Introduction to Information Security

Christian J. Rudder

November 2024

Contents

This page is left intentionally blank.

The following five sections are from Concise Work Section Modules [4].

Available at: https://github.com/Concise-Works/sect-modules

— 1 —

Network Security

1.1 Transport Layer Security & Encryption

Before, all communication sent "**over the wire**" (from device to device), was sent "**in the clear**" (unencrypted). This means that anyone could view data sent between devices in plain text. This is a problem when setting up infrastructure such as banking, e-commerce, or any other service that requires sensitive information to be sent over the internet.

Definition 1.1: Integrity & Authenticity

Integrity is the assurance that data has not been altered in transit.
Authenticity is the assurance that the data is coming from the correct source.

Definition 1.2: Transport Layer Security (TLS)

TLS is a protocol providing end-to-end encryption of data. It authenticates the server via **TLS certificates** to ensure the client is connecting to the correct host. It also ensures integrity of the data.

The Engineering Task Force (IETF) published the first version of TLS in 1999. As of today the most recent version is TLS 1.3. (2018). [2]

Definition 1.3: Secure Sockets Layer (SSL) [Deprecated

SSL is the predecessor to TLS. It was developed by Netscape in the 1990s. SSL 3.0 was released in 1996. SSL 3.0 was found to be insecure and was replaced by TLS 1.0 in 1999. [2]

Definition 1.4: Certificate Authority (CA)

A CA is a third-party entity that issues digital certificates. Often called **SSL certificates** or TLS certificates. The protocol supports both SSL and TLS. Despite SSL's deprecation the name stuck due branding issues. Browsers and Operating systems have a list of trusted CAs called the **root store**. A full list of Microsoft's trusted CAs can be found here:
https://ccadb.my.salesforce-sites.com/microsoft/... [3]

Definition 1.5: Encryption

Encryption is the process of converting plaintext into ciphertext (indiscernible text).
Decryption is the process of converting ciphertext back into plaintext.

Definition 1.6: Symmetric & Asymmetric Encryption

Key: is a seed/piece of information used to encrypt or decrypt data.
Symmetric Encryption: uses the same key for both encryption and decryption.
Asymmetric Encryption: uses a public key for encryption and a private key for decryption. [1]

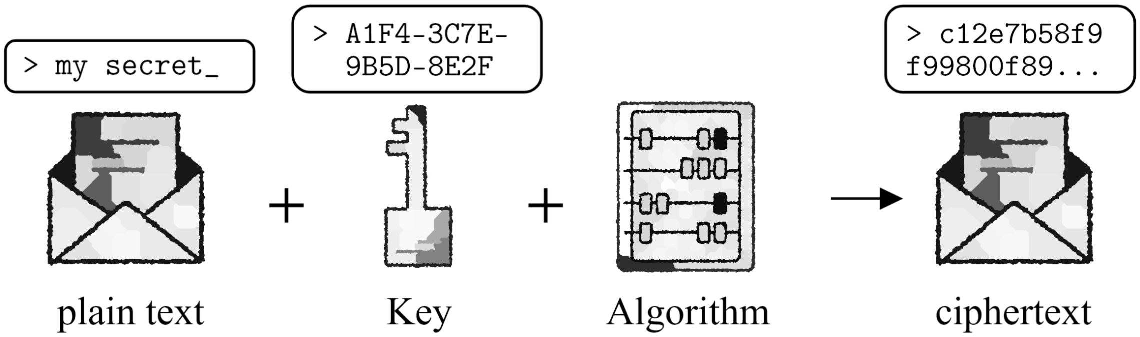


Figure 1.1: High-level depiction of encryption.

Encryption takes a key, data, and an algorithm to produce ciphertext. Decryption takes the same key, ciphertext, and algorithm to produce the original data.

Definition 1.7: Hashing

Hashing is the process of converting data into a fixed-length string of characters. Hashing is a one-way function, meaning it cannot be reversed (theoretically). In practice, it is computationally infeasible to reverse a hash without brute force (trying all possible inputs) or exploiting weaknesses in the hashing algorithm. Some hash algorithms use the text itself as input, while others may incorporate a separate key (e.g., HMAC).

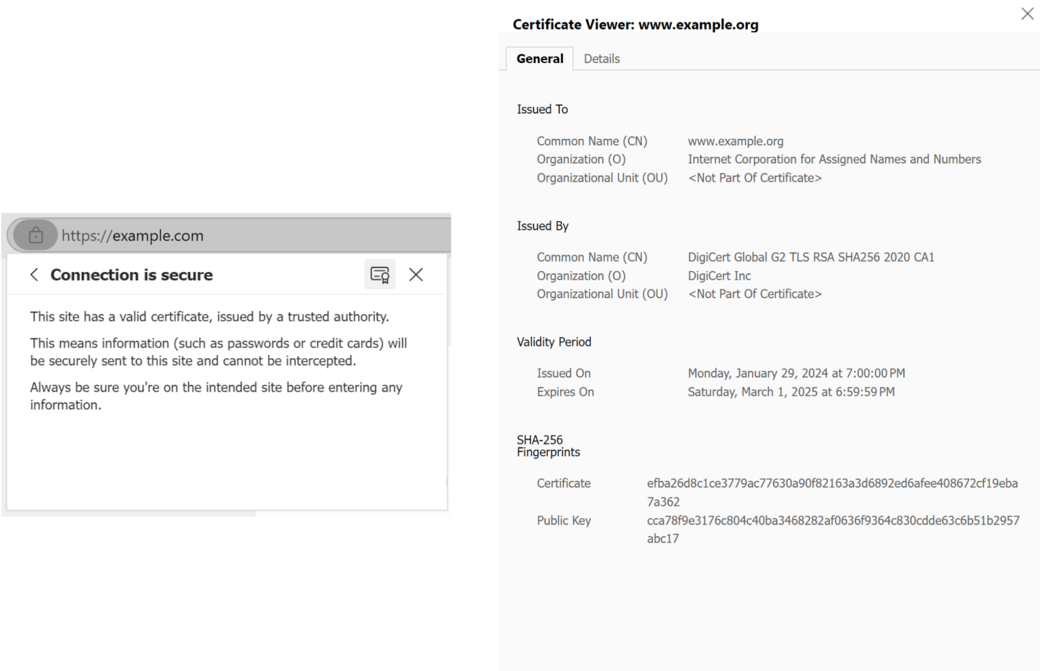
Definition 1.8: Hypertext Transfer Protocol Secure (HTTPS)

A version of HTTP that uses TLS to encrypt data.

Definition 1.9: SSL/TLS Certificate Specifications

- **Common Name (CN)**: The domain name the certificate is issued for.
- **Subject Alternative Name (SAN)**: Additional domain names or subdomains covered by the certificate.
- **Key Length**: A minimum of 2048 bits, ensuring strong encryption.
- **Hashing Algorithm**: Typically SHA-256 for secure data integrity.
- **Valid From/To**: The validity period, usually up to 397 days.
- **Issuer**: The trusted Certificate Authority (CA) that issued the certificate.
- **Extended Key Usage**: Specifies purposes like server authentication or client authentication.

[3]



https://example.com

Connection is secure

This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Certificate Viewer: www.example.org

Issued To

Common Name (CN)	www.example.org
Organization (O)	Internet Corporation for Assigned Names and Numbers
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Organization (O)	DigiCert Inc
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, January 29, 2024 at 7:00:00 PM
Expires On	Saturday, March 1, 2025 at 6:59:59 PM

SHA-256 Fingerprints

Certificate	efba26d8c1ce3779ac77630a90f82163a3d6892ed6afee408672cf19eba7a362
Public Key	cca78f9e3176c804c40ba3468282af0636f9364c830cdde63c6b51b2957abc17

Figure 1.2: SSL certificate obtained through the Edge browser on example.com

Bibliography

[1] Daniel Adetunji. Symmetric and asymmetric key encryption – explained in plain english, April 2023. Accessed: 2024-12-14.

[2] Cloudflare. What is tls (transport layer security)? https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/, n.d. Accessed: 2024-12-14.

[3] Kinsta. Tls vs ssl: What's the difference? which one should you use? https://kinsta.com/knowledgebase/tls-vs-ssl/, 2019. Published December 19, 2019. Updated August 14, 2023. Accessed: 2024-12-14.

[4] Concise Works. Sect modules. https://github.com/Concise-Works/sect-modules, n.d. Accessed November 2024.