

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







2/14

- Cryptography
- Encryption
- Decryption
- •Cipher





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





 The order of the units is changed. Mathemacically 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

11/1/2023

Introduction to Cryptography /19ECT301 COMMUNICATION NETWORKS /K.SURIYA/ECE/SNSCT

5/14





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

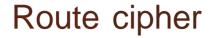


Rail Fence cipher











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

EJXCTEDECDAEWRIORFEONALEVSE

8/14





Columnar transposition

- ZEBRAS
- "632415"
 - 6 3 2 4 1 5
 - WEARED
 - ISCOVE
 - R E D F L E
 - ΕΑΤΟΝΟΕ

• EVLNA CDTES EAROF ODEEC WIREE



Double transposition



- STRIPE
- "56423 I "
 - 5 6 4 2 3 1
 - E V L N A C
 - D T E S E A R O F O D F
 - E C W I R E

Ε

• CAEEN SOIAE DRLEF WEDRE EVTOC





l'flyszkowski transposition

 тОРîАТО 4 3 2 1 4 3 • S264 NEARE \square TSCOV F D fi L E R E TOMATO EATONC • 432143 F

• 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
- Converring plain text to bit String

Converting plant text into its ASCII Representation

EXCLUSIVE OR of two string

Disadvantage

- $^{\circ}$ Key cannot be memorized written
- The amount of data is limited to key available
- ° Sensitivity

Can de advantage in computers

Using storage devices along with huge data for key transporting.







THANK U.....

11/1/2023

Introduction to Cryptography /19ECT301 COMMUNICATION NETWORKS /K.SURIYA/ECE/SNSCT 14/14