JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 11

Session Name- Block Cipher Techniques

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Feistel cipher structure**

Topic to be discussed today- Today We will discuss about **Block Cipher Techniques**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Block Cipher Techniques**

Block Cipher Techniques

Virtually, all symmetric block encryption algorithms in current use are based on a structure referred to as Feistel block cipher. For that reason, it is important to examine the design principles of the Feistel cipher. We begin with a comparison of stream cipher with block cipher.

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. E.g., Vigenère cipher.

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically, a block size of 64 or 128 bits is used.

Block cipher principles

most symmetric block ciphers are based on a Feistel Cipher Structure needed since must be able to decrypt ciphertext to recover messages efficiently. block ciphers look like an extremely large substitution would need table of 264 entries for a 64-bit block Instead create from smaller building block using idea of a product cipher in 1949 Claude Shannon introduced idea of substitution-permutation (S-P) networks called modern substitution-transposition product cipher these form the basis of modern block ciphers S-P networks are based on the two primitive cryptographic operations we have seen before:

- substitution (S-box)
- permutation (P-box)

provide confusion and diffusion of message

- diffusion – dissipates statistical structure of plaintext over bulk of ciphertext
- confusion – makes relationship between ciphertext and key as complex as possible

Reference-

1. **Book:** William Stallings, "Cryptography & Network Security", Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. What is block cipher?

Q2. What is stream cipher?

Q3. What block ciphers are based on the two primitive cryptographic operations?

Next, we will discuss about Data Encryption Standard.

- Academic Day ends with-
  National song 'Vande Mataram'