**DIGITAL SIGNATURE**

The 4 network problems which we discussed in last lectures i.e. confidentiality,integrity,non-repudation and authentication from these we cover the first problem i.e. confidentiality through asymmetric-key-cryptography in which sender send the transaction using receiver public key and receiver can only receive and decrypt by its own private key.

Digital signature is used to cover authentication factor .

In Digital Signature one more extra step of encryption and decryption is added to meet the confidentiality and authentication.



**Decrypting B’s Private Key**

**USING A’s Private Key**

**Using B’s Public Key**

**Encryption**

**Encrytion**

**Decrypting using A’s Public Key**