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.: 18

Session Name- Stream Ciphers and the Vernam cipher

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 **– Linear Cryptanalysis of Block Ciphers**

Topic to be discussed today- Today We will discuss about **Stream Ciphers and the Vernam cipher**

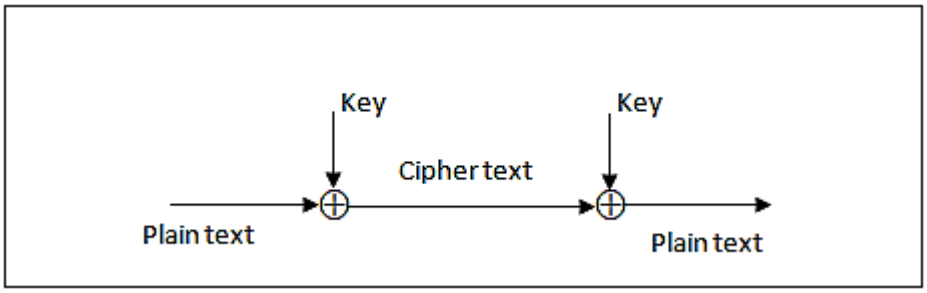
Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

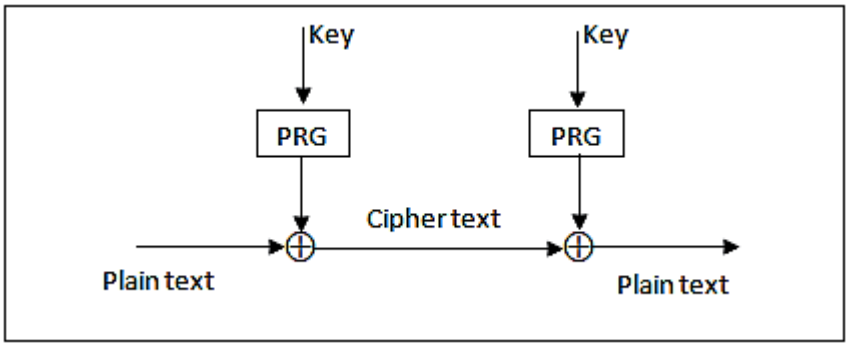
Introduction & Brief Discussion about the Topic**– Stream Ciphers**

Stream Ciphers and Vernam Cipher

- Process the message bit by bit (as a stream)
- The most famous of these is the **Vernam cipher**(also known as the **one-time pad**)
- Invented by Vernam, working for AT&T, in 1917
- Simply add bits of message to random key bits
- Need as many key bits as message, difficult in practice (i.e. distribute on a magnetic-tape or CDROM)
- Is unconditionally secure provided key is truly random



- Suggest generating key stream from a smaller(base)key



- use some pseudo-random function to do this

Reference-

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

QUESTIONS: -

Q1. Give an overview about Stream Ciphers.

Next, we will discuss more about Stream Ciphers.

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