BASICS OF CRYPTOGRAPHY

Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer. Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited $1000 in your account, but you do want to be darn sure it was the bank teller you were dealing with. The basic manner in which digital signatures are created is illustrated in Figure 1-3. Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.

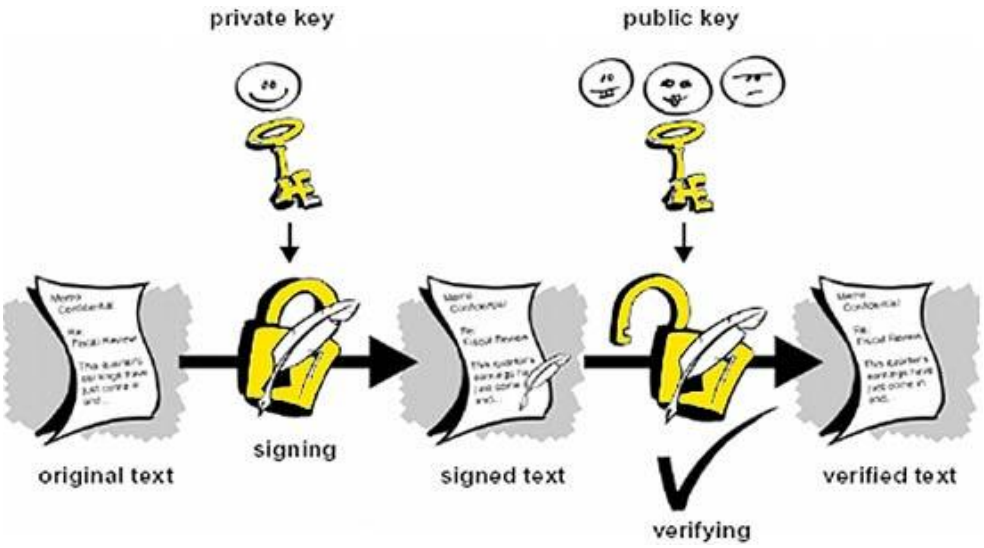

Figure 1-3 : Digital Signatures

Need for cryptography

- Secure communication
- Identification and Authentication
- Secret sharing
- E commerce
- Remote access

Techniques of Cryptography

- Matlab code for RSA Algorithm
- Matlab code for DES
- Matlab code for AES
- DSA
- Elliptic Curve Cryptosystems

Source : https://www.pantechsolutions.net/basics-of-cryptography