Can’t send the password in clear or the hashed value as hash is susceptible to replay attack.

Sniffing – external person monitoring the network.

A replay attack is a network security issue where a valid data transmission is maliciously or fraudulently repeated or delayed.

This type of attack is a form of network attack in which a valid data transmission is repeated or delayed. In a typical scenario, the attacker intercepts a data transmission, a packet or a series of packets containing valuable information (like authentication tokens), and then retransmits them to produce an unauthorized effect.

Here's how a replay attack typically works:

1. **Interception**: The attacker captures data being transmitted between two parties. This could include login requests, transaction details, or any other sensitive information.
2. **Replay**: The attacker then resends the captured information to the original recipient. The goal is to trick the recipient into thinking that the message is a new request.
3. **Unauthorized Access or Effect**: If successful, the replay attack can grant access to sensitive systems, allow for unauthorized transactions, or cause other harmful effects, depending on the nature of the intercepted data.

To prevent replay attacks, several strategies can be employed:

* **Timestamps**: Including a timestamp in the data packet, which the receiver checks to ensure timeliness.
* **Nonce**: A nonce (number used once) can be used so that each transmitted message is unique.
* **Encryption**: Employing strong encryption can make intercepted data useless to an attacker.

Sniffing

"Sniffing" in the context of network security refers to the practice of intercepting and examining data packets as they travel across a network. The purpose of sniffing can be either legitimate or malicious, depending on the intent of the individual performing the sniffing.

**Legitimate Uses of Sniffing**

1. **Network Management and Troubleshooting**: Network administrators use packet sniffing to monitor and troubleshoot network traffic. It helps in identifying network bottlenecks, lost packets, and other issues affecting network performance.
2. **Security Analysis**: Security professionals may use sniffing to monitor network traffic for signs of malicious activity, such as unauthorized data transmissions or intrusion attempts.
3. **Performance Analysis**: Analyzing network traffic can provide insights into usage patterns, helping to optimize network resources and performance.

Analyzing network traffic can provide insights into usage patterns

**Malicious Uses of Sniffing**

1. **Eavesdropping**: Malicious actors can use sniffing to intercept sensitive information, such as passwords, emails, and financial data, which are transmitted over the network.
2. **Man-in-the-Middle Attacks**: By capturing data packets, attackers can modify them and then forward them to the recipient, leading to a breach of data integrity.
3. **Session Hijacking**: Attackers can capture session tokens or cookies to gain unauthorized access to a user's account or session.

**Types of Sniffing**

* **Passive Sniffing**: This involves monitoring traffic without altering it in any way. It’s harder to detect and is usually effective in a non-switched network environment.
* **Active Sniffing**: Involves injecting packets into the network to induce responses or changes in network behavior. This method is used in switched networks.

**Countermeasures**

* **Encryption**: Using encryption protocols like SSL/TLS can help protect data in transit.
* **Secure Network Design**: Designing networks with security in mind, including the use of switches and VLANs, can limit the scope of sniffing.
* **Anti-Sniffing Tools**: These tools can detect the presence of sniffing programs on a network.
* **Strong Authentication Mechanisms**: Implementing multi-factor authentication can reduce the risks associated with intercepted credentials.

Understanding and implementing security measures against sniffing is crucial in safeguarding sensitive data and maintaining the integrity and confidentiality of network communications.

Can encrypt anything with a secret key and send it .Anyone who has public key can decrypt that. This is proof that I have secret key.

The scenario you've described seems to be a mix of concepts from symmetric and asymmetric cryptography. Let's clarify these concepts:

**Symmetric Cryptography**

In symmetric cryptography, the same key is used for both encryption and decryption. If you encrypt something with a secret key, only someone who has that same secret key can decrypt it.

This method does not involve a public key and is primarily used for ensuring data confidentiality.

**Asymmetric Cryptography**

Asymmetric cryptography, on the other hand, involves a pair of keys: a public key and a private (or secret) key. These keys have a unique relationship:

* Anything encrypted with the **public key** can only be decrypted with the corresponding **private key**.

If I want to send a message to someone have to encrypt using their public key.

* Conversely, anything encrypted with the **private key** can be decrypted with the corresponding **public key**. This is less common but is used in digital signatures.

**Your Scenario: Digital Signatures**

The scenario you describe aligns more with a digital signature, which is a use case of asymmetric cryptography:

1. **Signature Creation**: You encrypt data (typically a hash of the message) with your private key. This encrypted hash is your digital signature.
2. **Verification**: Others can use your public key to decrypt the signature. Since only your private key could have been used to encrypt the data in a way that your public key can decrypt, this process verifies that the signature was created by the holder of the private key.
3. **Proof of Ownership**: Successfully decrypting the signature with the public key proves that the signer possesses the corresponding private key, without revealing the key itself.

**Key Points**

* Encrypting data with a private key for others to decrypt with the public key is not about keeping the data secret (as anyone with the public key can decrypt it) but about proving authenticity and integrity.
* This method ensures that the data hasn't been tampered with and that it was indeed created by the holder of the private key.

This mechanism is a foundational principle in various security protocols, including SSL/TLS for secure web communications and in verifying the authenticity of software and digital documents.

A certificate, in the context of digital security and cryptography, refers to a digital certificate, also known as a public key certificate or identity certificate. It's a crucial component in securing digital communications and establishing trust over the internet. Here's an overview:

**Purpose of a Digital Certificate**

1. **Identity Verification**: Certificates confirm the identity of the certificate holder. For instance, a web server's certificate verifies that the server you're connecting to is actually the one it claims to be.
2. **Secure Communication**: They enable secure, encrypted communication between two parties, such as a web browser and a server.

**Components of a Digital Certificate**

A digital certificate typically includes:

1. **Public Key**: The certificate holder’s public key.
2. **Identity Information**: Information about the certificate holder, such as a domain name for websites.
3. **Issuer Information**: The details of the Certificate Authority (CA) that issued the certificate.
4. **Validity Period**: The timespan for which the certificate is valid.
5. **Serial Number**: A unique number assigned to each certificate for identification.
6. **Digital Signature**: The CA’s digital signature, ensuring the certificate's authenticity.

**How Digital Certificates Work**

* **Issuance**: A trusted third party, known as a Certificate Authority (CA), issues the digital certificate. The CA verifies the identity of the entity requesting the certificate (like a website) before issuing it.
* **Usage**: When you connect to a secure website (using HTTPS), the website presents its certificate. Your browser checks this certificate for authenticity.
* **Trust**: Your browser has a list of trusted CAs. If the certificate is signed by a trusted CA, the browser establishes a secure, encrypted connection using the website's public key.

**Certificate Authorities (CAs)**

* CAs play a vital role in the security of digital certificates. Examples include Let's Encrypt, VeriSign, and Comodo.
* They are responsible for ensuring that the information in the certificate is correct and that the certificate holder is indeed who they claim to be.

**Types of Certificates**

1. **SSL/TLS Certificates**: Used for securing internet communications, commonly seen on websites.
2. **Email Certificates**: For securing and authenticating email communications.
3. **Code Signing Certificates**: For verifying the authenticity and integrity of software code.

**Importance in Internet Security**

Digital certificates are a cornerstone of internet security. They prevent man-in-the-middle attacks, ensure data privacy, and help maintain trust in the digital world. Every time you see a lock icon in your web browser's address bar, it indicates a secure connection established using digital certificates.

For private key certificates , no need to ask any authority to sign it.

Must encrypt the private key certificate so it is not easily accessible to anyone who breaks into computer.

Someone can insert key logger into computer and find out password for bank transactions.

Security of private key certificate never greater than computer

Certificate kept on computer – soft certificate

Use and Importance of a Soft Certificate with a Private Key

1. **Authentication:** The private key in the certificate is used to authenticate the user or device to other systems. For instance, when connecting to a secure server, the server might request a certificate from the client (your computer) to verify the client's identity.
2. **Secure Communication:** In secure communication protocols like SSL/TLS (used in HTTPS), the private key is used to establish a secure, encrypted connection. It's part of the process that ensures that the data exchanged between your computer and the server remains confidential and unaltered.

Connecting SEB keypad and mastercard to computer for short amount of time to do things.What makes it better than a soft certificate.

Answer – smart card idea.

Schematic representation of what’s going on inside smart card.

On smart card is the secret key. Smart card communicating with keypad which is communicating with computer through some interface and data is going back and forth.

Reason – smart card is smart ,they are processors so can ask them to do things.

Once the cards have been made for you by the bank ,they are made with a kind of barrier in the card.

It shouldn’t be possible to access key through interface.

Operations inside card have access to key but from outside can only ask for these things to be done.

Can never ask to see the key.

This gives us a new concept. This is also the idea of a certificate.

This is what we call a hard certificate.

Critique of biometrics

Biometrics are not ultimate security solutions.

Biometrics can be false positives, someone else’s iris might match to ours. Might get false negatives,

Measurement is measured against stored biometrics.

Our fingerprints are left behind on things.

You're absolutely correct in stating that biometrics are not the ultimate security solution, and they do have limitations such as false positives and negatives. Let's explore these issues in more detail:

**False Positives in Biometrics**

* **Definition**: A false positive, also known as a Type I error, occurs when a biometric system incorrectly identifies an individual as someone else or grants access to an unauthorized person.
* **Implications**: This is a significant security risk, especially in high-security environments, as it allows unauthorized access.
* **Example**: A facial recognition system might incorrectly match a person's face with another individual in the database, granting them access to restricted areas or information.

**False Negatives in Biometrics**

* **Definition**: A false negative, or a Type II error, happens when the system fails to recognize an authorized person.
* **Implications**: This leads to inconvenience and potential operational delays, especially in critical applications like healthcare or law enforcement.
* **Example**: A fingerprint scanner might fail to recognize a registered user's fingerprint, perhaps due to minor injuries or changes in the skin.

**Dependence on Stored Biometric Data**

* **Data Storage**: Biometric systems work by comparing the presented biometric data (like a fingerprint or iris scan) with the stored data.
* **Security of Storage**: The security and integrity of the stored data are crucial. If the database is compromised, it can lead to widespread security breaches.
* **Irreversible Compromise**: Unlike passwords or PINs, biometric data cannot be changed. Once compromised, it cannot be 'reset' or 'reissued'.

**Other Limitations and Concerns**

1. **Environmental Factors**: Biometric systems can be sensitive to environmental conditions. For example, poor lighting can affect facial recognition, and dirty fingers can affect fingerprint scans.
2. **Physical Changes**: Changes in physical appearance, aging, injuries, or medical conditions can affect biometric recognition accuracy.
3. **Privacy Issues**: Storing and handling biometric data raises significant privacy concerns. Misuse or unauthorized access to biometric data is a serious invasion of privacy.
4. **Inclusivity**: Not all biometric systems are accessible to all users. For instance, people with certain disabilities might find it challenging to use some forms of biometric authentication.
5. **Cost and Complexity**: Implementing and maintaining biometric systems can be expensive and technologically complex, making it less feasible for smaller organizations.

**Conclusion**

While biometrics offer a high level of security and convenience, they are not infallible and should ideally be used as part of a multi-factor authentication system, rather than the sole method of security. This approach combines something you know (like a password), something you have (like a token), and something you are (biometrics) to enhance overall security.

Top of Form

The correct answer is: A face reader's digital output is recorded by a device and later connecting that recording device to an  authentication system can cause it to register that a legitimate face has just been presented. → Replay attack, My fingerprint reader on my computer signals that my fingerprint does not match → False negative, I have to remember my PIN code to be able to get money out at an ATM with my cash card → Multifactor authentication, My private key is kept on my computer with other useful data, which allows me to use that computer to surf to certain secure web sites and easily log on without the need of any token device → Soft certificate