Exercises.2\Task1.B

Certificates

1- What are digital certificates used for?

Digital certificates verify the authenticity of websites and encrypt online communication, ensuring that the site you're visiting is secure and trustworthy

2- Why are certificates important for online payments and banking security?

- They establish encrypted, secure connections that protect sensitive information like payment details and personal data from being exposed.

3- What other uses do certificates have?

- Digital certificates are also used to encrypt emails, secure VPN connections, and verify the authenticity of software through code signing.

4- What kind of attacks does TLS mitigate and why is this important for online banking?

- TLS (Transport Layer Security) helps prevent man-in-the-middle attacks by encrypting data, which is crucial for protecting sensitive banking information from being intercepted.

5- How do browsers use certificates for ensuring browsing security?

- Browsers check a website's digital certificate through trusted Certificate Authorities to confirm the site is legitimate and to create a secure connection.

6- What does the warning in the picture above mean?

- The warning indicates a problem with the website's certificate, meaning its identity can't be verified. This could expose users to risks such as data theft.

7- Why would it be bad if a trusted certificate authority was compromised?

- If a CA is compromised, attackers could issue fake certificates, allowing them to impersonate legitimate websites and steal sensitive information.

8- Why is certificate transparency important?

- Certificate transparency enables the tracking and logging of all issued certificates, helping to detect any mis-issued or malicious certificates, which strengthens internet security.

Reference
https://en.wikipedia.org/wiki/Certificate_Transparency