Assignment 3, 4, & 6th

Q.1) Explain chinese Reminder Theorem with example.

→ The CRT is used to solve a set of different Congruent equations with one variable but different moduli which are relatively prime.

(One Variable)

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}\right\} \text{(different Congruent equation)}$$

↑ (different moduli $m_1, m_2 \dots m_n$)

CRT states that the above equations have a unique Solution of a moduli are relatively prime.

→ $X (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_n M_n M_n^{-1}) \pmod{M}$

Example $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

Given :- $a_1 = 2$ $m_1 = 3$ To find $M_1 = 35$ M_1^{-1}

$a_2 = 3$ $m_2 = 5$ $M_2 =$ M_2^{-1}

$a_3 = 2$ $m_3 = 7$ $M_3 =$ $M_3^{-1} =$

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7 = 105$ $\boxed{M = 105}$

$M_1 = \frac{M}{M_1}$, $M_2 = \frac{M}{M_2}$, $M_3 = \frac{M}{M_3}$

$M_1 = 105/3$ $M_2 = 105/5$ $M_3 = 105/7$

$\boxed{M_1 = 35}$ $\boxed{M = 21}$ $\boxed{M_3 = 15}$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

use M_1^{-1} as 1 $\frac{35}{3} \Rightarrow 2$ Remainder

$35 \times 1 = 2 \bmod 3 \Rightarrow X$.

So use $M_1^{-1} = 2$.

$35 \times 2 = 1 \bmod 3$ $\quad 35/2 = 1$ Remainder.

So $\boxed{M_1^{-1} = 2}$

$M_2 \times M_2^{-1} = 1 \bmod m_2$.

$21 \times M_2^{-1} = 1 \bmod 5$

use M_2^{-1} = as 1 $\quad 21/5 = 1$ Remainder.

$21 \times 1 = 1 \bmod 5$

$\boxed{M_2^{-1} = 1}$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

use M_3^{-1} as 1.

$15 \times 1 = 1 \bmod 7$ $\quad 15/7 = 1$ Remainder.

$\boxed{M_3^{-1} = 1}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$\boxed{X = 23}$

Prove $23 = 2 \pmod{(3)}$ $\quad 23/3 = 21 \Rightarrow 2$ Remainder

$23 = 3 \pmod{(5)}$ $\quad 23/5 = 20 \Rightarrow 3$ Remainder

$23 = 2 \pmod{(7)}$ $\quad 23/7 = 21 \Rightarrow 2$ Remainder

Q2) Explain ElGamal Algorithm with example.

The ElGamal encryption algorithm is a public-key cryptosystem that allows secure communication between two parties.

1) 1. Key Generation :-

- Bob generates a large prime number q & a cyclic group F_q.
- He selects an element g from the cyclic group & a secret number a such that $\gcd(a, q) = 1$

- Bob computes $h = g^a$ & publishes Fq, h, g & g as his public key. He keeps a as his private key.

2) Encryption :-
- Alice wants to send a message M to Bob.
- She selects a random element k from the cyclic group such that gcd(k, q) = 1
- Alice computes :
  $P = g^k$ $S = h^k * M$.
- She sends the ciphertext pair (P, M * S) to Bob.

3) Decryption :
- Bob receives the ciphertext pair.
- He calculates $S' = P^a$
- To obtain the original message M, he divides M * S by S'.

→ Example) Suppose Alice wants to send the message "encryption" to Bob using ElGamal with the following parameters :
q = A large prime number (e.g. 11)
g = An element from the cyclic group (e.g. 7)
a = Bob's secret key (e.g. 5)
h = Bob's public key (computed as $h = g^a$)

1) Encryption :-
- Alice selects a random : k (e.g. 3)
- She computes :
  $P = g^k = 7^3 = 343 \pmod{11} = 1$
  $S = h^k * M = 5^3 * M = 125 * M$
- Alice sends the ciphertext pair : (P, 125 * M).

2) Decryption :-
- Bob calculates $S' = P^a = 1^5 = 1$.
- He divides the received value 125 * M by S' to obtain the original message : M.

Q.3) Comparison between MD5 & SHA

	MD5	SHA
1)	MD5 can have 128 bits length of message digest	SHA1 can have 160 bits length of message digest
2)	MD5 is simple than SHA	SHA1 is more complex than MD5
3)	MD5 provides indigent or poor security	While it provides balanced or tolerable security.
4)	The speed of MD5 is fast in comparison of SHA1's speed.	The speed of SHA1 is slow in comparison of MD5's speed.
5)	MD5 was presented in the year 1992	While SHA1 was presented in the year 1995
6)	MD5 has 64 rounds	SHA has 20 rounds.
7)	MD5 is vulnerable against cryptanalysis	7) SHA is not vulnerable against cryptanalysis
8)	It is less secure than SHA	8) SHA High secure than MD5.

Q.5 Explain Digital signature algorithm & Digital Signature Standard.

→ Digital Signature Algorithm (DSA):

- The Digital Signature Algorithm (DSA) is a cryptographic algorithm used for generating & verifying digital signatures. Here are the key Points about DSA:

- Purpose :- DSA is primarily employed for authenticating electronic documents. It ensures that a digital data originates from a trusted source.
- Hashing & signing:
  - A hash code is generated from the original message using a secure hash algorithm
  - The sender's private key is used to create a digital signature by encrypting the hash value.
  - The resulting signature consists of two components : 's' & 'r'.
- Verification :-
  - At the receiver's end, the hash code of the received message is computed
  - The verification function takes inputs including the hash code, signature components 's' & 'r' & the sender's public key.
  - If the computed signature matches the received 'r' component, the signature is considered valid.
- Benefits :-
  - Enhanced security in data exchanges
  - Fast document delivery.
  - Non-repudiation (signer cannot deny their signature)
  - Automatic timestamping:
- Challenges :-

1) Compatibility issues (e.g. Software versions, drivers)
2) proper management of keys.
3) Corporate use cases (e.g. E-tagging for commodity import)

Digital Signature Standard (DSS):

- The DSS is a Federal Information Processing Standard (FIPS) that defines algorithms for generating digital signatures. Here's what you need to know:
- Algorithms Supported:
  1) Initially, FIPS 186 specified the DSA for digital signatures.
  2) Later revisions (FIPS 186-1 & FIPS 186-2) introduced additional algorithms:
     - Elliptic Curve Digital signature Algorithm (ECDSA)
     - RSA digital signature algorithm.
- Focus:- DSS provides the digital signature function but does not address encryption or key exchange strategies.
- Usage: DSS is commonly used for authenticating electronic documents in various applications.

Q.5) Compare PGP, MIME & S/MIME

PGP	S/MIME
1) It is designed for processing the plain text.	1) While it is designed to process email as we as many multimedia files.
2) PGP is less costly as compared to S/MIME	2) While S/MIME is comparatively expensive.
3) PGP is good for personal as well as office use.	3) While it is good for industrial use.
4) PGP is less efficient than S/MIME	4) While it is more efficient than PGP
5) It depends on user key exchange.	5) Whereas it relies on a hierarchically valid certificate for key exchange.

6) PGP is comparatively less convenient.	6) PGP due to the secure transformation of all the applications.
7) PGP contains 4096 public keys.	7) While it contains only 1024 public keys.
8) PGP is also be used in VPNs.	8) While it is not used in VPNs, it is only used in email services.
9) PGP uses Diffie hellman digital signature.	9) While it uses Elgamal digital signature

Q.6) Explain applications of cryptographic Hash Functions.

- A typical use of a cryptographic hash would be as follows:

1) Alice poses a tough math problem to Bob, & claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not Huffing. Therefore, Alice writes down her solution, appends a random nonce, computes its hash & tells Bob the hash value. This way, when Bob comes up with the solution himself a few days later, Alice can prove that she had the sol^n earlier by reveling the nonce to Bob.

2) A related application is password verification.

→ Passwords are usually not stored in clear text, for obvious reasons, but insted in digest form. To authenticate a user, the password presented by the user is hashed & compared with the stored hash. This is sometimes referred to as one-way encryption.

Q.7) Explain Secure Hash Algorithm (SHA)

-> SHA stands for Secure Hash Algorithm

- It is a family of cryptographic functions designed to keep data secure.
- These algorithms transform data using a hash function, which involves bitwise operations, modular additions, & compression functions.
- The result of this transformation is a fixed-size string that looks nothing like the original data.

• Key characteristics of SHA.

1) One-Way Function :- Once data is transformed into its hash value, it's virtually impossible to reverse the process & retrieve the original data.
2) Pre-Image Resistance :- Finding the original message given its hash value is computationally challenging. This property thwarts brute force attacks.
3) Collision Resistance :- Different inputs should produce distinct hash values to prevent unintended collisioins.

• Common SHA Algorithms :

- SHA-1 :- Developed in 1993, it produces a 160 bit (20-byte) hash value. Widely used but now considered obsolete due to vulnerabilities
- SHA-2 :- A family of algorithms (including SHA-224, SHA-256, SHA-384, & SHA-512) with stronger encryption. Used in security protocols like TLS, SSL & IPsec.
- SHA-3 :- Introduced as a successor to SHA-2 designed to withstand emerging threats.

- Applications of SHA:
- Password Encryption:-
Servers store users' hash value insted of actual passwords. If an attacker breaches the database, they won't find plain-text passwords.
- Data Tampering Detection:-
Even minor changes to a file result in drastically different hash values, making tampering noticeable.

Q.8) Write note on information protection law: Indian perspective

→ The information Technology ACT, 2000 (IT Act) is a crucial piece of legislation in India that addresses various aspects related to technology, electronic transaction, & cyber activities.
Here are some key points:

1) Background & origin.
- The It Act emerged from a resolution by the United nations Commission on International Trade Law (UNCITRAL) in 1997. UNCITRAL adopted the Mode Law on Electronic Commerce, which laid the groundwork for regulating electronic transactions globally.

2) Cyber Crimes & challenges:
- Cyber crimes are rapidly growing worldwide & India is no exception.
- The IT Act addresses serval pressing concerns related to misuse of technology in ciberspace.

q.9) What is Cyber Stalking ? How to identify & detect Cyber Stalking.

→ Threatening behavior or unwanted advances directed at another using the Internet & other forms of online & computer communications, called as ~~cyber~~ stalking.

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.

to identify & detect cyber stalking some signs are there

1) Signs of cyberstalking:

- Excessive Messages : If Someone sends you an overwhelming number of messages.
- Inappropriate Content : Receiving inappropriate or offensive messages.
- Social Media Behavior :- Liking all your old posts or manipulating you into interacting with them online.
- Trolling :- Deliberate attempts to provoke or upset you.
- Other Behaviors :- Online impersonation, GPS tracking, threatening messages catfishing & doxing are also associated with cyberstalking.

q.10) Consider a Diffie-Hellman Scheme with a common prime $q=11$, & primitive root $a=2$

a) If user A has the public key $Y_A=9$ What is A's private key X_A.

b) If user B has the public key $Y_B=3$ what is B's private key X_B.

1) If user A has the public key $Y_A = 9$ what is A's private key X_A

2) If use B has the public key $Y_B = 3$ what is B's private key X_B

→ i) $q = 11$, $\alpha = 2$, $Y_A = 9$, $X_A = ?$

$2 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

~~$2^9 \bmod 11 =$~~

~~$2^{10} \bmod 11 =$~~

Since $2^e \bmod 11$ for $0 < i < 11$ contains all numbers from 1 to 11-1, the size of this set is equal to $\phi(q)$, ther order of q.

From the above values $2^6 \bmod 11 = 9$

therefor $\boxed{X_A = 6}$

ii) From the above values..

$\alpha^{X_B} \bmod 11 = Y_B$

$\alpha^{X_B} \bmod 11 = 3$

$2^{X_B} \bmod 11 = 3$

$\therefore 2^8 \bmod 11 = 3$ from above values

$\therefore \boxed{X_B = 8}$

B 9/4/24

=11 Assignment No. 5 #11

Q.1) Difference between Packet filtering firewall & proxy (Application- level Gateway)

	Packet filtering firewall	Proxy. (Application level Gateway)
1)	Packet filtering firewall is simplest.	1) Application level Gateway Even more complex.
2)	Screens based on connection rules.	2) Screens based on behaviour or proxies
3)	Auditing is difficult	3) Activity can audit
4)	low impact on network ~~pre~~ performance.	4) High impact on network performance.
5)	Network topology can not hide	5) Network topology can hide from the attacker.
6)	Transparent to user.	6) Not transperent to user.
7)	~~Seer ob or~~ see only addresses & service protocol type.	7) Sees full data portion of a packet.

Q.2) Explain access control & its types in detail.

→ Acess control is an important tool of security to protect data & other resources.

- The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control includes
  1. Authentication of users.
  2. Authorization of their privileges.
  3. Auditing to monitor & record user actions.
- There are 3 types of access controls.

1) Discretionary access control
2) Mandatory access control
3) Role-based access control.

1) Discretionary access control. (DAC)

- Definition :- DAC assigns privileges based on rules specified by users. File systems often default to DAC, where file creators set access control parameters for their files.
- How It works : Users maintain control over access settings & can modify them at any time. A super admin role may override user ownership.
- Example :- In Windows & macos file systems, users automatically gain ownership of files they create, allowing them to view, edit, & share those files at their discription.

Benefits :-

1) Flexibility
2) Decreased IT Burden

2) Mandatory Access Control (MAC) :-

→ Definition :- Common in government & military organizations, MAC enforces access permissions based on hierarchical security levels.

- How It works :- The operating system enforces access restrictions created by system administrators.
- Example :- classified information systems use MAC to ensure strict control over data acess.
- Benefits :

High Security :- MAC provides strong security by enforcing predefined access rules.

Consistency :- Uniform access control across the organization.

3) Role - Based Access Control (RBAC) :-

- Definition :- RBAC assigns permissions Based on predefined roles. Users are grouped into roles, & access rights are associated with those roles
- How it works :- Administrators define roles (e.g. "manager", "developer") & allocate permissions accordingly.
- Ex) :- A project management system granting different access levels (view, edit, delet) based on user roles.
- Benefits.

1) Efficiency :-
Simplifies access management by grouping users.

2) Scalability :-
Easily adapts to organizational changes.

Q.3) Write a short note on any one.
i) Honeypot (ii) Distributed DOS attack

Honeypot:-

- honeypot is a system that can detect, monitor & sometimes tamper with the activities of an attacker.
- When attakers access the system, the honeypot monitors their activity without their knowledge We might set up a honeypot to ~~dri~~ provide an early warning system for a corporation, to discover an attacker's methods, or as an intentional target to monitor the activities of malware in the wild.
- Honeypots are designed to:-
  a) Divert an attacker from accessing critical systems.
  b) collect information about the attacker's activity.
  c) Encourage the attacker to stay on the system long enough for administrators to respond.
- Honeypots don't provide security for an organization but if implemented & used correctoly they enhance existing security policies & techniques.

Q.4) Discuss various flooding attacks.
→ Flooding attacks are classified based on network protocol used.
1) ICMP flooding.
2) UDP flooding.
3) TCP SYN flooding

- Flood attacks are also known as Denial of service (DOC) attacks. In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine. and& allow permitted network traffic.
For example, an ICMP flood attack, ~~attacker~~ occurs when a system receives too many ICMP ping commands & must be use all its resources to send reply commands.
- To prevent flood attacks in the default attacks in the default packet handling page, you can specify thresholds for the allowed number of packets per second for different types of traffic When the number of packets received on an interface exceeds the specified threshold, the device starts to drop traffic of that type on the interface.
- Source system sends a large number of TCP SYN packets to the target system. the SYN packet are used to begin a new TCP connection.
- When the target receives a SYN packet, it replies with TCP SYN ACK packet, which acknowledges the SYN packet & Sends connection setup information back to the source of the SYN
- The target also places the new connection information into a pending connection buffer.

Q.5) Explain any 2 types of Instrusion detection systems?

→ Types of Instrusion detection systems.

1) NIDS :- Network Instrusion Detection Sysem
A NIDS is tries to detect malicious activity such as denial of service attacks ; port scans or even attempts to crack into computers by network security monitoring of network traffic

- NIDS are placed at a strategic point or points within the network to monitor traffic to & form all devices on the network
- The majority of commercial instruction detection systems are network based.
- These IDSs detect attacks by capturing & analyzing network Packets.

2) HIDS :- Host-based IDSs
- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitered
- The agents supervise the OS & write data to log files & activate alarm.
- Host-based IDSs operad on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activitis with great reliability & precision determining exactly which processes & users are involved in a particular attack on the operating system.