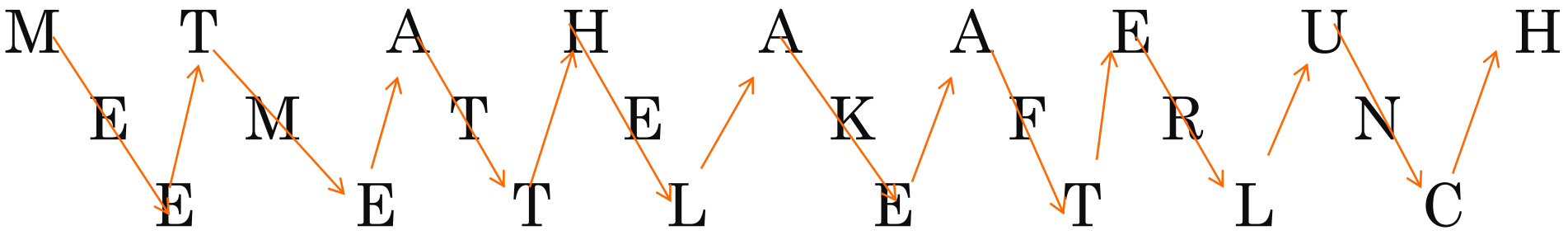
Our message has 23 letters and so split after the 12th letter.

MEMATRHTGPRY ETEFETEOAAT

Reading the original message by writing down the first letter of the left half, then the first letter of the right half, then the second letter from the left half, then the second letter from the right half, and so on.

Rail Fence cipher…

- **Example**: encipher the message" meet me at the lake after lunch" , choosing rail=3;

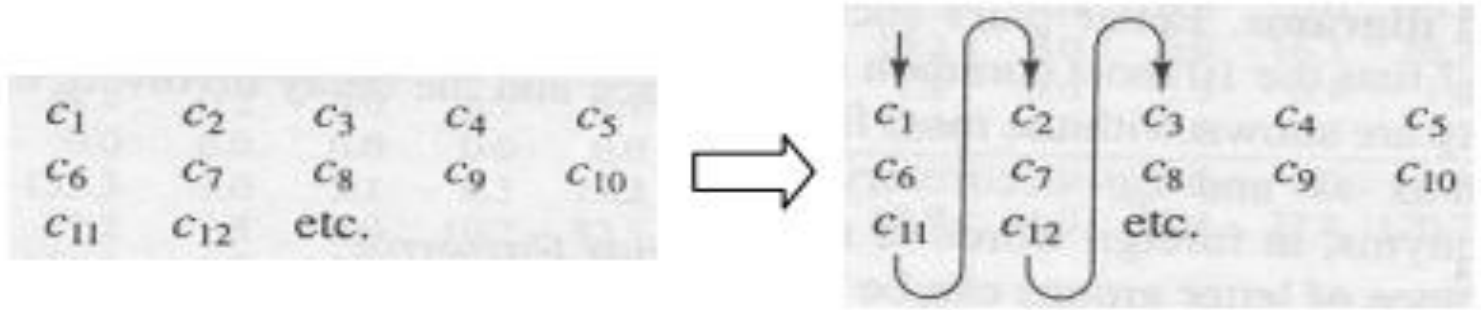


The ciphertext is:

MTAHAAEUHEMTEKFRNEETLETLC

2. COLUMN TRANSPOSITION CIPHER

- Columnar Transposition
  - A rearrangement of the characters of the plaintext into columns.



- Exapmle This is a message to show how a columnar transposition works

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns

- Alice and Bob can agree on the number of columns and use the second method. Alice write the same plaintext (Meet me at the park), row by row, in table of four columns.

M	**E**	**E**	**T**
M	E	A	T
T	H	E	P
A	R	K	

- She then creates the ciphertext

"MMTAEEHREAEKTTP" by transmitting the Characters column by column.

COLUMN TRANSPOSITION CIPHER

- **Example**:

  key=4312567

  plaintext= attack postponed until two am xyz

key	4	3	1	2	5	6	7
plaintext	A	T	T	A	C	K	P
	O	S	T	P	O	N	E
	D	U	N	T	I	L	T
	w	O	A	M	X	Y	Z

Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

COLUMN TRANSPOSITION CIPHER

- **Example**:

  key= 632415

  plaintext= WE ARE DISCOVERED FLEE AT ONCE

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

CIPHERTEXT= EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

Double Transposition Cipher

- To encrypt with a double transposition cipher, we first write the plaintext into an array of a given size and then permute the rows and columns according to specified permutations.
- **For example**, suppose we write the plaintext **attack at dawn** into a 3x4 array:

A	T	T	A
C	K	A	T
D	A	W	N

Now if we transpose(permute) the rows according to(1,2,3)→(3,2,1) and then transpose the columns according to (1,2,3,4)→(4,2,1,3), we obtain

Double Transposition Cipher

A	T	T	A
C	K	A	T
D	A	W	N

D	A	W	N
C	K	A	T
A	T	T	A

N	A	D	W
T	K	C	A
A	T	A	T

- The ciphertext is then read from the final array: NADWTKCAATAT.
- For the double transposition, the key consists of the size of the matrix and the row and column permutations.
- Anyone who knows the key can simply put the ciphertext into the appropriate sized matrix and undo the permutations to recover the plaintext

Double Transposition Cipher

- For example, to decrypt the ciphertext is first put into a 3 x 4 array.
- Then the columns are numbered as (4,2,1,3) and rearranged to (1,2,3,4), and the rows are numbered (3,2,1) and rearranged into (1,2,3).

N	A	D	W
T	K	C	A
A	T	A	T

D	A	W	N
C	K	A	T
A	T	T	A

A	T	T	A
C	K	A	T
D	A	W	N

And we see that we have recovered the plaintext, namely, attack at down.

Next Lecture

- Playfair Algorithm
- Stream Vs block ciphers
- Key Management