



SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution



Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

TOPIC –Transposition Techniques



Keywords

- Cryptography
- Encryption
- Decryption
- Cipher



- In cryptography, a *TRANSPOSITION CIPHER* is a method of encryption by which the positions held by units of plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.



- The order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.



Mosc Common Game Anagram



TSPSH ALSIS EASAM GIMEE

THIS IS A SAMPLE MESSAGE



- Rail Fence cipher
- Route cipher
- Columnar transposition
- Double transposition
- Myszkowski transposition



Rail Fence cipher

W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . 9 . O . E . R . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . . .



Route cipher

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

EJXCTEDECDAEWRIORFEONALEVSE



Columnar transposition



- ZEBRAS
- "6 3 2 4 1 5"

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					

- EVLNA CDTES EAROF ODEEC WIREE



Double transposition

- STRIPE
- "564231"

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

- CAEEN SOIAE DRLEF WEDRE EVTOC



l'fyszkowski transposition

- TOPiATO
 - S264
- | | | | | | | |
|--|---|---|---|----|---|---|
| | 4 | 3 | 2 | 1 | 4 | 3 |
| | N | E | A | R | E | D |
| | I | S | C | O | V | E |
| | R | E | D | fi | L | E |
| | E | A | T | O | N | C |
| | E | | | | | |

- ROFOA CDTED SEEEA CWEIV RLENE



Break Columnar Transposition Cipher



- Cryptanalyst must be aware that he is dealing with cipher
- Frequency of E,T,A,O,I,N, etc
- No of Columns
- Suspect
- Assumption



One-Time Pads

- Random Bid String
- Converting plain text to bit String
 - Converting plant text into its ASCII Representation
- EXCLUSIVE OR of two string

Disadvantage

- Key cannot be memorized – written
- The amount of data is limited to key available
- Sensitivity

Can be advantage in computers

Using storage devices along with huge data for key transporting.



THANK U.....