Computer Security

Homework 2

Exercise 1:

1. Suppose a password is chosen to concatenate 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?

$$alphabet = 26\ chars$$

$$avg\ english\ word\ lenght = 4.7\ chars$$

$$avg\ pasword\ size = 4.7\ (7) = 32.9 \sim 33\ chars$$

$$E = -p(\log_2(p))$$

$$E = -\sum_{i=1}^{33} p_i(\log(p_i))$$

$$p = \frac{1}{26}$$

$$E = -\sum_{i=1}^{33} \frac{1}{26}\left(\log\left(\frac{1}{26}\right)\right) \sim 5.9659$$

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?

$$alphabet = 62\ chars$$

$$pasword\ size = 10$$

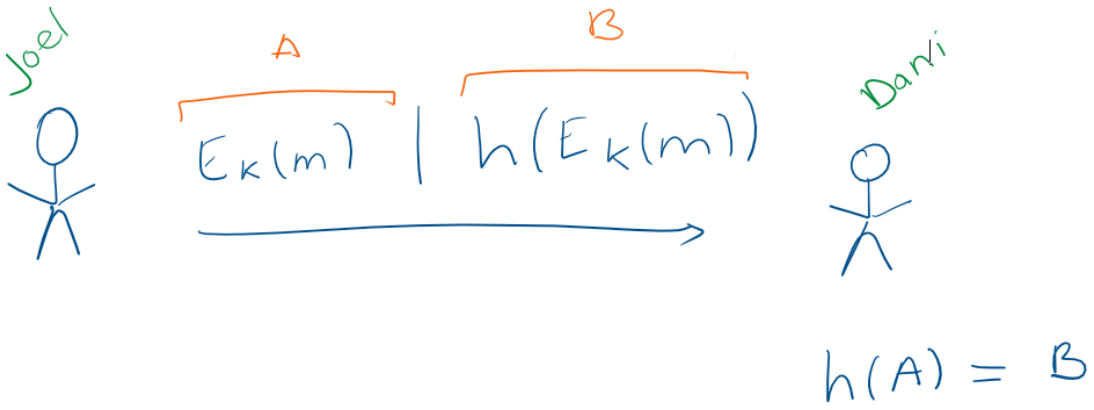
$$p = \frac{1}{62}$$

$$E = -\sum_{i=1}^{10} \frac{1}{62}\left(\log\left(\frac{1}{62}\right)\right) \sim 0.9603$$

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

Exercise 2:

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



Before sending information:

Joel and Dani agree on a shared secret *k*, hash function *h* and encrypting method *E*. *(This step provides authentication through a handshake)*

After that:

a. Joel applies a hash function with both the encrypted message and the secret.
b. Joel sends both the encrypted message (A) and the hashed value of the encrypted message (B).
c. Dani receives both packages of (A) and (B)
d. Dani then applies a hash function to (A) and verifies that H(A) gives the same value as B.

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

- Hash functions generate a fixed-size hash value that uniquely represents the input data.
- Even a small change in the input data results in a significantly different hash value.

- Hash functions are computationally efficient. They can quickly generate hash values for large datasets, making them suitable for real-time data verification and validation tasks.
- By comparing hash values, recipients can verify the authenticity of the data.

3. **Disadvantages and Limitations of Using Hash Functions:**

- Vulnerability to Attacks: Weaker hash functions can be vulnerable to attacks, such as collision attacks, where two different inputs produce the same hash value. It is crucial to use cryptographically secure hash functions to mitigate these vulnerabilities.
- A collision can occur when two different inputs produce the same hash value. Attackers can substitute malicious data for legitimate data without detection, compromising integrity and authentication.
- Preimage Attacks: Given a hash value, find any input that produces that specific hash so attackers can reverse-engineer hashed passwords or other sensitive data.
- By exploiting physical implementation aspects like timing or power consumption attackers can gain information about the hash function.

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

   Password Storage: Instead of storing the actual password in a database, systems store the hash of the password. During login, the system hashes the entered password and compares it to the stored hash. This way, even if the stored hashes are compromised, attackers don't immediately gain access to user passwords.

Exercise 3:

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

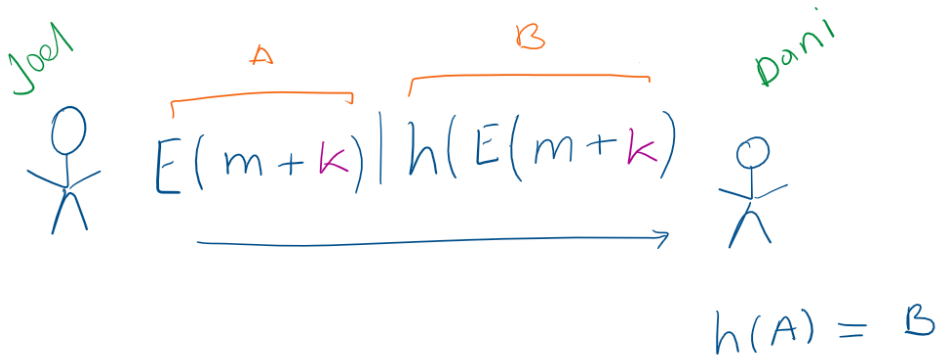
   A Message Authentication Code (MAC) is a cryptographic technique that “allows you to verify that a message was not altered, or a message was not fraudulently introduced onto the system” (IBM, 2014) It is a short piece of information, a tag, that is generated using a secret key and appended to the message.

   It provides:

Integrity: As this tag allows the recipient to verify that the received message has not been altered or tampered with during transmission.

Authenticity: Since both the sender and receiver share a secret cryptographic key used in the MAC calculation, the MAC comparison also ensures the authenticity of the message.

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



Before sending information:

Joel and Dani agree on a shared secret k, hash function h and encrypting method E.

After that:

- Joel applies a hash function with both the encrypted message and the secret.
- Joel sends both the encrypted message (A) and the hashed value of the encrypted message (B).
- Dani receives both packages of (A) and (B)
- Verification: Upon receiving the message and the MAC, the Dani then recalculates the MAC using the received message, the shared secret key, and the same hash function to (A) and verifies that H(A) gives the same value. If the calculated MAC matches the received MAC, the recipient can be confident that the message has not been tampered with and was indeed sent by the legitimate sender.

To note:

Why not send only the encrypted message?

- Because there can be a 3rd person (Sebastian) that can alter both the encrypted message and the hashed value. That way, Dani would not know that the hash and the data have been modified.

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

MACs allow recipients to verify that the received data has not been tampered with during transmission while it authenticates the sender of the message, confirming the identity of the source and preventing impersonation attacks.
The use of a shared secret key in MACs adds another layer of security, as even if the key is compromised, attackers cannot generate valid MACs without it.

Exercise 4:

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

- Compute $n = pq$

$$n = 391$$

- Compute $\lambda(n) = (p - 1) * (q - 1)$

$$\lambda(n) = (17 - 1) * (23 - 1) = 352$$

- Choose public exponent (e) such that $2 < e < \lambda(n)$ and $gcd(e, \lambda(n)) = 1$

$$e = 135$$

- solve for d the equation $de \equiv 1 \ (mod\ \lambda(n))$

$$352 - 135(2) = 82$$
$$135 - 82(1) = 53$$
$$82 - 53(1) = 29$$
$$53 - 29(1) = 24$$
$$29 - 24(1) = 5$$
$$24 - 5(4) = 4$$
$$5 - 4(1) = 1$$
$$4 - 1(4) = 0$$

$$1 = 5 - 4(1)$$
$$1 = 5 - (24 - 5(4))$$
$$1 = -24 + 5(5)$$
$$1 = -24 + 5(29 - 24)$$
$$1 = 145 - 24(6)$$
$$1 = 29(5) - (53 - 29(1))(6)$$
$$1 = -318 + 29(11)$$
$$1 = -53(6) + (82 - 53(1))(11)$$
$$1 = -53(17) + 902$$
$$1 = 82(11) - 53(17)$$
$$1 = 82(11) - (135 - 82(1))(17)$$
$$1 = 82(28) - (2295)$$

$$1 = -(17)(135) + (352 - 135(2))(28)$$
$$1 = -(73)(135) + (352)(28)$$
$$1 = -(73)(135) + (135(2) + 82)(28)$$

$$-73 \,\%\, 352 = 279$$

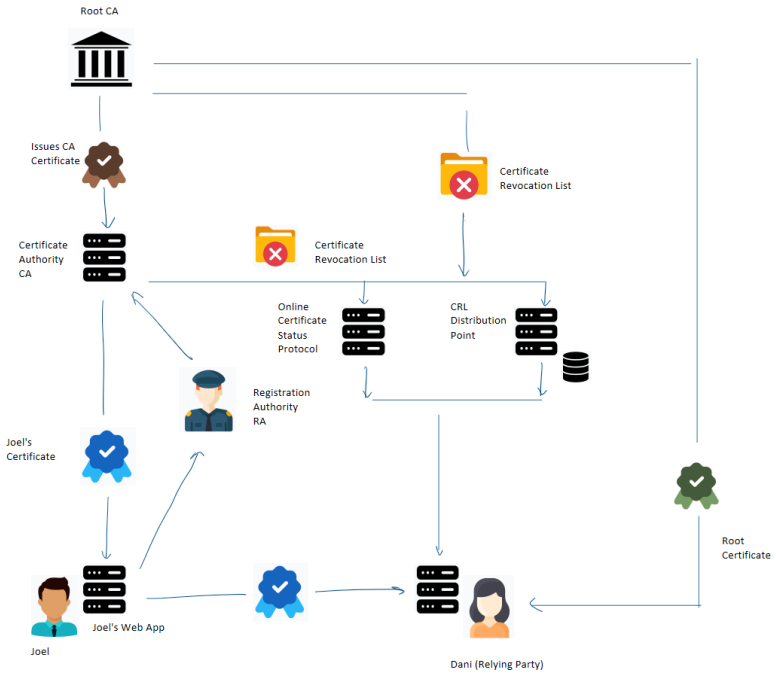
$$public_{key} = (N, e) = (391, 135)$$
$$privatec_{key} = (N, d) = (391, 279)$$

- Choose the private key (i.e., the decryption key) D such that the following equation is true

$$(D\ x\ E)\ mod\ (P - 1)\ x\ (Q - 1) = 1$$
$$(279\ x\ 135)\ mod\ (17 - 1)\ x\ (23 - 1) = 1$$
$$privatec_{key} = (N, d) = (391, 279)$$

Exercise 5:

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



- **Certificate Authority (CA):** The CA is a trusted entity responsible for issuing digital certificates. It verifies the identity of entities (individuals, organizations, servers, etc.)

and signs their public keys to create certificates. They manage Certificate Revocation Lists (CRLs) to revoke compromised or expired certificates.

- **Registration Authority (RA):** The RA acts as the verifier for the CA, validating certificate requests and authenticating users before their certificates are issued. They forward verified requests to the CA for certificate issuance.
- **Certificate Revocation List (CRL) Server:** The CRL server maintains a list of revoked certificates, ensuring users can check the validity of certificates before trusting them. Publish and distribute CRLs containing revoked certificate information. There is the CRL distribution point that acts like a database storage for all the invalid certificates and the Online Certificate Status Protocol that acts like the API for requesting the validity of a specific certificate.
- **Certificate Policy (CP) and Certificate Practice Statement (CPS):** CP and CPS documents outline the policies and procedures followed by the PKI system. CP defines the CA's policies for issuing certificates, while CPS provides detailed procedures on how these policies are implemented. They define rules for identity verification, certificate issuance, revocation, and renewal with security practices, and compliance with industry standards.
- **Relying Parties (Users and Devices):** They are individuals, organizations, servers, and devices that use digital certificates for secure communication, authentication, and data integrity.

Example Scenario: Let’s say Joel wants to secure his website, and Dani wants to connect securely to it.

- Joel obtains a digital certificate for his website from a Certificate Authority (CA) through a Registration Authority (RA) which verifies his identity.
- Dani, as the relying party, relies on the certificate to ensure secure communication with the correct website. Certificates are embedded in software by trusted CAs and can be validated using Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP).
- Also, CA authorities get their certificates from a Root CA which verifies the compliance and security of CA's. This root CA has a Certificate Revocation list with information on the relying CA's certificates.

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

Advantages:

- It ensures confidentiality and integrity of data, making it difficult for unauthorized parties to intercept or modify sensitive information.

- Digital signatures verify that the data has not been altered, assuring that the received data is genuine and unmodified.

- They can scale to support a large number of users, devices, and services.
- PKI enables the revocation of compromised or expired certificates, ensuring that even if a certificate is compromised, it can be invalidated and prevented from further use.

Challenges of Implementing a PKI System:

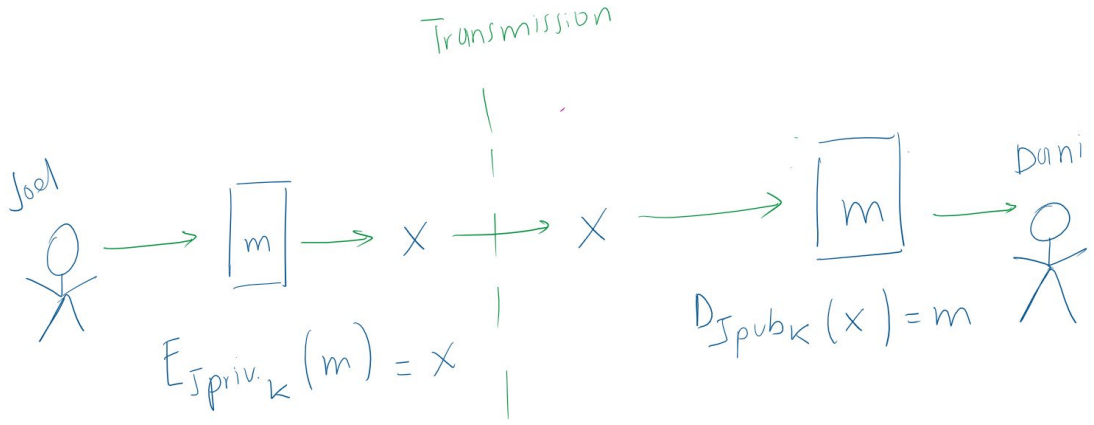
- Implementing a PKI system can be complex, involving various components, protocols, and standards.
- Managing cryptographic keys securely is challenging. Keys must be generated, stored, and distributed securely.
- Establishing trust relationships between different CAs and ensuring interoperability between various systems.
- PKI must comply with local and international laws and regulations.
- Single Point of Failure: The root CA in a PKI system can become a single point of failure. If compromised, it can lead to widespread security issues.

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

When a user visits a website, the web server presents its SSL/TLS certificate to the user's during the initial handshake. The user verifies the certificate's authenticity using the CA's public key, ensuring the website's identity.

Exercise 6:

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



- Joel generates a key pair (public key and private key).

- The public key is shared openly, while the private key is kept secure.

1. Signing Process:
    - Joel encrypts the message with his private key, creating the digital signature.
2. Verification Process:
    - Dani receives the message encrypted with the digital signature.
    - Dani decrypts the digital signature using Joel's public key, obtaining the message.

To note:

This process does not provide security at all because anyone can decrypt the message using Joel's public key. However, by decrypting using Joel's public key, it ensures that it was encrypted with Joel's private key.