Jessica Braganza
BE Comp 2
F17112151

PAGE NO :
DATE :

ICS Assignment 7

1) Explain ECC Algorithm

Ans. 1) An elliptic curve is a set of points on the co-ordinate plane satisfying an equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$

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

3) ECC can be done with atleast two types of arithmetic each of which gives different definitions of multiplication zp arithmetic. GF (2^n) arithmetic, which can be done with shifts and $\oplus$ s.

4) To form a cryptographic system using elliptic curves, we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete logarithms.

5) Consider the equation $Q = KP$ where $Q, P \in Ep(a,b)$ and $K < p$. It is relatively easy to calulate Q given K and P but it is relatively hard to determine K given Q and P.
This is called the discrete logarithmic problem for elliptic curves.

2) Application of ECC Algorithm

Ans. 1) Encryption

2) Digital Signatures

3) Pseudo-Random generators.

4) Integer factorization algorithms.

5) Lenstra Elliptic curve Factorization

6) Five prime fields Fp for certain prime p of sizes 192, 224, 256, 384 and 521

7) Five binary fields F_{2^m} for m equal 163, 233, 283, 409, and 571, each binary field one elliptic curve and one koblitz curve

Scanned with CamScanner

3) Difference between ECC and RSA.

Symmetric key size (bits)	RSA key size (bits)	Elliptic key size bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

	ECC	RSA
1)	Elliptic curve crypography (ECC)	The Rivest-Shamir-Aldeman system (RSA)
2)	Each participant needs a private key.	Each participant has a private key and public key.
3)	Easier implementation of back doors curves recommend by NIST.	Security of the system depends on the possibilities of factorising n
4)	Edward curves montgommery curve bernsteins elliptic curve.	Algorithm of fermat quadratic sieve number field sieve.

4) How is computer security categorized ?

Ans. 1) Critical Infrastructure Security :

It consists of the cyber physical systems that modern societies rely on.

eg. electricity grid, traffic lights.

Scanned with CamScanner

2) Application security :

uses Software and hardware methods to tackle external threats that can arise in the development stage of an application, they are much more accessible over networks, causing the adoption of security measures during development phase to an imperative phase of the project.

eg. Firewalls, antivirus programs.

3) Network security -

It guards against unauthorized intrusion of your internal networks due to malicious.

eg. extra logins, new passwords.

4) Cloud security :

A software based security tool that protects and monitors the data in your cloud resources.

Cloud providers are constantly creating and implementing new security tools to help enterprise users better secure their data.

5) Internet of Things (IOT) security :

IOT devices are frequentely sent in a vulnerable state and offer little to no security patching. This poses unique security challenges for all users.

Q) How to classify different attacks in computer and information system?

Ans: Passive Attack :

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

2) It attempts to learn or make use of information from the system but does not affect system resources.

3) The attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to data.

- Release of message content.
- Traffic Analysis

Active Attack -

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

2) These attacks cannot be prevented easily.

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

Scanned with CamScanner