Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems

Cryptosystems can be of two types:

- **Asymmetric** Cryptosystems
- **Symmetric** Cryptosystems

ASYMMETRIC CRYPTOSYSTEMS

In an asymmetric cryptosystem (or public key cryptosystem), there are two different keys used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key.

The transmitter and the receiver both have two keys in an asymmetric system. However, the private key is kept private and not sent over with the message to the receiver, although the public key is.

SYMMETRIC CRYPTOSYSTEMS

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the ecryption/decryption

would know it. In a symmetric cryptosystem, the encrypted message is sent over without any public keys attached to it.

ADVANTAGES AND DISADVANTAGES OF **SYMMETRIC** CRYPTOSYSTEMS

ADVANTAGES

- A symmetric cryptosystem is faster.
- In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmiited with the data, the chances of data being decrypted are null.
- A symmetric cryptosystem uses password authentication to prove the receiver's identity.
- A system only which possesses the secret key can decrypt a message.

DISADVANTAGES

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.
- Cannot provide digital signatures that cannot be repudiated

ADVANTAGES AND DISADVANTAGES OF **ASYMMETRIC** CRYPTOSYSTEM

ADVANTAGES

- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated

DISADVANTAGES

- A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.