**Identity and Authentication**

1. **What is the difference between identity and authentication?**
   1. It is the capability of an **authentication system** to prove that a user is, in fact, the person or application that he or she is claiming to be. **Identification** is the ability to determine uniquely who is using the system or what application is running on the system.
2. **In what situations should each of these be used or not used?**
   1. The **authentication** process always takes precedence over the **authorization** process. This is due to the fact that identification is a prerequisite for authorization since *you cannot authorize a user or service before you identify them.*

**Authentication Methods**

Name three types of authentication methods used today. Explain the advantages and disadvantages of each.

**Two-Factor Authentication:** There are several pros to 2FA, including adding a second layer of security, adding variety, and being cost-effective. The cons are that it takes time, is not foolproof, and may not function properly at times.

**Challenge Handshake Authentication Protocol:** The authenticator challenges the requestor with a hashed message. CHAP is one-way, but if the values match, the authentication succeeds. There is no problem with mutual authentication because the secret set is the same in both directions. However, it does not work as well for large installations, as each secret must be accessible both ways. Furthermore, it cannot use commonly available irreversibly encrypted password databases.

**Biometric:** In addition to high security and assurances, biometric identification provides answers to questions like what a person has and what he/she is. Since each individual has their own unique set of biometrics, they are difficult to steal or fake. Biometric authentication has a number of disadvantages, such as high costs, data breaches, privacy concerns, bias, and the possibility of false positives or errors.

**Caesar Encryption**

1. **Give at least two examples of a type of encryption that is in the Caesar model.**
   1. Traditionally, Caesar ciphers shift each letter of the plaintext message by three letters. This is a substitution cipher, which is characterized by the consistent substitution of letters for each other.
2. **Explain the process of deciphering a Caesar shift.**
   1. It is possible to decrypt the ciphertext by applying the same amount of shifts in the opposite direction

**AES and DES. Two modern Encryption Standards**

1. **How are AES and DES both different than the Caesar encryption model?**
   1. The Feistel network is utilized by DES for structuring the encrypted block, whereas AES utilizes a series of substitutions and permutations to generate the encrypted block.
2. **Explain the differences between AES and DES and why one is superior to the other.**
   1. Through substitutions and permutations, AES creates the encrypted block, resulting in greater security than DES. AES is the world's most widely used cipher since DES has known vulnerabilities that can be easily exploited.
3. **Explain how the XOR operator works and how it relates to encryption algorithms.**
   1. By bitwise XORing all characters with a given key, a string of text can be encrypted. Then, when you want to decrypt the output, simply apply the XOR function to the output again with the key.
4. **The AES algorithm uses as block cypher. What alternatives are there to block cyphers? What are the advantages and disadvantages of a block cypher?**
   1. It is possible for stream ciphers to be used as an alternative to block ciphers. Due to the necessity of capturing the entire block for encryption/decryption, block ciphers have the advantages of high diffusion and strong tamper resistance without detection. Moreover, block ciphers are vulnerable to errors, since an error in one symbol can result in an entire block being altered.

**Symmetric vs Asymmetric Encryption**

1. **Explain the differences between symmetric and asymmetric encryption.**
   1. In symmetric encryption, a single key needs to be shared among all recipients, whereas in asymmetric encryption, messages are encrypted and decrypted using a pair of public keys and private keys.
2. **What are the advantages and disadvantages of each method?**
   1. Symmetric encryption has the advantage of speed and efficiency when dealing with large volumes of data; however, it has the disadvantage that the key must be kept secret. This can pose a particular challenge when encryption and decryption take place at different locations, requiring the key to be moved between them safely.
3. **Explain the difference between a public and private key.**
   1. There are two types of encryption keys: private keys and public keys. Private keys are used for both encrypting and decrypting sensitive data. They are shared by the sender and recipient of encrypted data. Public keys are used primarily for encrypting data.
4. **Explain the role of prime numbers in the creation of a public and private key.**
   1. The prime factors of a composite number are difficult to find without knowing the factors in the first place, which is why prime numbers are used in cryptography. As a result, someone without the necessary key cannot intercept the message and read it.

**Hashing vs Encryption**

1. **Explain the purpose of a hashing algorithm. Explain how it is different than encryption.**
   1. Hashing is one-way, which means that the plaintext cannot be reversed. Encryption is two-way, which means that the data can be decrypted.
2. **Explain how a computer system can use hashing to ensure passwords are private.**
   1. Hashing is the process of converting any password (or other piece of data) into a short string of letters and/or numbers using an encryption algorithm. Cyber criminals do not gain access to your password when a website is hacked, rather, they obtain access to the encrypted “hash” created by your password. In the absence of a corresponding salt, the data cannot be retrieved.
3. **Explain how hackers use a rainbow table and how you can defeat them.**
   1. Using passwordless authentication such as biometrics should be used instead of passwords, salting is recommended when storing passwords, you should monitor your servers and refrain from using outdated hashing algorithms.

**Sources:**

Identity, B. (n.d.). Rainbow table attack: Beyond identity. What is a Rainbow Table Attack? | Beyond Identity. Retrieved from https://www.beyondidentity.com/glossary/rainbow-table-attack

Passwordless authentication: What it is and how it works. Beyond Identity. (n.d.). Retrieved September 22, 2022, from https://www.beyondidentity.com/resources/passwordless-authentication

Stubbs, R. (n.d.). An overview of symmetric encryption and the key lifecycle. Cryptomathic. Retrieved September 22, 2022, from https://www.cryptomathic.com/news-events/blog/an-overview-of-symmetric-encryption-and-the-key-lifecycle