============Start lecture 12 notes==========================

Q. Define the following terms: Cryptography, Cryptanalysis.

<u>What is Cryptography?</u>

“Cryptography is the science of using mathematics to encrypt and decrypt data.”

▪ Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

▪ Cryptography can be strong or weak.

▪ Cryptographic strength is measured in the time and resources it would require recovering the plaintext.

▪ The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool.

What is Cryptanalysis?

▪ Cryptanalysis is the science of analyzing and breaking secure communication.

▪ Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.

▪ How difficult? ▪ Given all of today's computing power and available time — even a billion computers doing a billion checks a second — it is not possible to decipher the result of strong cryptography before the end of the universe.

Q. What is conventional cryptography?

▪ In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.

▪ The Advanced Encryption Standard (AES) is an example of a modern conventional cryptosystem.

Q. Distinguish between symmetric and asymmetric cryptography

▪ In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.

▪ Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.

Q. Give two advantages and two disadvantages of symmetric cryptography

▪ Conventional encryption has benefits.

▪ It is very fast.

▪ It is especially useful for encrypting data that is not going anywhere.

▪ Expensive - due to the difficulty of secure key distribution.

▪ Sender and recipient must agree upon a key and keep it secret between themselves.

▪ If they are in different physical locations, they must trust a courier or some other secure communication medium to prevent the disclosure of the secret key during transmission.

▪ Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key.

Q. Give a brief account of Asymmetric Cryptography in terms of public and private keys.

▪ Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.

▪ You publish your public key to the world while keeping your private key secret. ▪ Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.

▪ Only the person who has the corresponding private key can decrypt the information.

▪ It is computationally infeasible to deduce the private key from the public key.

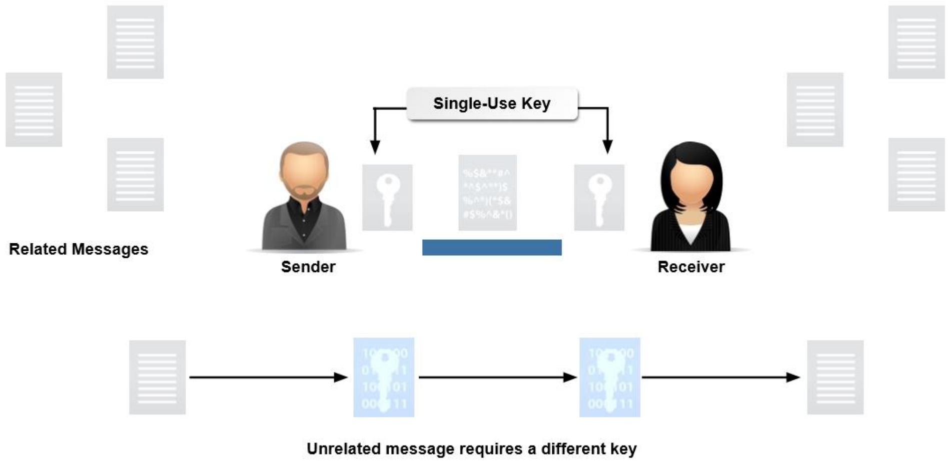
▪ The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely.

▪ The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

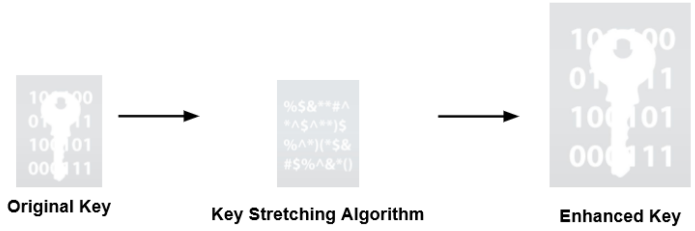
▪ Some examples of public-key cryptosystems are: ▪ Elgamal (named for its inventor, Taher Elgamal) ▪ RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) ▪ Diffie-Hellman (named for its inventors) ▪ DSA, the Digital Signature Algorithm (invented by David Kravitz).

▪ Public key encryption was the technological revolution that provides strong cryptography to the adult masses.

Q. What do you understand by the term “session key”?



Q. What do you understand by the term “key stretching”?



Key stretching makes it harder to crack passwords and passphrases.

Q. What do you understand by the term “ciphertext”?

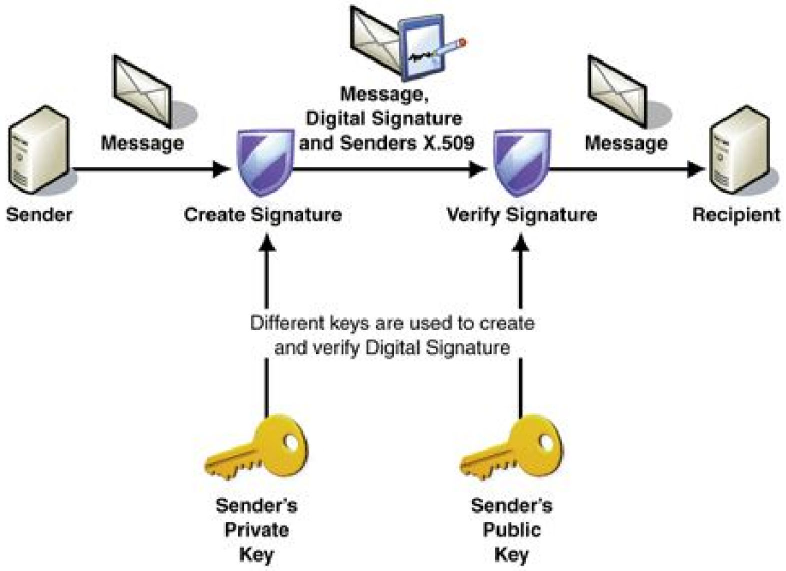
The method of disguising plaintext in such a way as to hide its substance is called encryption.

▪ Encrypting plaintext results in unreadable gibberish called ciphertext

Q. Give account of how cryptographic strength can be measured.

▪ Cryptography can be strong or weak. ▪ Cryptographic strength is measured in the time and resources it would require to recover the plaintext. ▪ The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool. ▪ How difficult? ▪ Given all of today's computing power and available time — even a billion computers doing a billion checks a second — it is not possible to decipher the result of strong cryptography before the end of the universe.

Q.With the aid of a block diagram briefly describe the principle of operation of a Digital Signature.



Q.What is a hash function and how is it used in digital signatures.

▪ Digital Signatures have some problems. ▪ They can be slow and produce an enormous volume of data — at least double the size of the original information. ▪ An improvement on this is the addition of a one-way hash function in the process. ▪ A one-way hash function takes variable-length input — in this case, a message of any length, even thousands or millions of bits — and produces a fixed-length output, known as the message digest; say, 160-bits. ▪ The hash function ensures that, if the information is changed, an entirely different output value is produced.

Q.List the three components of a Digital Certificate.

A digital certificate consists of three things: ▪ A public key. ▪ Certificate information. ("Identity" information about the user, such as name, user ID, and so on.) ▪ One or more digital signatures.

Q.How are digital Certificates distributed?

▪ Certificates are used when it's necessary to exchange public keys with someone else. ▪ For small groups of people who wish to communicate securely, it is easy to manually exchange USB Keys or emails containing each owner's public key. ▪ This is manual public key distribution, and it is practical only to a certain point. ▪ Beyond that point, it is necessary to put systems into place that can provide the necessary security, storage, and exchange mechanisms so coworkers, business partners, or strangers could communicate if need be.

Q.Explain the terms PKI and CA in the context of Digital Certificate management

Public Key Infrastructure ▪ A PKI contains the certificate storage facilities of a certificate server, but also provides certificate management facilities (the ability to issue, revoke, store, retrieve, and trust certificates). ▪ The main feature of a PKI is the introduction of what is known as a Certification Authority, or CA ▪ which is a human entity — a person, group, department, company, or other association — that an organization has authorized to issue certificates to its computer users. (A CA's role is similar to a country's government Passport Office.)

▪ A CA creates certificates and digitally signs them using the CA's private key. ▪ Because of its role in creating certificates, the CA is the central component of a PKI. ▪ Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and so, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Q.What is Certificate Revocation and how is it implemented?

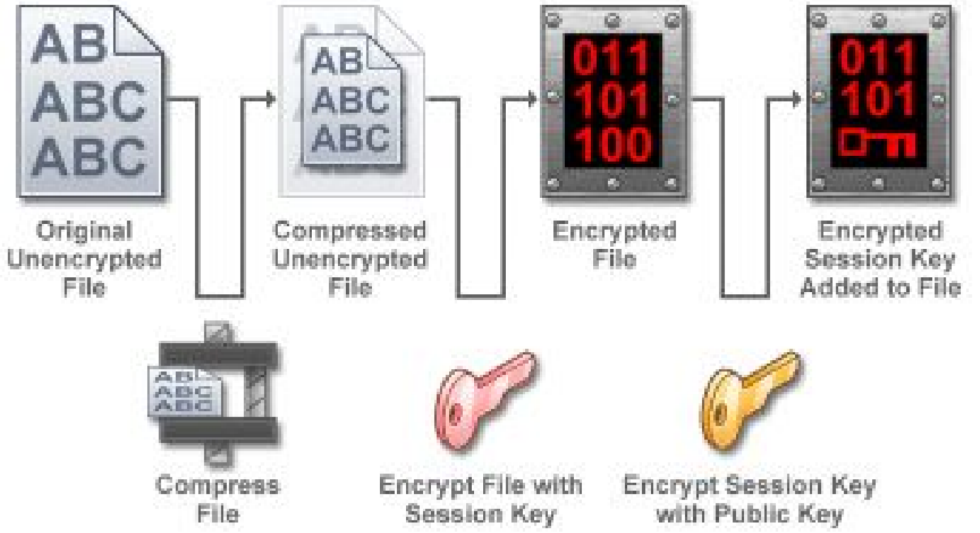
▪ Certificates are only useful while they are valid. ▪ It is unsafe to simply assume that a certificate is valid forever. ▪ In most organizations and in all PKIs, certificates have a restricted lifetime. This constrains the period in which a system is vulnerable should a certificate compromise occur. ▪ Certificates are created with a scheduled validity period: a start date/time and an expiration date/ time.

Q.Give a detailed account of how PGP works in terms of Encryption, Decryption, keys, Signing and Certificates.

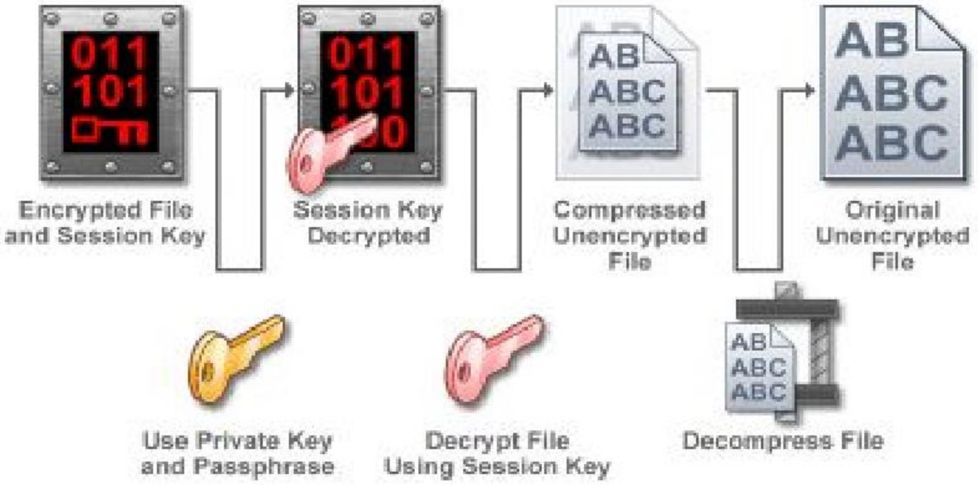
What is Pretty Good Privacy (PGP)? ▪ “It’s personal. It’s private. And it’s no one’s business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don’t want your private electronic mail (email) or confidential documents read by anyone else. There’s nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.” ▪ Phil Zimmermann

How PGP Works – Encryption ▪ PGP combines some of the best features of both conventional and public key cryptography. ▪ PGP is a hybrid cryptosystem. ▪ When a user encrypts plaintext with PGP, PGP first compresses the plaintext. ▪ Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. ▪ Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. ▪ Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis.

▪ PGP then creates a session key, which is a one-time-only secret key. ▪ This key is a random number generated from the random movements of your mouse and the keystrokes you type. ▪ This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. ▪ Once the data is encrypted, the session key is then encrypted to the recipient's public key. ▪ This public key-encrypted session key is transmitted along with the ciphertext to the recipient


AB ABC ABC
Original Unencrypted File
AB ABC ABC
Compressed Unencrypted File
011 101 100
Encrypted File
011 101
Encrypted Session Key Added to File
Compress File
Encrypt File with Session Key
Encrypt Session Key with Public Key

How PGP Works - Decryption ▪ Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.


011 101
Encrypted File and Session Key
011 101
Session Key Decrypted
AB ABC ABC
Compressed Unencrypted File
AB ABC ABC
Original Unencrypted File
Use Private Key and Passphrase
Decrypt File Using Session Key
Decompress File

How PGP Works - Keys ▪ Keys are stored in encrypted form. ▪ PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called keyrings. ▪ As you use PGP, you will typically add the public keys of your recipients to your public keyring. ▪ Combines the convenience of the key distribution of public key encryption with the speed of conventional encryption.

How PGP Signing Works ▪ PGP uses a cryptographically strong hash function on the plaintext the user is signing. ▪ This generates a fixed-length data item known as a message digest. ▪ Then PGP uses the digest and the private key to create the "signature" ▪ PGP transmits the signature and the plaintext together. ▪ Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature.

Q.Describe the web of trust process in PGP.

▪ PGP uses digital signatures as its form of introduction. ▪ When any user signs another's key, he or she becomes an introducer of that key. As this process goes on, it establishes a web of trust.

Encryption and Decryption

▪ Data that can be read and understood without any special measures is called plaintext or cleartext.

▪ The method of disguising plaintext in such a way as to hide its substance is called encryption.

▪ Encrypting plaintext results in unreadable gibberish called ciphertext.

▪ You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. ▪ The process of reverting ciphertext to its original plaintext is called decryption.

How does Cryptography work?

▪ A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.

▪ A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext.

▪ The same plaintext encrypts to different ciphertext with different keys.

▪ The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

▪ A cryptographic algorithm, plus all possible keys and all the protocols that make it work make up a cryptosystem.

▪ Data Encryptions Standard (DES) ▪ 3DES ▪ AES ▪ Blowfish ▪ Twofish ▪ RC 4, 5, 6

===========End lecture 12 notes=======================