Transposition Techniques

Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

Outline

- **Transposition Techniques**
  - ✓ **Rail Fence**
  - ✓ **Simple Columnar**
  - ✓ **Multi stage Columnar**

Transposition Techniques

Transposition Techniques

- We will use a **different notion** in **Classical Cryptography**: **Permuting The Plaintext.**
- A **very different kind of mapping** is achieved by **performing some sort of permutation** on the **plaintext letters**. This technique is referred to as a **TRANSPOSITION CIPHER.**

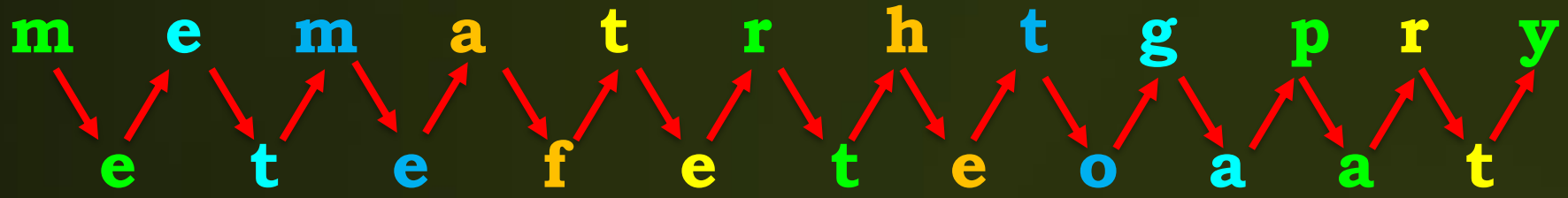
Rail Fence Transposition Technique

Rail Fence Transposition Technique

- The **simplest Transposition cipher** is the **Rail Fence Technique**,
  - ✓ The **Plaintext** is written down as a **sequence of diagonals** and then **read off as a sequence of rows.**

Rail Fence Transposition Technique

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



- The **encrypted message** is

MEMATRHTGPRYETEFETEOAAT

Limitations with Rail Fence Transposition Technique

- This **Rail Fence Transposition Technique** is very easy to **analyze by cryptanalyst**

Simple Columnar Transposition Cipher

Simple Columnar Transposition Cipher

- A **more complex scheme** is to write the **message in a rectangle, row by row**, and read the message off, **column by column**, but **permute the order of the columns.**
- The **order of the columns** then becomes the **key to the algorithm..**

Simple Columnar Transposition Cipher

- The **plaintext** is written **horizontally** onto a **piece of paper** of fixed width and the **ciphertext is read off vertically**
- **Decryption** is a matter of **writing the ciphertext vertically** onto a piece of paper of identical width and then **reading the plaintext off horizontally.**

For Example

- **Plaintext :** attack postponed until two a mxyz

Key	4	3	1	2	5	6	7
Plain Text	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

Analysis

- A **pure columnar transposition cipher** is easily **recognized**
  - ✓ it has the **same letter frequencies** as the **original plaintext.**
- **Cryptanalysis** is **fairly straightforward** and involves **laying out the ciphertext** in a matrix and **playing around with column positions**.
- **Digram and trigram frequency** tables can be useful.

Multi stage of Columnar Transposition Cipher

Multi stage of Columnar Transposition Cipher

- The **Transposition Cipher** can be made **significantly more secure** by performing **more than one stage of transposition.**
- The result is a **more complex permutation** that is not **easily reconstructed.**

First Stage Transposition

- **Plaintext :** attack postponed until two a mxyz

Key	4	3	1	2	5	6	7
Plain Text	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

Multi stage of Columnar Transposition Cipher

- if the foregoing **message is reencrypted** using the same algorithm,

  - **Ciphertext:** **TTNAAPTMTSUOAODWCOIXKNLYPETZ**

Key	4	3	1	2	5	6	7
Plain Text	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Multi stage of Columnar Transposition Cipher

- To visualize the result of the **double transposition**, designate the **letters in the original plaintext message** by the **numbers** designating their position.
- Thus, with **28 letters in the Original message**, the original sequence of letters is

a t t a c k p o s t p o n e

01 02 03 04 05 06 07 08 09 10 11 12 13 14

d u n t I l t w o a m x y z

15 16 17 18 19 20 21 22 23 24 25 26 27 28

Multi stage of Columnar Transposition Cipher

- After the **first transposition, we have**

Key	4	3	1	2	5	6	7
Plain Text	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

Key	4	3	1	2	5	6	7
First Transposition	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	27	28

03 10 17 24 04 11 18 25 02 09 16 23 01 08

15 22 05 12 19 26 06 13 20 27 07 14 21 28

Multi stage of Columnar Transposition Cipher

- After the **Second transposition, we have**

Key	4	3	1	2	5	6	7
Cipher Text	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z
Key	4	3	1	2	5	6	7
Second Transposition	3	10	17	24	4	11	18
	25	2	9	16	23	1	8
	15	22	5	12	19	26	6
	13	20	27	07	14	21	28

17 09 05 27 24 16 12 07 10 02 22 20 03 25

15 13 04 23 19 14 11 01 26 21 18 08 06 28

Analysis

- This is a **much less structured permutation** and is much **more difficult to cryptanalyze**

Outline

- **Transposition Techniques**
  - ✓ **Rail Fence**
  - ✓ **Simple Columnar**
  - ✓ **Multi stage Columnar**

Thank U