"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.: 15

Session Name- IDEA (IPES)

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 **– Data Encryption Standard Designing Principals**

Topic to be discussed today- Today We will discuss about **IDEA (IPES)**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Data Encryption Standard Designing Principals**

IDEA (IPES)

- It is developed by James Massey & Xuejia Lai at ETH originally in Zurich in 1990, then called IPES :

Name changed to IDEA in 1992.

- encrypts 64-bit blocks using a 128-bit key
- based on mixing operations from different (incompatible) algebraic groups (XOR, Addition mod 2^(16) , Multiplication mod 2^(16) +1)
- all operations are on 16-bit sub-blocks, with no permutations used, hence its very efficient in s/w
- IDEA is patented in Europe & US, however non-commercial use is freely permitted
- used in the public domain PGP secure email system (with agreement from the patent holders)
- currently no attack against IDEA is known (it appears secure against differential cryptanalysis), and its key is too long for exhaustive search

Overview of IDEA

IDEA encryption works as follows:

- the 64-bit data block is divided by 4 into: X_(1) , X_(2) , X_(3) , X_(4)
- in each of eight the sub-blocks are XORd, added, multiplied with one another and with six 16-bit sub-blocks of key material, and the second and third sub-blocks are swapped
- finally some more key material is combined with the sub-blocks

IDEA sub-keys

- the encryption keying material is obtained by splitting the 128-bits of key into eight 16-bit sub-keys, once these are used the key is rotated by 25-bits and broken up again etc
- the decryption keying material is a little more complex, since inverses of the sub-blocks need to be calculated

The keys used may be summarized as follows:

Round	Encryption Keys Decryption Keys	
1	K1.1 K1.2 K1.3 K1.4 K1.5 K1.6 K9.1-1 -K9.2 -K9.3 K9.4-1	K8.5
	K8.6	
2	K2.1 K2.2 K2.3 K2.4 K2.5 K2.6 K8.1-1 -K8.3 -K8.2 K8.4-1	K7.5
	K7.6	
3	K3.1 K3.2 K3.3 K3.4 K3.5 K3.6 K7.1-1 -K7.3 -K7.2 K7.4-1	K6.5
	K6.6	
4	K4.1 K4.2 K4.3 K4.4 K4.5 K4.6 K6.1-1 -K6.3 -K6.2 K6.4-1	K5.5
	K5.6	
5	K5.1 K5.2 K5.3 K5.4 K5.5 K5.6 K5.1-1 -K5.3 -K5.2 K5.4-1	K4.5
	K4.6	
6	K6.1 K6.2 K6.3 K6.4 K6.5 K6.6 K4.1-1 -K4.3 -K4.2 K4.4-1	K3.5
	K3.6	
7	K7.1 K7.2 K7.3 K7.4 K7.5 K7.6 K3.1-1 -K3.3 -K3.2 K3.4-1	K2.5
	K2.6	
8	K8.1 K8.2 K8.3 K8.4 K8.5 K8.6 K2.1-1 -K2.3 -K2.2 K2.4-1	K1.5
	K1.6	
Output	K9.1 K9.2 K9.3 K9.4 K1.1-1 -K1.2 -K1.3 K1.4-1	

where: K1.1^(-1) is the multiplicative inverse mod 2^(16) +1

-K1.2 is the additive inverse mod 2^(16) and the original operations are: (+) bit-by-bit XOR + additional mod 2^(16) of 16-bit integers

* Multiplication mod 2^(16) +1 (where 0 means 2^(16))

Reference-

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

QUESTIONS: -

Q1. What is IDEA? Explain briefly.

Next, we will discuss about Differential Cryptanalysis of Block Ciphers.

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