****

**Faculty of Engineering Science and Technology(FEST)**

**Department of Computing and Technology**

**Indus University, Karachi**

**Teacher: Miss, Ayesha Arshad**

**Student Name: Adeel Khan**

**Section: BSSE-6-A**

**Student ID:1533-2017**

**Subject: Data Security & Encryption**

Assignment

Q. Write down understanding about Public-key cryptography

Ans: Public-key cryptography: Sometimes referred to as asymmetric cryptography, public key cryptography is a class of cryptographic protocols based on algorithms. This method of cryptography requires two separate keys, one that is private or secret, and one that is public. Public key cryptography uses a pair of keys to encrypt and decrypt data to protect it against unauthorized access or use. Network users receive a public and private key pair from certification authorities. If other users want to encrypt data, they get the intended recipient’s public key from a public directory. This key is used to encrypt the message, and to send it to the recipient. When the message arrives, the recipient decrypts it using a private key, to which no one else has access.

Two of the best-known uses of public key cryptography are:

* *Public key encryption*, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.
* [*Digital signatures*](https://en.wikipedia.org/wiki/Digital_signature), in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as a signature is mathematically bound to the message it originally was made with, and verification will fail for practically any other message, no matter how similar to the original message.
* It is widely used for TLS/SSL which makes HTTPS possible, making HTTP a secure platform for web also use SSL certificates to do so.
* A public key cryptography is essential and useful while establishing a communication over an internet using HTTPS. A website’s SSL/TSL certificates carry the public key and private key is being held on the original server – the owner.
* TSL handshakes use public key to authenticate the original identity of the server and exchange data that is used for generating the session keys. A key exchange algos uses the public-private to agree both side for session keys, which are then used as symmetric encryption once the handshake is complete. After agreement between clients and server for session keys it can be stole by the bad actors to decrypt the communications.
* Some assurance of the authenticity of a public key is needed in this system to avoid the same data which uses by another users.
* encryption algorithm is very secure that can protect attacker from deducing the plaintext from the ciphertext and the encryption public key.
* Though the public keys thye are related mathematically, it is not be feasible to calculate the private key from the public key.
* Speed of the public key is very common challenge anr cite associated with public cryptography
* It is the most secure protocol because users never need to transmit their private keys to anyone.