VIGNAN'S NIRULA
INSTITUTE OF TECHNOLOGY & SCIENCE FOR WOMEN
(Approved by AICTE, New Delhi & Affiliated to JNTU Kakinada)
Vignan Avenue, Peda Palakaluru, Guntur - 522009
Department of Information Technology

Innovative Teaching Practice

Course Information:

Faculty Name	**:** Mr.R. Srinivas, Mrs.V.Sasikala
Course Name	**:** Cryptography and Network Security
Class	**:** III B.Tech II Semester
Academic Year	**:** 2022-2023
Activity Name	**:** Collaborative Learning
Topic	**:** Diffie-Hellman Key Exchange

Objective of the Activity:

The objective of the Collaborative Learning activity is to engage students in a group-based exploration of the Diffie-Hellman Key Exchange protocol, a fundamental method for securely exchanging cryptographic keys over a public channel.

Pre-Class Preparation:

Students are required to:

- **Review the textbook or online resources** on key exchange protocols, focusing on:
  - The principles of the Diffie-Hellman Key Exchange and its significance in cryptography.
  - The mathematical foundation of the protocol, including modular arithmetic and prime numbers.
  - The advantages of using Diffie-Hellman over other key exchange methods.
  - Potential security vulnerabilities, such as man-in-the-middle attacks.
- **Prepare notes** on key topics like:
  - Steps involved in the Diffie-Hellman Key Exchange process.
  - Real-world applications of the protocol in secure communications.
  - Strategies for enhancing security during key exchange.
- **Formulate questions** about any unclear aspects of the Diffie-Hellman protocol, especially regarding its implementation and security considerations.

In-Class Collaborative Learning Activity:

Instructions:

1. **Group Formation (5 minutes):**
   - Students will be divided into small groups of 4-5. Each group will be assigned a set of tasks related to the Diffie-Hellman Key Exchange, where they will collaborate to explore the concepts in detail.
2. **Collaborative Exploration (15 minutes):**
   - Each group will work together on the following questions and tasks:
     1. Define the Diffie-Hellman Key Exchange and explain how it works.
     2. Identify at least two major advantages of using the Diffie-Hellman protocol for key exchange.
     3. Discuss potential vulnerabilities associated with the Diffie-Hellman Key Exchange and how they can be mitigated.

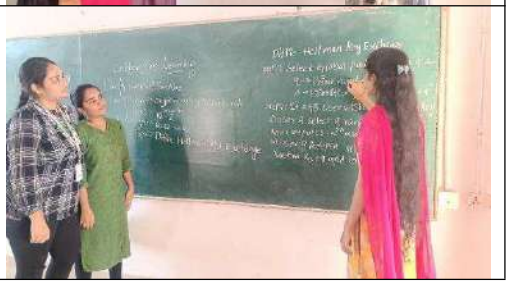
4. Propose a real-world scenario where the Diffie-Hellman protocol could be effectively utilized in securing communication**.**
5. Case Study Discussion Groups will be provided with a hypothetical scenario involving key exchange between two parties. They must propose a plan for implementing the Diffie-Hellman protocol securely.

3. **Group Presentation (15 minutes):**
   - Each group will present their findings to the class. Presentations should include:
     - An overview of the Diffie-Hellman Key Exchange and its steps.
     - Advantages and potential vulnerabilities of the protocol.
     - Proposed solutions and their potential effectiveness in securing the key exchange process.

Class Discussion (10 minutes):

After the presentations, the class will engage in a broader discussion about the Diffie-Hellman Key Exchange, with the instructor clarifying any misconceptions or providing additional examples from industry or research on key exchange protocols.

Images / Screenshot of the practice

Collaborative Learning	**Screenshot of the practice**
On the topic Diffie-Hellman Key Exchange presented by: 20NN1A1221 20NN1A1224 20NN1A1228	
On the topic Diffie-Hellman Key Exchange presented by: 20NN1A1231 20NN1A1235 20NN1A1236	

Benefits of the Practice:

1. **Encourages Peer-to-Peer Learning:** The collaborative nature of the activity allows students to explain concepts to one another, reinforcing their understanding and clarifying any doubts.
2. **Promotes Critical Thinking:** By analyzing the Diffie-Hellman protocol and its vulnerabilities, students engage in critical thinking, applying their theoretical knowledge to real-world cryptographic challenges.

Signature of Faculty Member **Head of the Department**