2. Cryptography

Thursday, February 11, 2021 12:58 PM

Confidentiality
Integrity

Vendors charge clients for every invocation of the service. The client must authenticate and prove themselves in order to get the service.

Web services have a flexible method of implementing confidentiality.

Fine grained confidentiality provided by SOAP enabled services because of selective encryption

SOAP enabled web service provides integrity through authentication (username, encrypted password). However, attacks on this system are possible. A new method of implementing integrity is introduced.

Playback attacks

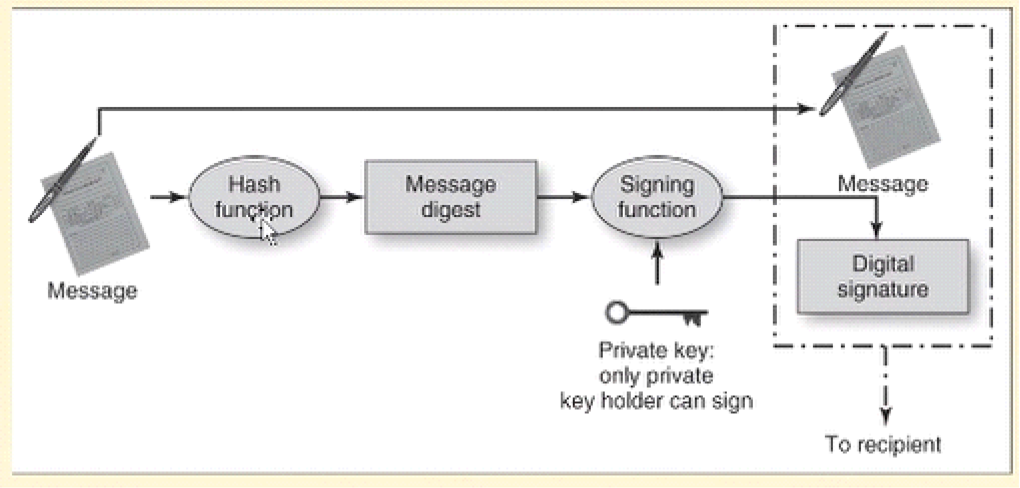
Confidentiality through encryption:

1. **Symmetric-key cryptography (private key)**
   - Sender and receiver share a binary key. Bigger the key, longer it takes to break the code. Faster compared to other encryption methods.
   - AES, DES
2. **Asymmetric-key cryptography (public key)**
   - Private and public key each for sender and receiver
   - RSA
   - Encrypt with private, decrypt with public and vice versa.

3. **Hybrid cryptography**
   - Simplified key exchange like public key cryptography
   - Speed of encryption/decryption matches the symmetric key cryptography

1. Browser and web portal have public and private keys.
2. Public keys are exchanged.
3. Browser generates a symmetric key that is encrypted using web portal's public key and shared with the portal(RSA).
4. Information is transmitted (via encryption with symmetric key(AES))
5. The symmetric key is destroyed

Digital Signature:



- Key: binary number generated using an algorithm using prime numbers
- Sharing keys is difficult --> asymmetric key cryptography