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.: 16

Session Name- Differential 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 **– IDEA (IPES)**

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

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

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

Differential Cryptanalysis of Block Ciphers

Differential Cryptanalysis is a recently (in the public research community) developed method which provides a powerful means of analyzing block ciphers. It has been used to analyze most of the currently proposed block ciphers with varying degrees of success. Usually have a break-even point in number of rounds of the cipher used for which differential 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

Overview of Differential Cryptanalysis

It is a statistical attack against Feistel ciphers and it uses structure in cipher not previously used. Here, the design of S-P networks is such that the output from function f is influenced by both input and key

R(i)=L(i-1) (+) f(K(i) (+) R(i-1))

Hence, cannot trace values back through cipher without knowing the values of the key

Biham & Shamir's key idea is to compare two separate encryptions (using the same key) and look at the XOR of the S-box inputs and outputs and this is independent of the key being used

$$Ra(i)=f(K(i)(+)Ra(i-1))$$

$$Rb(i)=f(K(i)(+)Rb(i-1))$$

Hence,

$$Y(i)= Ra(i)(+)Rb(i)$$

$$= f(K(i)(+)Ra(i-1)(+)K(i)(+)Rb(i-1))$$

$$= f(Ra(i-1)(+)Rb(i-1)) = f(X(i))$$

further various input XOR - output XOR pairs occur with different probabilities.

Hence, knowing information on these pairs gives us additional information on the cipher

XOR Profiles and Characteristics

- It starts by compiling a table of input vs output XOR values, an **XOR Profile** for each S-box

- A particular input XOR value and output XOR value pair will occur with some probability call such a specified pair, a **characteristic** can infer information about key value in one round, if find a pair of encryptions matching a characteristic, and hence knowing input and output XOR values have several variant forms of differential cryptanalysis, will discuss just the general form used for attacking many rounds (>8) of a cipher. This can describe 1-round characteristic by:

  f(x')->y', Pr(p)

  (a',b')->(b',a'(+)f(b')) with prob p

  useful characteristics:

  (i) f (0')->0', Pr(1) ie always A.(x,0)->(0,x) always

  (ii) f(x')->0', Pr(p_(0)) B.(0,x)->(x,0) with probability p_(0)

Attack multiple rounds using **n-round characteristic. A n-round characteristics** combine one round characteristic whose outputs & inputs match probability of n-round characteristic is product of the 1-round characteristic probabilities 2-Round Iterative Characteristic, some common characteristic.0000c structures are:

* a 2-round characteristic:
  A. A.(x,0)->(0,x) always
  B. B.(0,x)->(x,0) with probability p
* a 3-round characteristic:
  A. (x,0)-> (0, x) always
  B. (0, x)->(x,x) with probability p1
  C. C.(x,x)->(x,0) with probability p2

Perform attack by repeatedly encrypting plaintext pairs with known input XOR until obtain expected output XOR matching n-round characteristic being used. If all intermediate rounds also match required XOR (which is unknown) then have a right pair, if not then have a wrong pair, relative ratio is S/N for attack. Now, assume know XOR at intermediate rounds (if right pair) then deduce keys values for the rounds - right pairs suggest same key bits, wrong pairs give random values for large numbers of rounds, probability is so low that more pairs are required than exist with 64-bit inputs optimizations of this attack can be made, trading memory for search time, and number of rounds used in their latest paper, Biham and Shamir show how a 13-round iterated characteristic can be used to break the full 16-round DES.

Reference-

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

QUESTIONS: -

Q1. Give an overview about Differential Cryptanalysis.

Q2. What are XOR profiles and characteristics?

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

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