CONNECTION SECURITY AND CRYPTOGRAPHY

By Lassine Pierre Guindo

WHAT IS CRYPTOGRAPHY?

- Cryptography is the practice of securing information by converting it into an unreadable format.
- It ensures confidentiality, integrity, authentication, and non-repudiation of data.
- Used in everyday applications such as secure messaging, online banking, and data protection.
- Example: Encrypted passwords protect accounts from unauthorized access.

WHY IS CRYPTOGRAPHY IMPORTANT?

PREVENTS UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION.

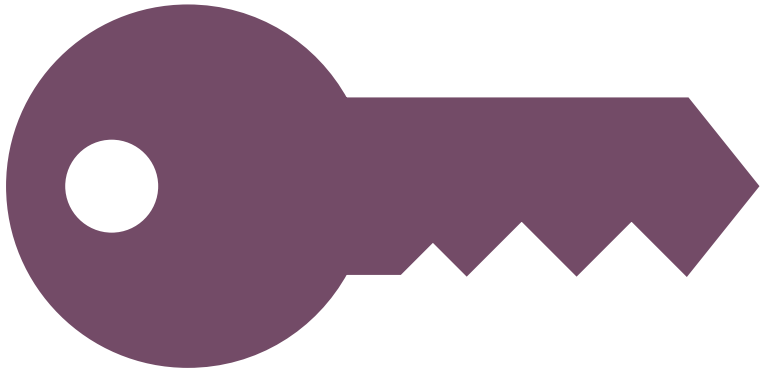
PROTECTS FINANCIAL TRANSACTIONS, ONLINE COMMUNICATION, AND STORED DATA.

ENSURES THAT DATA REMAINS PRIVATE AND UNCHANGED DURING TRANSMISSION.

EXAMPLE: WITHOUT ENCRYPTION, AN ATTACKER INTERCEPTING AN ONLINE PAYMENT COULD SEE CREDIT CARD DETAILS.

SYMMETRIC VS. ASYMMETRIC ENCRYPTION

- Symmetric encryption is efficient but requires both parties to have the same key, making secure key exchange challenging.
- Asymmetric encryption solves this issue by using a public key for encryption and a private key for decryption.
- Example: Websites use asymmetric encryption (TLS) to secure user logins.



THE ROLE OF KEY EXCHANGE AND DIGITAL SIGNATURES

Key Exchange Protocols allow two parties to securely share encryption keys over an unsecured network.

Example: Diffie-Hellman Key Exchange enables devices to establish a shared secret key.

Digital Signatures verify the authenticity and integrity of messages or documents.

Example: Used in secure emails and software updates to ensure the sender is legitimate and the data is not tampered with.

HOW TLS SECURES INTERNET CONNECTIONS

Transport Layer Security (TLS) encrypts data between users and websites.

It works in three steps:

- Handshake: The website and user establish a secure connection using asymmetric encryption.
- Data Encryption: The session switches to symmetric encryption for efficiency.
- Authentication: The website proves its identity using digital certificates.
- Example: When logging into a bank's website, TLS prevents attackers from seeing sensitive information.

CASE STUDY – THE EQUIFAX DATA BREACH (2017)

- **Incident Overview:**
- Equifax, a major credit reporting agency, suffered a data breach exposing **147 million records**.
- Stolen data included names, Social Security numbers, and credit card details.
- **Cause of the Breach:**
- Failure to encrypt stored sensitive data.
- Unpatched security vulnerability in their web application.

LESSONS FROM THE EQUIFAX BREACH

- **Stronger encryption:** All stored sensitive data should be encrypted.
- **Better key management:** Regular updates and secure storage of encryption keys.
- **Multi-Factor Authentication (MFA):** Additional security layers to prevent unauthorized access.
- **Regular security patches:** Ensuring software is up to date to prevent known vulnerabilities.
- **Example:** If Equifax had encrypted customer data properly, even if attackers accessed the files, they would not have been able to read them.

CONCLUSION

- Cryptography is essential for protecting sensitive data online.
- Symmetric encryption is fast but requires secure key exchange.
- Asymmetric encryption is more secure and used in TLS for internet security.
- Strong encryption practices and proper security management can prevent major breaches like Equifax.

REFERENCES & BIBLIOGRAPHY

- Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley.
- Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice.* Pearson.
- Equifax Data Breach Report (2018). *U.S. Government Accountability Office (GAO).*