ICS Lab 3.

Questions

1. What are public and private keys? State their roles

Ans Private key concept in key sharing keys. In the private key the same key is shared between sender and receiver. The same key is used for encryption and decryption. It is faster than public key cryptograph

Public key : In a public key, two keys are used for encryption and decryption. is done by other key. One key is used to encrypt the plain text to convert it into cipher text and public key is used to decrypt. Only public key is known as to all users then private key is hidden from all.

2. Differentiate symmetric and asymmetric key cryptograph.

Ans

Symmetric Key	Assymmetric key
1. It only requires a single key for both encryption and decryption	1. It requires two keys a public key and a private key, one for encryption other for decryption
2. The size of cipher text is the same of original plain text.	2. The size of cipher text is the same or larger than original text.
3. The process is very fast	3. The process is slow
4. It is used when a large amount of data is required to transfer	4. It is used to transfer small amounts of data.
5. It provides confidentiality	6. It provides confidentiality authenticity, non-repudiation
6. Key length: 128 or 256 bits	6. Key length ≥ 2048 bits
7. Security is low because of single key use.	7. Security is high because of single pair key use.
8. Mathematical representation $P = D(K, E(P))$	8. Mathematical Representation $P = D(Kd, KE(Ke, (P)))$