Assignment :- 02

Ques 1:- Distinguish between public and private keys in an asymmetric-key cryptosystem.

Ans:-

	Private key	Public key
1.	Private key is used to both encrypt and decrypt the data and is shared between the sender and receiver of encrypted data.	The public key is only used to encrypt data and to decrypt the data, the private key is used and is shared.
2.	The private key mechanism is faster.	The public key mechanism is slower.
3.	The private key is kept secret.	The public key is free to use.
4.	The private keys mechanism is called symmetric being a single key between two parties.	The public key mechanism is called asymmetric being two keys for different purposes.
5.	The private key is to be shared between two parties.	The public key can be used anyone.
6.	Performance testing checks the reliability, scalability, and speed of the system.	Load testing checks the sustainability of the system.

Ques 2:- Distinguish between symmetric and asymmetric key cryptosystems

Ans:-

	Symmetric Key	Asymmetric key.
1.	It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
2.	The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
3.	The encryption process is very fast.	The encryption process is ~~very~~ slow.
4.	It is usid when large amount of data is required to transfer.	It is used to transfer small amount of data
5.	It only provides confidentiality.	It provides confidentiality, authencity and non-repudiation
6.	Ex:- 3DES, AES, DES and RC4.	Ex:- ECC, El Gamal, DSA and RSA.