MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

SY B.Tech Semester-IV (AY 2022-23)

Computer Science and Engineering (Cybersecurity and Forensics)

Assign No.	List of Assignments
1.	Write a program using JAVA or Python or C++ to implement any classical cryptographic technique.
2.	Write a program using JAVA or Python or C++ to implement Feistal Cipher structure
3.	Write a program using JAVA or Python or C++ to implement S-AES symmetric key algorithm.
4.	Write a program using JAVA or Python or C++ to implement RSA asymmetric key algorithm.
5.	Write a program using JAVA or Python or C++ to implement integrity of message using MD5 or SHA
6.	Write a program using JAVA or Python or C++ to implement Diffie Hellman Key Exchange Algorithm
7.	Write a program using JAVA or Python or C++ to implement Digital signature using DSA.
8.	Demonstrate Email Security using - PGP or S/MIME for Confidentiality, Authenticity and Integrity.
9.	Demonstration of secured web applications system using SSL certificates and its deployment in Apache tomcat server
10.	Configuration and demonstration of Intrusion Detection System using Snort.
11.	Configuration and demonstration of NESSUS tool for vulnerability assessment.

MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Write a program using JAVA or Python or C++ to implement Diffie Hellman Key Exchange Algorithm

Objectives:

- To key exchange

Diffie Hellman Algorithm

1. Choose prime number **n** and **g** where g is a primitive root of n.
2. User A selects X_A as his **private key randomly**. i.e. $X_A < n$
3. User B selects X_B as his **private key randomly**. i.e. $X_B < n$
4. User A computes his **public key** i.e. $Y_A = (g^{XA}) \bmod n$
5. User B computes his **public key** i.e. $Y_B = (g^{XB}) \bmod n$
6. Exchange their public keys
7. User A computes key called **shared secret key**. i.e. $k = (Y_B{}^{XA}) \bmod n$
8. User B computes key called **shared secret key**. i.e. $k = (Y_A{}^{XB}) \bmod n$
9. Both user communicate each other using one of the **symmetric encryption technique**.

They use shared secret key as the encryption key for selected algorithm.

Agree upon two numbers:

P Prime Number 13

G Generator of P 6

Private = 5

Randomly generate a Private Key

Private = 4

(6^{5}) MOD 13

(7776) MOD 13

Public = 2

Calculate Public Key:

$(G^{Private})$ MOD P

(6^{4}) MOD 13

(1296) MOD 13

Public = 9

Exchange Public Keys

(9^{5}) MOD 13

(59049) MOD 13

Shared Secret = 3

Calculate the Shared Secret

$(Shared\ Public^{Private})$ MOD P

(2^{4}) MOD 13

(16) MOD 13

Shared Secret = 3

PRACTICAL NETWORKING .NET

INPUT/OUTPUT

Examples

1. Solve if p = 17 and q = 7 using Diffie Hellman algorithm. Assume A = 5, and B = 3