1. Explain the concept of asymmetric cryptography. How asymmetric encryption works? Also explain its types.

Ans:

2. Write short notes on any five topics:

1. Cryptography

Ans: Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

- **Secret Key Cryptography (SKC):** Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption.

- **Public Key Cryptography (PKC):** Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver’s public key. The receiver decrypts the message using his/her private key. For nonrepudiation, the sender encrypts plain text using a private key, while the receiver uses the sender’s public key to decrypt it. Thus, the receiver knows who sent it.

- **Hash Functions:** These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

2. Pretty Good Privacy

Ans: Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991.

PGP and similar software follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system, which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

3. Application security

Ans: Application security is the use of software, hardware, and procedural methods to protect applications from external threats.

Once an afterthought in software design, security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Actions taken to ensure application security are sometimes called countermeasures. The most basic software countermeasure is an application firewall that limits the execution of files or the handling of data by specific installed programs. The most common hardware countermeasure is a router that can prevent the IP address of an individual computer from being directly visible on the Internet. Other countermeasures include conventional firewalls, encryption/decryption programs, anti-virus programs, spyware detection/removal programs and biometric authentication systems.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as threat modeling. In this context, a threat is any potential or actual adverse event that can compromise the assets of an enterprise, including both malicious events, such as a denial-of-service (DoS) attack, and unplanned events, such as the failure of a storage device.

4. WEP encryption

Ans: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network’s physical security measures by...