Understanding Public Key Infrastructure

Public Key Infrastructure

Public key infrastructure is an architecture which supports mechanisms like integrity and confidentiality. It is heavily used in e-commerce, where business transactions are frequent and should be much secured. In fact business transaction starts only after the two parties authenticate each other and are assured about each other.

In my earlier blogs, I mentioned that the infrastructure based on symmetric algorithms require sharing of "secret key" between sending and all the receiving users. This, no doubt, involves risk of an unwanted entity getting access to the key and thus breaking the security.

However, in PKI, there are two keys involved- one is meant to be publicly distributed, called as Public key and the other one –Private key, which should be held only by the correct user. The private key is so important in PKI infrastructure that it is recommended to keep it in HSM (Hardware Security module) devices.

The public key and the private key are mathematically related to each other. It is not feasible to derive the corresponding Private Key from the public key and vice versa.

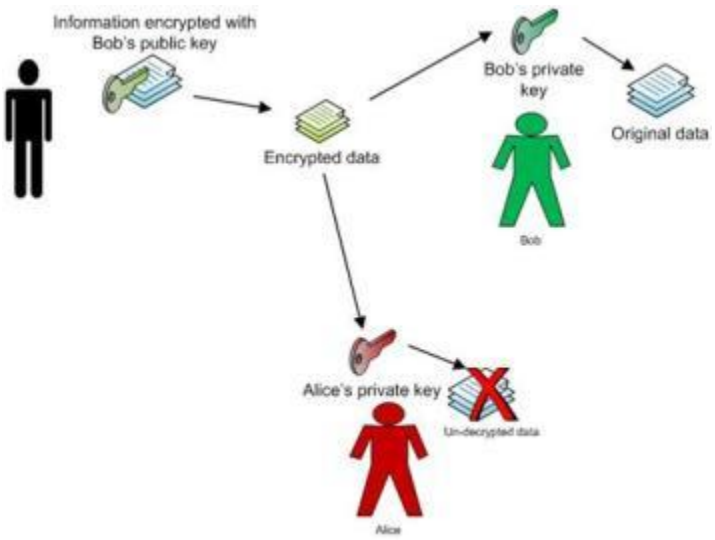
Application of PKI

PKI is mainly applied for –

- Encryption/decryption of data
- Digitally signing the information or documents
  Lets us try to understand the first application from an example -

  A scenario involving an information-provider and multiple clients or information seeking, requires that the information should be accessed only by the correct customer and there should be no chance of person Alice being able to view the data meant for Bob. (refer to diagram below)

  So, all customers should generate public – private key pair and share the public part of the pair, with the information providing firm. The firm is supposed to encrypt the information using the public key of the target customer. Once the information is encrypted, even the information provider cannot decrypt it (since he doesn't have the private keys)



For Digitally Signing the information, private key is necessary. This ensures the data is provided by the correct user (since he only possesses the private key).
This is the difference between encryption mechanism, where the public key is needed and signature process which needs private key. In case of any modifications or tampering of the data, the digital signature is no longer valid. This ensures that the data is received as it is and is not corrupt.

RSA algorithm

RSA is widely used algorithm for Public key cryptography. It is the first algorithm which can encrypt/decrypt as well as digitally sign the data. RSA stands for Rivest, Shamir and Adleman, who are the publishers of this algorithm.

The RSA public key consists of

- modulus n
- The public exponent e. Public exponent is needed for encryption.

The private key consists of

- modulus n
- The private exponent d. Private exponent is needed for decryption.

Briefly, the algorithm involves selecting and multiplying two prime numbers and through added mechanisms, deriving a set of two numbers that are the public key and the private key.

RSA is comparatively much slower than the symmetric key algorithms. Thus it is not preferred to use for encrypting or decrypting the large amount of data.

Source: http://www.go4expert.com/articles/understanding-public-key-infrastructure-t24711/