Assignment No:4

① Define authentication system. Illustrate the need of mutual authentication over one-way authentication with an example.

⇒ An authentication system is a security mechanisms that verifies the identity of users, devices, or applications before granting access to a system, network or service. It ensures that only authorized entities can access specific resources by using credentials such as passwords, biometrics, digital certificates, etc.

In one-way authentication, only one party (typically the client) verifies the identify the other party (typically the server) This is commonly used in basic login mechanisms, where a client provides credentials to authenticate with a server.

Mutual authentication ensures that both the client and the server verify each other's identity before exchanging data. This prevents man-in-the-middle (MITM) attacks and unauthorized access.

Example: Scenario: Online Banking

① One-way authentication: A user visits an online banking website. The user enters their credentials. The bank server verifies the credentials and grants access.

Risk: If a hacker sets up a fake website (phishing attack), the user might enter their credentials, leading to account compromise.

② Mutual Authentication: The user visits an online banking website. The website provides a digital certificate to verify its legitimacy. The user's device verifies the certificate before entering credentials. The user provides credentials, and the bank server authenticates the user.

Advantage: Prevents phishing attacks.

CamScanner

② Explain about working Mechanism of Kerberos. How it differ from Needam Schroder?

⇒ Kerberos is a secret network authentication protocol that provides secure authentication over an insecure network using secret-key cryptography. It is widely used in distributed systems to prevent eavesdropping and replay attacks.

Steps in Kerberos Authentication:

① User Authentication Request:

The user logs in and request a Ticket Granting Ticket (TGT) from the Authentication Server (AS). The request includes the user's ID encrypted with a secret key (derived from password).

② Authentication Server (AS) Response:

The AS verifies the user's identity. It issues an encrypted TGT and a session key, which are sent to the user. The TGT is encrypted with the secret key of the Ticket Granting Server (TGS).

③ Service Ticket Request:

When the user wants to access a specific service, they send the TGT to the TGS. The TGS decrypts the TGT and verifies it. If valid, the TGS generates a Service Ticket and sends it to the user.

④ Accessing the Service:

The user presents the Service Ticket to the Service Server. The service server verifies the ticket and grants accessing.

Differences between Kerberos and Needam Schroder are:

Feature	Kerberos	Needam-Schroder
Authentication Model	Uses trusted third-party (KDC) for authentication.	Uses a key distribution center (KDC) for session key exchange.
Encryption Type	Uses symmetric key cryptography (Originally DES, now AES)	Two versions: symmetric (NSP-SK) and public-key (NSP-PK) cryptography.

Feature	Kerberos	Needham-Schroeder
Vulnerability	Protects against replay attacks using time-stamped tickets.	Vulnerable to replay attacks (fixed in modified versions)
Session Keys	Uses TGT and session keys for secure access to multiple services.	Exchanges a session key directly betⁿ the communicating parties
Mutual Authentication.	Yes, ensures both user and service verify each other.	Originally Needham-Schroeder didn't include mutual authentication

Hence, Kerberos improves upon Needham-Schroeder by using ticket-based authentication, time stamps and mutual authentication, making it more secure against replay attacks.

③ What is Rabin Miller primality test? Find if 61 is prime or not.

⇒ The Rabin Miller primality test is a probailistic algorithm used to determine if a given number is prime.

Steps of the Miller-Rabin primality test for 61:

(i) Express the number in the form of $n-1 = 2^k m$ (where m is odd)

i.e. $61-1 = 2^2 \times 15$ so, $k=2$ and $m=15$

(ii) Choose a random base a (where $1 \leq a \leq n-1$)

Let's pick $a=2$

(iii) Compute $b \equiv a^m \bmod n$.

i.e. $b \equiv 2^{15} \bmod 61$

$b = 11 \bmod 61$

Since, $b \neq 1$ proceed to next step.

(iv) Compute $b \equiv b^2 \bmod n$.

i.e. $b \equiv 11^2 \bmod 61$

$b \equiv 60 \bmod 61$

or, $b = -1$

Since, $b \equiv -1 \pmod n$. The number 61 is prime.

④ Miller-Rabin test for primality is based on the fact that there are only two numbers in Z_p that when squared give us 1. What are those numbers?

⇒ The Miller-Rabin primality test is based on the property that in the field Z_p (p is prime number), the only solutions to the eqn: $x^2 \equiv 1 \pmod{p}$ are: $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$. In other words, the only numbers in Z_p that when squared, give 1, are 1 and $p-1$.

⑤ What is meant by the strong collision resistance property of a hash function?

The strong collision resistance property of a hash function means that it should be computationally infeasible to find two different inputs x & y such that: $H(x) = H(y)$ (where, H is hash function and $x \neq y$.)

Its Importance:

i) Prevents Digital Signature forgery
ii) Ensures Data Integrity
iii) Security Against Attacks

⑥ How does Kerberos protocol ensure authentication and confidentiality in secure system? Explain.

⇒ Kerberos is a network authentication protocol that ensures that only legitimate users and services can communicate while maintaining confidentiality and integrity of the exchanged data.

Authentication in Kerberos is achieved through a trusted third-party known as Key Distribution Center (KDC), which consists of: ① Authentication Server (AS)
② Ticket Granting Server (TGS)

Authentication Process

① User Requests Authentication (Login)
② Request for Service Ticket
③ Accessing the Service

* The user is authenticated without sending passwords over the network.

Kerberos protects confidentiality using strong encryption and secure key exchange mechanisms:

① Encrypted Communication using symmetric-key cryptography.
② Session key for secure Communication.
③ Prevention of Replay Attacks.
④ Mutual Authentication

⑦ How Hash functions differ from MAC? Given a message m, discuss what arithmetic and logical functions are used by MD4 to produce message digest of 128 bits.

⇒ Differences between Hash Functions and Message Authentication Codes (MACs) are:

Feature	Hash Functions	MACs
Purpose	Ensures data integrity	Ensures data integrity + Authentication
Key Usage	No secret key used.	Requires a secret key
Output	Fixed-length message digest (hash value)	Fixed-length MAC value
Security	Provides collision resistance but no authentication.	Provides authentication (prevents message tampering)
Examples	SHA-256, MD5, SHA-3.	HMAC-SHA 256, HMAC-MD5,

CamScanner

Message Digest Algorithm 4 (MD4) is a cryptographic hash function that generates a 128-bit message digest using bitwise logical and arithmetic operations.

MD4 Processing Steps

① Padding the Message: The message m is padded so that its length is 448 mod 512. A 1-bit is appended, followed by zeroes and the message length (in bits) are as a 64-bit value.

② Initializing Buffers: MD4 maintains four 32-bit registers:

A = 01 23 45 67, B = 89 AB CD EF, C = FE DC BA 98

D = 76 54 32 10

These values acts as initial states for processing.

③ Processing in 512-bit Blocks: The padded message is divided into 512-bit blocks. Each block is processed in three rounds, each using logical and arithmetic functions.

④ MD4 Logical and Arithmetic Functions:

- Round 1: Nonlinear bitwise function (F)

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

- Round 2: Majority function (G)

$$G(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$$

- Round 3: XOR function (H)

$$H(X,Y,Z) = X \oplus Y \oplus Z$$

⑤ Updating Registers: After processing, the values of A, B, C, D are updated using bitwise shifts and additions.

⑥ Final Output: After processing all blocks, the concatenation of A, B, C and D forms the 128-bit message digest.

CamScanner

⑧ What do you mean by digital Signature? How digital signature can be enforced using encryptions? Illustrate with example.

⇒ A digital signature is a cryptographic mechanism used to verify the authenticity, integrity and origin of a message or document. It ensures that the sender of the message is legitimate and that the message has not been altered. It uses asymmetric cryptography where a private key is used to sign the message and a public key is used to verify the signature.

How Digital Signature are enforced using Encryption:

Digital signature rely on hashing and public-key encryption to ensure authenticity and integrity. The process involves two main steps:

① Signing the Message (Sender's Side)

The sender computes a hash of the original message using a hash function. The hash is encrypted using the sender's private key, creating the digital signature. The sender sends both the message and the digital signature to receiver.

② Verifying the Signature (Receiver's side)

The receiver decrypts the digital signature using the sender's public key to obtain the original hash. The receiver computes the hash of the received message. If both hashes match, the signature is valid, ensuring:

- Authenticity - Message is from the claimed server.
- Integrity - Message was not altered.
- Non-repudiation - Sender cannot deny signing the message.

Example: Digital Signature Using RSA

Let's assume Alice wants to send a signed message to Bob.

Step 1: i) Alice writes a message: "Transfer 1000 to Bob"

ii) Alice computes the hash (using SHA-256): Hash = SHA-256("Transfer 1000 to Bob")

iii) Alice encrypts the hash using her private key:
Digital Signature = Encrypt(Hash, Alice's Private Key)

iv) Alice sends the message + digital signature to Bob.

Step 2: i) Bob receives the message and digital signature.

ii) Bob decrypts the signature using Alice's public key:
Decrypted hash = Decrypt(Digital Signature, Alice's public key)

iii) Bob computes the hash of the received message:
Computed Hash = SHA-256("Transfer 1000 to Bob")

iv) If Decrypted Hash == Computed Hash, the signature is valid.

(10) Differentiate between direct digital signature and arbitrated digital signature. How signing and verifying process is done in Digital Signature standard.

⇒ The differences between direct digital signature and arbitrated digital signature are:

Feature	Direct Digital Signature	Arbitrated Digital Signature
Definition	A digital signature that is created directly bet" the sender and the receiver without involving a third party.	A digital signature where a trusted third party (arbiter) is involved in signing and verification.
Trust Dependency	Relies on the sender's private key and the receiver's trust in the sender.	Relies on a trusted third party (arbiter) to ensure validity.
Verification	The receiver verifies the signature	The arbiter verifies the signa-

CamScanner

Feature	Direct Digital Signature	Arbitrated Digital Signature
	using the sender's public key.	ture before forwarding the message.
Security Concerns	Vulnerable to key compromise; sender may deny signing the message.	Provides non-repudiation and resolves disputes with the help of the arbiter.
Usage	Used in peer-to-peer communications and blockchain transactions.	Used in high-security transactions, Legal contracts and dispute prone scenarios.

Signing and Verifying Process in Digital Signature Standard:
The Digital Signature Standard (DSS) is U.S. government standard for digital signatures, based on the Digital Signature Algorithm (DSA).
Step 1: Signing Process
① Hash the Message
② Generate Signature using DSA
Then the sender sends the message and signature to receiver.
Step 2: Verification Process
① Hash the Received Message
② Verify the signature

(11) How padding is done in SHA-1? How 160-bit of hash value is generated by taking an input message of variable size using SHA-1?

⇒ Secure Hash Algorithm 1 (SHA-1) processes a message in 512-bit blocks. If the input message is not a multiple of 512 bits, padding is applied to ensure it conforms to the required block size.

CamScanner

SHA-1 Padding Steps:

① Append a '1' Bit : A single 1-bit is added to the message.

② Append Zeros: Zeros are added until the message length is 448 mod 512 (so that 64 bits remain for the length field).

③ Append Message Length: The 64-bit representation of the original message length (in bits) is appended at the end.

SHA-1 generates a 160-bit (20-byte) hash by processing variable sized input in 512-bit blocks using a five-stage hashing process.

Steps of SHA-1 Hash Computation:

① Message Preprocessing (Padding)
② Initialize five 32-bit Hash Value
③ Processing Each 512-bit Block (80 rounds)
④ Updating Hash Values
⑤ Final Hash Value Computation

⑫ Define authentication system and its components. How hardware-based challenge response systems can be used as authentication approach.

⇒ An authentication system is a security mechanisms used to verify the identity of users, devices, or systems before granting access to resources.

Authentication system consists of five components:

① The set A of Authentication Information is the set of specific information with which entities prove their identities

② The set C of Complementary Information is the set of

information that the system stores and uses to validate the authentication information.

③ The set F of complementation functions that generate the complementary information from the authentication information. i.e. for $f \in F$, $f: A \rightarrow C$

④ The set L of authentication functions that verify identity. i.e. for $l \in L$, $L: A \times C \rightarrow \{true, false\}$

⑤ The set S of selection functions that enable an entity to create or alter the authentication and complementary information.

A challenge-response authentication system (CRAS) is a method where the system generates a random challenge, and the user/device must generate a valid response to authenticate.

How it works:

① Challenge Generation: The authentication system sends a random challenge to the user or device.

② Response Computation: The user/device processes the challenge using a cryptographic function and a secret key. The computed response is sent back to the authentication system.

③ Verification: The authentication system performs the same cryptographic function to verify if the received response is correct. If the response matches, authentication is successful.

CamScanner

(13) How padding is done in MD5? What enhancements in MD4 are done to get better hash function MD5?

⇒ MD5 padding Steps:

① Append a '1' Bit : A single 1-bit is added to the message.

② Append zeros : Zero bits are added until the message is 448 mod 512 (so that 64 bits remain for length field)

③ Append Message length: The 64-bit representation of the original length (in bits) is appended at the end.

Enhancements in MD5 over MD4

MD5 is an improved version of MD4, designed to provide better security and collision resistance.

Feature	MD4	MD5 (Enhancements)
Rounds	3 Rounds	4 Rounds (Added Complexity)
Bitwise operations	Weaker mixing of bits.	Improved bitwise operations for diffusion.
Message padding	Similar padding	More structured padding to prevent length extension attacks
Security	Faster but weaker	More computational steps for better security
Checksum vulnerability	Susceptible to collisions	Stronger against checksum forgery

(14) What do you mean by password aging? How online dictionary attack differ from offline attacks?

⇒ Password aging is a security policy that enforces periodic password changes for users. It sets a maximum password lifespan, requiring users to update their passwords after a specified time to reduce the risk of password-based attacks.

CamScanner

Password Aging is important due to following reasons:

1) It reduces the chances of attackers using stolen passwords for extentended periods.
2) It helps mitigate brute-force and dictionary attacks.
3) It forces user to create stronger, more secure passwords regularly.

A dictionary attack is a type of password-cracking technique that systematically tries common passwords. These attacks can be either online or offline based on how they are executed.

Feature	Online Dictionary Attack	Offline Dictionary Attack
Attack Method	Tries password guesses against a live authentication system (eg. login page)	Uses a captured database of hashed passwords & tries to crack them offline.
Speed	Slower, limited by network and system restrictions.	Faster, as the attacker can use unlimited resources.
Detection Risk	High - Systems detect and block multiple failed attempts	Low - No direct interaction with authentication servers, so detection is difficult.
Prevention	Multi-factor Authentication (MFA), CAPTCHA, Rate Limiting.	Strong hashing (eg. bcrypt, Argon2) Salting passwords.

(15) What is the importance of Trap Door function in cryptography?

⇒ A trapdoor function is a one-way mathematical function that is easy to compute in one direction but hard to reverse unless a special piece of information (the "trapdoor") is known. It is a crucial concept in public-key cryptography.

CamScanner

Importance of Trapdoor function:

① Foundation of Public-key Cryptography: Trapdoor functions allows secure key exchange, digital signatures, etc.

② Asymmetric Encryption: A public key is used for encryption and a private key (trapdoor) is required for decryption.

③ Digital Signature: The trapdoor function ensures that only the private key holder can generate the signature.

④ Key Exchange Mechanism: Secure key exchange relies on trapdoor functions to prevent interception.

⑤ Enhances Security Against Attacks: Without the trapdoor, reversing the function requires solving computationally infeasible problems.

⑯ What are errors in Biometric? Explain.

⇒ Biometric systems use physical or behavioural characteristics to verify identity, such as fingerprints, facial recognition, etc. However, these systems are prone to errors due to various factors like sensor quality, environmental conditions, etc.

Types of Biometric Errors:

① False Acceptance Rate (FAR):- It is the probability that an unauthorized person is mistakenly accepted as an authorized user.

② False Rejection Rate (FRR):- It is the probability that an authorized person is wrongly rejected by the biometric system.

③ Equal Error Rate (EER) - Accuracy Indicator:
It is the point where FAR and FRR are equal.

CamScanner

(17) How MAC differs from Hash? What is difference between authentication and authorization? Explain with examples.

⇒ MAC provides both integrity + authencity, while Hash only ensures integrity.

Differences between Authentication and Authorization:

Feature	Authentication	Authorization
Definition	Verifies who you are.	Defines what you can do.
Purpose	Confirms identity using credentials (password, biometrics, etc).	Grants or restricts access to resources based on permissions.
Process	First step in security	Second step after authentication.
Example	logging into an account with a password.	Accessing admin-only pages after login.
How it Works?	Uses passwords, biometrics, OTPs.	Uses roles, permissions, access control lists (ACLs)
Example in Web Apps.	A user enters a username and password to login.	Once logged in, the user can access certain pages based on their role.

(18) What is meet in Middle Attack in Data Encryption Standard (DES)? Explain.

⇒ The Meet-In-the-Middle (MitM) attack is a cryptanalytic attack that reduces the time complexity of brute-force attacks against double encryption schemes. It is particularly relevant to Double DES (2DES) which applies DES encryption twice with two different keys.

How the Meet-in-the-Middle Attack Works?

Instead of trying all 2^{112} possible key combinations, the attacker breaks the encryption into two separate computations, significantly reducing complexity.

CamScanner

⊙ Steps of the Attack:

① Encryption Phase (Forward Computation)

→ The attacker encrypts the plaintext (P) will all possible values of K1. Stores intermediate results $X = E_{K1}(P)$ in a lookup table.

② Decryption Phase (Backward Computation)

→ The attacker decrypts the ciphertext (C) with all possible values of K2. If $D_{K2}(C)$ matches any intermediate X in the table, a key-pair candidate (K1, K2) is found.

③ Final Key Verification

→ The correct key pair is tested on another plaintext-ciphertext pair to verify correctness.

How to Prevent MitM attacks:

① Using Triple DES (3DES)

② Using Advanced Encryption Standard (AES)