"बेटी बचाओ, बेटी पढ़ाओ"

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.: 17

Session Name- Linear Cryptanalysis of Block Ciphers

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 **– Differential Cryptanalysis of Block Ciphers**

Topic to be discussed today- Today We will discuss about **Linear Cryptanalysis of Block Ciphers**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Linear Cryptanalysis**

Linear Cryptanalysis of Block Ciphers

Linear Cryptanalysis is another recently developed method for analyzing block ciphers like differential cryptanalysis it is a statistical method. Again, have a break-even point in number of rounds of the cipher used for which linear cryptanalysis is faster than exhaustive key-space search, if this number is greater than that specified for the cipher, then it is regarded as broken in Linear Cryptanalysis want to find a linear approximation which holds with Prob

p! =^ (1)/_ (2)

P [i1, i2,...,ia](+)C[j1,j2,...,jb]=K[k1,k2,...,kc]

where ia,jb,kc are bit locations in P,C,K

That can determine one bit of key using maximum likelihood algorithm, using a large number of trial encryptions effectiveness of linear cryptanalysis is given by

|p - 1/2|

DES can be broken by encrypting 2^(47) known plaintexts

PL[7,18,24](+)PR[12,16](+)CL[15](+)CR[7,18,24,29](+)F16(CR,K16)[15] = K1[19,23](+)K3[22](+)K4[44](+)K5[22](+)K7[22](+)K8[44](+)K9[22](+)K11[22](+) K12[44](+) K13[22](+) K15[22]

this will recover some of the key bits, the rest must be searched for exhaustively

LOKI with 12 or more rounds cannot be broken using linear cryptanalysis

Reference-

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

QUESTIONS: -

Q1. Give an overview about Linear Cryptanalysis.

Next, we will discuss about Stream Ciphers and the Vernam cipher.

- Academic Day ends with-
  National song ‘Vande Mataram’