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.

Demonstrate Email Security using - PGP or S/MIME for Confidentiality, Authenticity and Integrity.

Objectives:

- To provide Confidentiality, Authentication and Integrity.

- confidentiality
  - protection from disclosure
- authentication
  - of sender of message
- message integrity
  - protection from modification
- non-repudiation of origin
  - protection from denial by sender

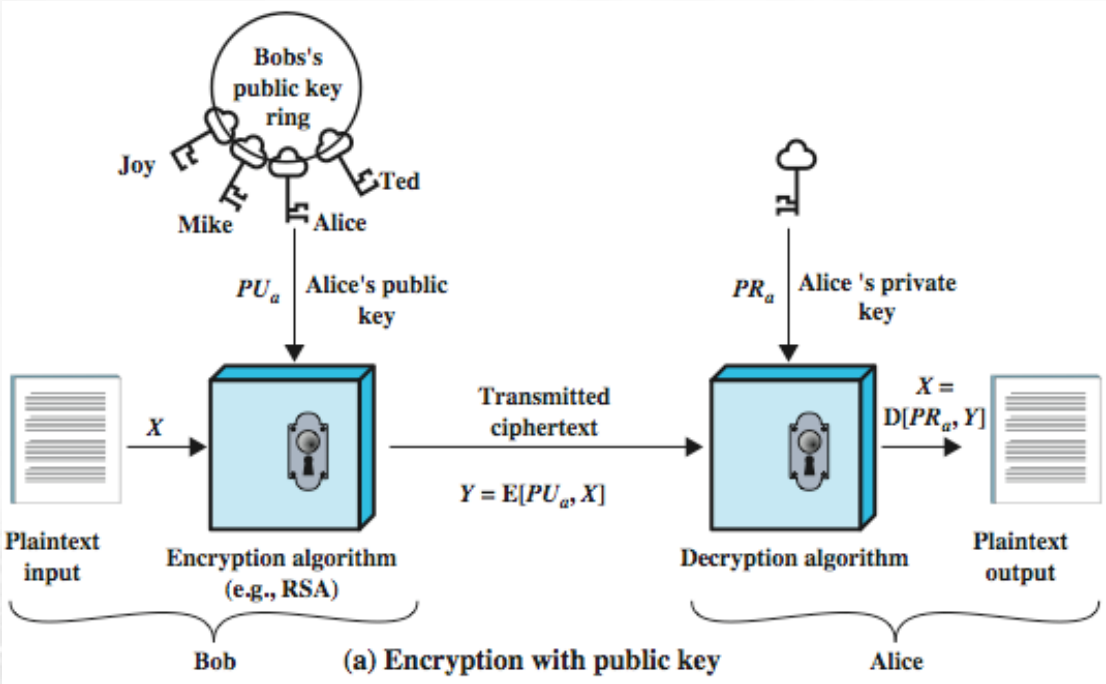
Pretty Good Privacy (PGP)

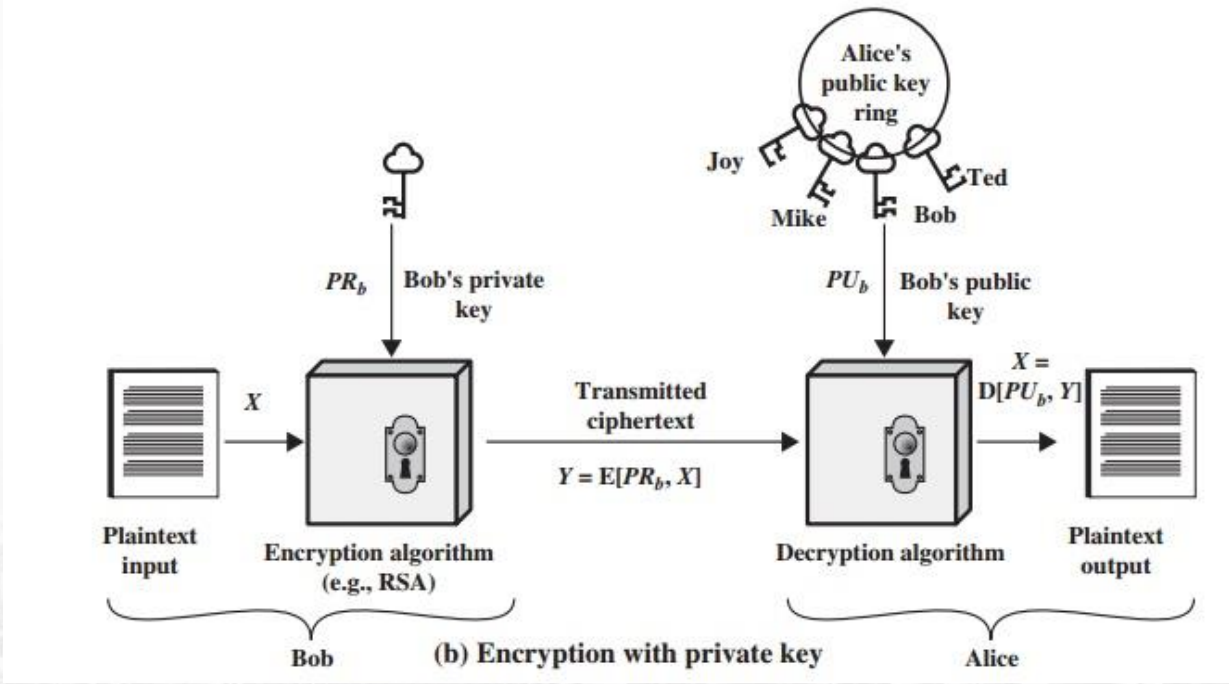
- Open source, freely available software package for secure e-mail
- de facto standard for secure email
- developed by Phil Zimmermann
- selected best available crypto algs to use
- Runs on a variety of platforms like Unix, PC, Macintosh and other systems
- originally free (now also have commercial versions available)

- PGP is a type of Public Key cryptography.
- When you begin using PGP, it generates two keys that belong uniquely to you. One PGP key is Private and stays in your computer, while the other key is Public. You give this second key to your correspondents
- It is a computer program that encrypts (scrambles) and decrypts (unscrambles) data.
- For example, PGP can encrypt the word “MITWPU” so that is reads, “457mrt%$354.”
- It can also decrypt this back into “MITWPU” if you have PGP.

Who Uses PGP Encryption?

- Individuals who are valuing privacy are the ones using PGP.
- Taxpayers storing IRS records, politicians running election campaigns and journalists protecting their sources are just a few examples of individuals using PGP to keep their computer files and their E-mail confidential.
- Businesses also use PGP to protect their customers, their employees and themselves.


Bobs's public key ring
Joy
Ted
Mike
Alice
PU_a
Alice's public key
PR_a
Alice 's private key
X
Transmitted ciphertext
$Y = E[PU_a, X]$
$X = D[PR_a, Y]$
Plaintext input
Encryption algorithm (e.g., RSA)
Decryption algorithm
Plaintext output
Bob
(a) Encryption with public key
Alice


Alice's public key ring
Joy
Ted
Mike
Bob
PR_b
Bob's private key
PU_b
Bob's public key
X
Transmitted ciphertext
$Y = E[PR_b, X]$
$X = D[PU_b, Y]$
Plaintext input
Encryption algorithm (e.g., RSA)
Decryption algorithm
Plaintext output
Bob
(b) Encryption with private key
Alice

Steps

- Enter the following at the command line: **pgp –kg**
- For RSA enabled versions, choose the key type:

  1.DSS/DH

  2.RSA
- Select the key size you want to generate. 1024
- Enter your user ID.: using your real name makes it easier for others to identify you as the owner of your public key. Umesh.raut@mitwpu.edu.in
- Enter the validity of key e.g. 0
- Enter a passphrase for your private key

  The software asks you to enter some random text to help it accumulate some random bits to create the keys. (enter/press some random key)

• The generated key pair is placed on your public and secret key rings.

Eg. Use the **–kx** command option to copy your new public key from your public key ring and place it in a separate public key file suitable for distribution to your friends.

The public key file can be sent to your friends for inclusion in their public key rings.

e.g. C:\Program Files (x86)\Network Associates\PGPcmdln> **pgp -kxa abc@gmail.com akey.txt**

Protecting your keys

• By default, the private and public key rings (pubring.pkr and secring.skr) are stored along with the other program files in the directory. If you want to secure the keys, keep separate or keep in different location.

Distributing your public key

• After you create your keys, you need to make them available to others so that they can send you encrypted information and verify your digital signature. Send the a key to others through mail/pendrive etc

Option Description

• -a When used with other options such as encryption or signing, converts a file to ASCII-armored format (creates a.asc file)

-e Encrypt using public key encryption

-kg Generate a key

-ka Add keys to the key ring

-kx Extract keys from the key ring and send to key server