Pamela Mena – 00211564

Homework 2

Exercise 1

1. Suppose a password is chosen as a concatenation of seven lower-case dictionary words. Each word is selected uniformly at random from a dictionary of size 50,000. An example of such a password is "mothercathousefivenextcrossroom". How many bits of entropy does this have?

$$Entropy\ (bits) = \log_2(N^L)$$

$$N \rightarrow size\ of\ the\ dictionary$$

$$L \rightarrow length\ of\ the\ password$$

$$Entropy = \log_2(50000^7)$$

$$Entropy = 7 \times \log_2(50000)$$

$$Entropy = 109.2675\ bits$$

2. Consider an alternative scheme where a password is chosen as a sequence of 10 random alphanumeric characters (including both lower-case and upper-case letters). An example is "dA3mG67Rrs". How many bits of entropy does this have?

$$Entropy\ (bits) = \log_2(N^L)$$

$$Entropy = \log_2(62^{10})$$

$$Entropy = 10 \times \log_2(62)$$

$$Entropy = 59.5419\ bits$$

3. Which password is better, the one from 1. or 2.?

The 7-word password is the better password, as it has slightly higher entropy than the 10-character alphanumeric password. This means that it would be more difficult for an attacker to crack using a brute-force attack. However, the 10-character alphanumeric password is also a very strong password, and it would be very difficult for an attacker to crack.

Ultimately, the best password scheme will depend on specific needs and preferences. For example, if the goal is looking for the highest possible level of security, then the 7-word password is the better option. In the other hand, looking for a password that is easier to remember, then the 10-character alphanumeric password is a good choice.

Exercise 2

1. Design a data verification system using hash functions. Explain the steps involved in the process.

Data Verification System Using Hash Functions:

a. A user must input their data into the system, it could be any digital information, documents, passwords, or a file.
b. Generate a hash value of the data generated by a hash function takes an input and produces a consistent-sized output that is unique.
c. The hash value is stored in the secure storage location that might be a database or a distributed ledger technology such as blockchain or alongside the original data. It's crucial to securely store this hash value.
d. To verify the authentication, the system should perform a comparison between the hash value generated using the hash function and the hash value retrieved from the secure storage location.
e. The two hash values are compared and if both hash values are equivalent, the data is considered to be authentic. Otherwise, the data has been tampered with.

2. Discuss the advantages and disadvantages of using hash functions for data verification.

Advantages:

- The hash functions are very efficient at calculating hash values.
- Hash functions are resistant to collision attacks, which means that it is very difficult to find two different pieces of data that have the same hash value.
- They are transparent algorithms, which means that anyone can inspect the code to verify that it is working as intended.

Disadvantages:

- The hash functions can produce false positives, which means that two different pieces of data may have the same hash value.
- Hash functions are irreversible, which means that it is impossible to calculate the original data from the hash value.
- The use of hash functions for data verification it can be vulnerable to preimage attacks, where the attacker tries to find the original data that produces the hash value.

3. Provide an example of a real-world application where a data verification system using hash functions is used.

Digital signatures serve to confirm the legitimacy of electronic documents. At present, when a document receives a digital signature, a hash value is computed and subsequently encrypted with the private key of the signer. This encrypted hash value is affixed to the document as its

digital signature. During the verification process, the hash value of the document is recalculated and compared to the encrypted hash value within the digital signature. If these two hash values correspond, the document is deemed genuine.

Exercise 3

1. Define what a Message Authentication Code (MAC) is and how it is used in cryptography.

A message authentication code (MAC) is a cryptographic checksum employed in network communication to ensure the message's integrity and authenticity. It's a concise piece of data used to confirm that a message remains unaltered during transit and originated from the claimed sender. It functions as a means to verify that a message hasn't been tampered with during its journey and indeed originated from the anticipated sender.

2. Explain the process of generating and verifying a MAC.

There are 2 perspectives from which the process can be explained:

<u>Generating a MAC (Sender's Perspective)</u>

a. The sender and receiver must share a secret key, it is known only by the sender and is used to generate and verify the MAC.
b. The sender has a message or data they want to protect, can be a plaintext message, a file, or any piece of data that needs to be authenticated.
c. To generate the MAC, the sender combines the secret key and the message. Where a MAC algorithm involves using a hash function.
d. Finally, the sender sends the original message and the generated MAC to the receiver.

<u>Verifying a MAC (Receiver's Perspective)</u>

a. The receiver knows that the sender and they share a secret key.
b. Receives the message and the MAC from the sender, might be sent alongside the message.
c. The receiver uses the same MAC algorithm, the secret key, and the received message to recalculate the MAC.
d. The receiver compares both MACs. If the two MACs match, it indicates that the message is authentic. If they don't match, it suggests that the message has been altered during transit.
e. Based on the comparison result, the receiver can decide the authenticity of the ciphertext. If the MACs match, the ciphertext is considered valid and unaltered. If the MACs don't match, the receiver may reject the message.

3. Discuss the importance of using MACs in secure communication systems.

Message Authentication Codes (MACs) play an important role in secure communication systems, offering robust mechanisms to confirm the authenticity and integrity of messages. This verification process serves as a potent defense against data tampering and spoofing attacks, ensuring that the transmitted data remains unaltered and has indeed been sent by the expected source.

MACs are integral components of secure communication systems, countering critical threats like spoofing attacks. In the event of an attempt to tamper with a message, the MAC difference signals a problem, allowing the receiver to quickly spot the change and protect the communication's integrity. Furthermore, MACs are indispensable in the realm of secure protocols such as IPsec, TLS, and SSH, where they ensure the authenticity and integrity of transmitted data.

Exercise 4

1. Given the values of p = 17 and q = 23, generate a pair of keys for RSA.

The pair of keys for RSA were obtained using a small python script:

$$Public\ Key(e,n): 3\ 391$$

$$Private\ Key(d,n): 235\ 391$$

Exercise 5

1. Design a public key infrastructure (PKI) system. Explain the components and their roles in the system.

A public key infrastructure (PKI) system encompasses a collection of rules, protocols, equipment, and software designed for the establishment, administration, and invalidation of digital certificates. These certificates are digital records that associate a public key with a specific identity. PKI systems serve to enhance the security of diverse applications, such as internet browsing, email, and the verification of digital signatures.

The main components of a PKI system are:

Certificate Authority (CA): The Certification Authority (CA) has the duty of granting and withdrawing digital certificates. It is tasked with providing digital certificates to end users following a confirmation of their identity.

Registration authority (RA): The Registration Authority (RA) has the duty of enrolling certificate applicants and gathering their details. It serves as an intermediary between users and

the Certification Authority (CA), conducting identity verifications and verifying certificate applications.

Certificate repository: The duty is of enrolling certificate applicants and gathering their details. It serves as an intermediary between users and the Certification Authority (CA), conducting identity verifications and verifying certificate applications.

Certificate revocation list (CRL): The CRL is a list of digital certificates that have been revoked. The CRL is typically published by the CA or the RA.

2. Discuss the advantages and challenges of implementing a PKI system.

Advantages:

- PKI systems can help to improve the security of communication and data by verifying the identity of users and devices, and by encrypting communication.
- PKI systems can help to reduce the risk of fraud.
- These systems can help organizations to comply with regulations that require strong authentication and data protection.
- PKI systems can help to improve the efficiency of business processes by automating tasks such as user authentication and digital signature verification.

Disadvantages:

- PKI systems can be expensive to implement and maintain.
- PKI systems can be complex to implement and manage.
- These systems require users to be trained on how to use them properly.
- The PKI systems from different vendors may not be interoperable.

3. Provide an example of a real-world application where a PKI system is used.

In a real-world application, a PKI system secure browsing experience offered by HTTPS. This protocol employs PKI to encrypt communication between web browsers and servers, ensuring user data privacy and guarding against man-in-the-middle attacks. When users access an HTTPS-enabled website, their browser authenticates the website's digital certificate. This certificate contains vital information about the website, including its domain name and public key. Once the digital certificate's authenticity is confirmed, the browser establishes a secure, encrypted connection with the web server.

Exercise 6

1. Design a system for digital signatures based on public-key cryptography. Explain the steps involved in the process and the role of each component.

The system for digital signatures components and their roles:

Signer: The signer is the entity that creates the digital signature, has a private key that is used to sign messages. The signer is responsible for creating the digital signature.

Verifier: The party responsible for authenticating the digital signature using the signer's public key and ensuring its validity. Verification of the digital signature is within the verifier's purview.

Hash function: The cryptographic function that produces a hash value from a given input. This hash value serves the purpose of validating the message's integrity.

The process to create and verify digital signatures:

1. The sender calculates the message's hash for the purpose of signing.

2. The sender protects the hash value by encoding it with their private key.

3. The sender sends both the encrypted hash value and the message to the recipient.

4. The recipient computes the hash value of the received message.

5. The recipient deciphers the encrypted hash value using the sender's public key.

6. The recipient confirms the consistency of the two hash values, ensuring that if they are identical, the message remains unaltered.

References

TechTarget. (2023). Message Authentication Code (MAC). Available at: https://www.techtarget.com/searchsecurity/definition/message-authentication-code-MAC#:~:text=What%20is%20a%20message%20authentication,guarantee%20its%20integrity%20and%20authenticity

Chockhani. (2003). Internet X.509 Public Key Infrastructure. Available at: https://www.rfc-editor.org/rfc/rfc3647

IBM. (2021). Public key cryptography. Available at: https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography

Shreyaadaga. (2022). Password verification using Hashing. Available at: https://medium.com/@shreyaadaga/password-verification-using-hashing-6bbcc0342e2