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.: 13

Session Name- Data Encryption Standard Modes of use

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**

Topic to be discussed today- Today We will discuss about **DES Modes of use**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

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

Data Encryption Standard (DES) modes of use

- DES encrypts 64-bit blocks of data, using a 56-bit key
- we need some way of specifying how to use it in practise, given that we usually have an arbitrary amount of information to encrypt
- the way we use a block cipher is called its Mode of Use and four have been defined for the DES by ANSI in the standard: ANSI X3.106-1983 Modes of Use) modes are either:

Block Modes

– Splits messages in blocks (ECB, CBC)

Electronic Codebook Book (ECB)

– Where the message is broken into independent 64-bit blocks which are encrypted C_(i) = DES_(K1) (P_(i))

Cipher Block Chaining (CBC)

Again the message is broken into 64-bit blocks, but they are linked together in the encryption operation with an IV C_(i) = DES_(K1) (P_(i)(+)C_(i-1)) C_(-1)=IV

Stream Modes

– On bit stream messages (CFB, OFB)

Cipher Feedback (CFB)

– Where the message is treated as a stream of bits, added to the output of the DES, with the result being feedback for the next stage

C_(i) = P_(i)(+) DES_(K1) (C_(i-1)) C_(-1)=IV

Output Feedback (OFB)

– Where the message is treated as a stream of bits, added to the message, but with the feedback being independent of the message

  C_(i) = P_(i)(+) O_(i) O_(i) = DES_(K1)(O_(i-1)) O_(-1)=IV

  each mode has its advantages and disadvantages

Limitations of Various Modes

ECB

– repetitions in message can be reflected in ciphertext
– if aligned with message block
– particularly with data such graphics
– or with messages that change very little, which become a code-book analysis problem
– weakness is because enciphered message blocks are independent of each other

CBC

– Use result of one encryption to modify input of next
– Hence each ciphertext block is dependent on all message blocks before it
– Thus, a change in the message affects the ciphertext block after the change as well as the original block

CFB

– when data is bit or byte oriented, want to operate on it at that level, so use a stream mode
– the block cipher is use in encryption mode at both ends, with input being a feed-back copy of the ciphertext
– can vary the number of bits feedback, trading off efficiency for ease of use
– again, errors propagate for several blocks after the error

OFB

– also, a stream mode, but intended for use where the error feedback is a problem, or where the encryptions want to be done before the message is available

- is superficially similar to CFB, but the feedback is from the output of the block cipher and is independent of the message, a variation of a Vernam cipher
- sender and receiver must remain in sync, and some recovery method is needed to ensure this occurs
- although originally specified with varying m-bit feedback in the standards, subsequent research has shown that only 64-bit OFB should ever be used (and this is the most efficient use anyway)

DES Weak Keys

with many block ciphers there are some keys that should be avoided, because of reduced cipher complexity

these keys are such that the same sub-key is generated in more than one round, and they include:

Weak Keys

- he same sub-key is generated for every round
- DES has 4 weak keys

Semi-Weak Keys

- only two sub-keys are generated on alternate rounds
- DES has 12 of these (in 6 pairs)

Demi-Semi Weak Keys

- have four sub-keys generated
- none of these cause a problem since they are a tiny fraction of all available keys
- however, they MUST be avoided by any key generation program

Reference-

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

QUESTIONS: -

Q1. What are the modes of use of the DES?

Q2. Write limitations of various modes in DES?

Q3. Explain the data encryption standard weak keys.

Next, we will discuss about Data Encryption Standard Design Principals.

- Academic Day ends with-

  National song 'Vande Mataram'