8 PUBLIC KEY CRYPTOSYSTEMS

The most commonly used implementations of public key cryptography (also known as public-key encryption and asymmetric encryption) are based on algorithms presented by Rivest-Shamir-Adelman (RSA) Data Security.

Public key cryptography involves a pair of keys known as a public key and a private key (a public key pair), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key.

RSA public key pairs can be any size. Typical sizes today are 1024 and 2048 bits.

Public key cryptography enables the following:

Encryption and decryption, which allow two communicating parties to disguise data that they send to each other. The sender encrypts, or scrambles, the data before sending it. The receiver decrypts, or unscrambles, the data after receiving it. While in transit, the encrypted data is not understood by an intruder.

Nonrepudiation, which prevents:

The sender of the data from claiming, at a later date, that the data was never sent

The data from being altered.

Figure 1 shows you a simplified view of how public key cryptography works.

Figure shows how you can freely distribute the public key so that only you (the owner of the private key) can read data that was encrypted with the public key.

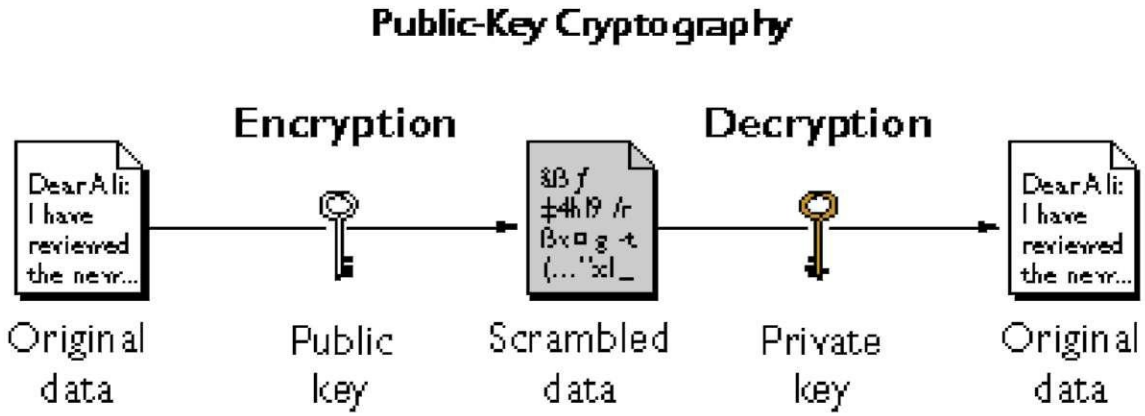

Figure – Public-key encryption

In general, to send encrypted data to someone, you must encrypt the data with that person's public key, and the person receiving the data decrypts it with the corresponding private key.

If you compare symmetric-key encryption with public-key encryption, you will find that public-key encryption requires more calculations. Therefore, public-key encryption is not always appropriate for large amounts of data. However, it is

possible to use public-key encryption to send a symmetric key, which you can then use to encrypt additional data.

The reverse of what is shown in the previous figure also works. That is, data encrypted with your private key can be decrypted only with your public key. However, this is not a desirable way to encrypt sensitive data because it means that anyone with your public key, which is by definition published, could decrypt the sensitive data. Despite this, private-key encryption is useful because it enables you to use your private key to sign data with your digital signature; anyone with your public key can be assured that only you sent the data. This is an important requirement for electronic commerce and other commercial applications of cryptography.