Sudesh Pawar
BE Comp A
F17111037

ICS A7

1) Explain ECC Algorithm?

→ An elliptic curve is a set of pts on the coordinate plane satisfying the equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$.

ii) In order to use the elliptic curves for Diffie Hellman there needs to be some mathematical operations on 2 points in set that will always produce a point also in the set.

iii) ECC can be done with atleast 2 types of arithmetic each of which gives different definitions of multiplicative arithmetic

iv) To form a cryptographic system using elliptic curves, we used to find a hard problem corresponding to factorizing the product of 2 primes or taking the discrete algorithms.

v) Consider eqⁿ of $Q = kP$ where $Q, P \in Ep(a,b)$ and $k < P$

It is relatively easy to calculate Q given k & P but it is relatively hard to determine k given Q & P. This is called logarithmic problem for elliptic curves

Q.2) List Applications of ECC Algorithm?

Ans. i) Elliptic Curve, Diffie-Hellman (ECDH) key agreement

ii) Elliptic curve based encryption e.g. Elgamo.

iii) Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature and authentication.

3) Difference between ECC & RSA

ECC	RSA
i) ECC stands for Elliptic Curve Cryptography (ECC)	i) The Rivest-Shamir Adleman Algorithm (RSA)
ii) Each participant needs a private key	ii) Each participant already has a private key.
iii) Given implementation & back doors curves recommended by NIST.	iii) Security of the system depends on possibilities of factorising n
iv) Edward Curves, Montgomery curves, Bensteins Elliptic Curve.	iv) Algorithm of fermat quadratic sieve number field ~~sieve~~ sieve.

Q.4) How is Computer security categorized?

Ans. Hackers/Crackers:

- These are people who have sophisticated computer security skills.
- They have a deep understanding of how various protocols, services, operating systems, drivers, network equipment, etc. work.

ii) Insiders / Disgruntled Personnel:

- These people are on your side but they can have malicious intent to impact your system.
- Insider threats are extremely hard to detect since you might believe them very closely.

iii) Malicious Software:

- These are software programs written with malicious intent.
- The purpose of these programs is to harm the information systems or extract useful information in an unauthorized manner.

Q.5) How to classify different attacks in Computer and Information Systems?

→ Passive Attack

The attacker indulges in eavesdropping on, or monitoring of data transmission.

ii) It attempts to learn or make use of information from the system but doesn't affect system resources.

iii) The attacker aims to obtain information that is in transmit. The term passive indicates that the attacker does not attempt to perform any modification

Active Attack:

i) Active attacks involve some modification of the data stream or the creation of a false stream.

ii) These attacks cannot be prevented easily.

- Masquerade
- Replay.
- Modification of Message.
- Denial of service.