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.

Write a program using JAVA or Python or C++ to implement RSA asymmetric key algorithm.

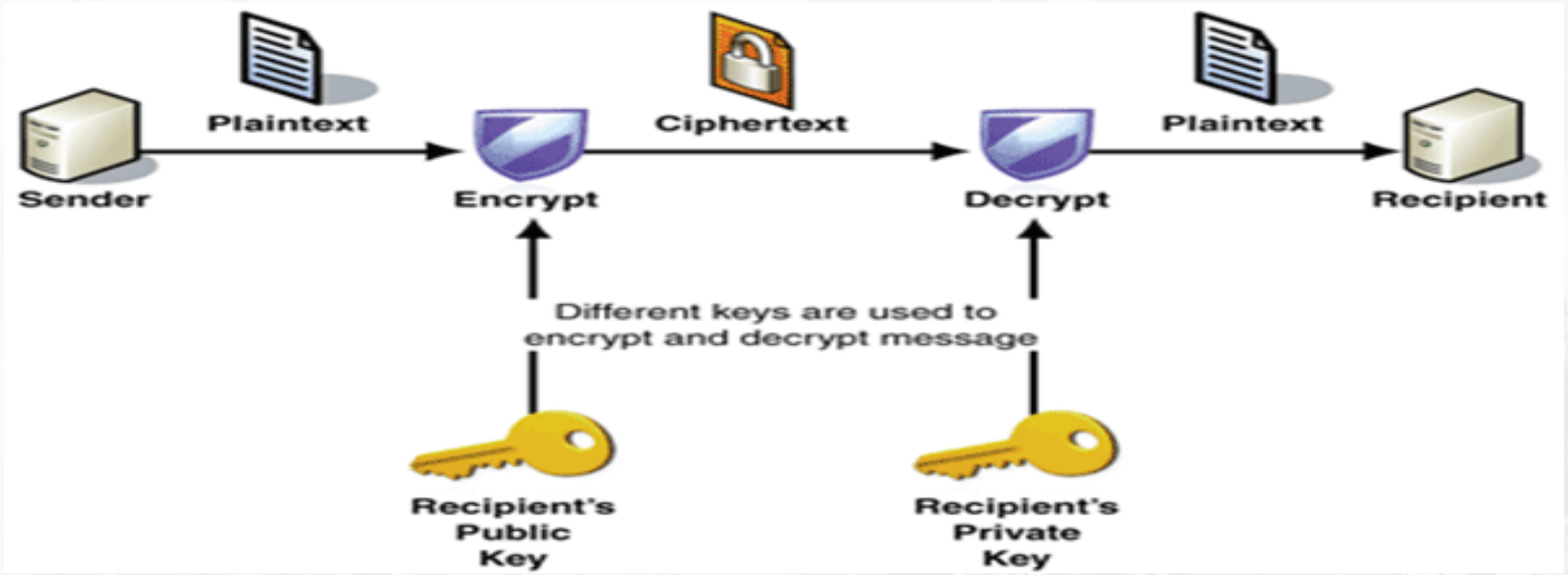
Objectives:

- Public key cryptography is used as a method of assuring the confidentiality, authenticity and non-repudiation of electronic communications and data storage.

Classical Cryptography

Basic Terminology

- Plaintext- the original message
- Ciphertext - the coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering ciphertext from plaintext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (codebreaking) - the study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - the field of both cryptography and cryptanalysis


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to
encrypt and decrypt message
Recipient's
Public
Key
Recipient's
Private
Key

RSA Encryption and Decryption

1. Selecting two large primes at random: **p, q**
2. Compute, **n = (p * q)**
3. Compute: **ø(n) = (p-1)(q-1)**
4. Select the public key (i.e. the encryption key) **e** such that it is not a factor of (p-1) and (q-1). It means **1< e < ø(n), GCD[e, ø(n)] = 1**
5. Select the private key (i.e. the decryption key **d**) : **(d * e) [mod (p-1)(q-1)] = 1**
6. Publish their public encryption key: **PU = {e, n}**
7. Keep secret private decryption key: **PR = {d, n}**

9. To encrypt a message M the sender:

   Computes Ciphertext : $\mathbf{C = M^e \bmod n}$, where $0 \leq M < n$

10. To decrypt the ciphertext C the owner:

    Computes: $\mathbf{M = C^d \bmod n}$

Note that: The message M must be smaller than the modulus n (block if needed)

Input/Output: For Encryption

1. Enter the prime no.: p, q (Check the given no is prime or not?)

2. Calculate : n, ø(*n*), e and d

3. Enter plaintext (message): M

4. For encryption, calculate: ciphertext (C)

For Decryption:

1. Enter the prime no.: p, q (Check the given no is prime or not?)

2. Calculate : n, ø(*n*), e and d

3. Enter ciphertext (message): C

4. For decryption, calculate: plaintext (M)

OUTPUT:

Enter the plain text: 10

Enter p: 7

Enter q: 17

Value of e is 5

Value of d: 77

Cipher Text:40

Plain Text:10