**15 a) Discuss the cryptographic tools used for providing the security.(NOV/DEC 2011)**

The ability to conceal the contents of sensitive messages and to verify the contents of messages and the identities of their senders have the potential to be useful in all areas of business. To be actually useful, these cryptographic capabilities must be embodied in tools that allow IT and information security practitioners to apply the elements of cryptography in the everyday.

**Public-key Infrastructure (PKI)** is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely. PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

**Digital certificates** are public-key container files that allow computer programs to validate the key and identify to whom it belongs. (More information about digital certificates appears in later sections of this chapter.) PKI and the digital certificate registries they contain enable the protection of information assets by making verifiable digital certificates readily available to business applications. This, in turn, allows the applications to implement several of the key characteristics of information security and to integrate these characteristics into business processes across an organization. These processes include the following:

**Authentication**: Individuals, organizations, and Web servers can validate the identity of each of the parties in an Internet transaction.

**Integrity**: Content signed by the certificate is known to not have been altered while in transit from host to host or server to client.

**Privacy**: Information is protected from being intercepted during transmission.

**Authorization**: The validated identity of users and programs can enable authorization rules that remain in place for the duration of a transaction; this reduces some of the overhead and allows for more control of access privileges for specific transactions.

**Non repudiation**: Customers or partners can be held accountable for transactions, such as online purchases, which they cannot later dispute. A typical PKI solution protects the transmission and reception of secure information by integrating the following components: A **certificate authority (CA)**, which issues, manages, authenticates, signs, and revokes users’ digital certificates, which typically contain the user name, public key, and other identifying information.

A **registration authority (RA)**, which operates under the trusted collaboration of the certificate authority and can handle day-to-day certification functions, such as verifying registration information, generating end-user keys, revoking certificates, and validating user certificates. Certificate directories, which are central locations for certificate storage that provide a single access point for administration and distribution.

Management protocols, which organize and manage the communications among CAs,RAs, and end users. This includes the functions and procedures for setting up new users, issuing keys, recovering keys, updating keys, revoking keys, and enabling the transfer of certificates and status information among the parties involved in the PKI’s area of authority. Policies and procedures, which assist an organization in the application and management of certificates, in the formalization of legal liabilities and limitations, and in actual business use.

Common implementations of PKI include systems that issue digital certificates to users and servers directory enrollment key issuing systems; tools for managing the key issuance and verification and return of certificates. These systems enable organizations to apply an enterprise-wide solution that provides users within the PKI’s area of authority the means to engage in authenticated and secure communications and transactions.

**Digital signatures**

Digital Signatures were created in response to the rising need to verify information transferred via electronic systems. Asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender’s private key to encrypt a message, the sender’s public key must be used to decrypt the message. When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted. This process is known as **non repudiation** and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature. Digital signatures are, therefore, encrypted messages that can be mathematically proven authentic.

These algorithms can be used in conjunction with the sender’s public and private keys, the receiver’s public key, and the Secure Hash Standard (described earlier in this chapter) to quickly create messages that are both encrypted and non repudiable. This process first creates a message digest using the hash algorithm, which is then input into the digital signature algorithm along with a random number to generate the digital signature. The digital signature function also depends upon the sender’s private key and other information provided by the CA. The resulting encrypted message contains the digital signature, which can be verified by the recipient using the sender’s public key.

**Digital Certificates**

A digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key. The certificate is often issued and certified by a third party, usually a certificate authority. Different client-server applications use different types of digital certificates to accomplish their assigned functions, as follows:

The CA application suite issues and uses certificates (keys) that identify and establish a trust relationship with a CA to determine what additional certificates (keys) can be authenticated. Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms. Development applications use object-signing certificates to identify signers of object-oriented code and scripts. Web servers and Web application servers use Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol (which is described shortly) in order to establish an encrypted SSL session. Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions via SSL.

Two popular certificate types are those created using Pretty Good Privacy (PGP) and thosecreated using applications that conform to International Telecommunication Union’s (ITU-TX.509 version 3. The X.509 v3 certificate.

It is an ITU-T recommendation that essentially defines a directory service that maintains a database (also known as a repository) of information about a group of users holding X.509 v3 certificates. An X.509 v3 certificate binds a distinguished name (DN**)**, which uniquely identifies a certificate entity, to a user’s public key. The certificate is signed and placed in the directory by the CA for retrieval and verification by the user’s associated public key.

**Certificate structure:**

Version

Certificate Serial Number

Algorithm ID

Algorithm ID

Parameters

Issuer Name

Validity

Not Before

Not After

Subject Name

Subject Public Key Info

Public Key Algorithm

Parameters

Subject Public Key

Issuer Unique Identifier (Optional)

Subject Unique Identifier (Optional)

Extensions (Optional)

Type

Criticality

Value

Certificate Signature Algorithm

Certificate Signature

**Hybrid cryptography systems**

The most common hybrid system is based on the Diffie-Hellman key exchange, which is a method for exchanging private keys using public key encryption. Diffie-Hellman key exchange uses asymmetric encryption to exchange **session keys**.