TRƯỜNG ĐẠI HỌC HÀNG HẢI VIỆT NAM

KHOA CÔNG NGHỆ THÔNG TIN

A red and blue logo

Description automatically generated

**BÁO CÁO BÀI TẬP LỚN**

***ĐỀ TÀI:***

**Giao thức bảo mật SSL/TLS**

HỌC PHẦN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

NHÓM N07

*Giảng viên hướng dẫn: TS. Nguyễn Hạnh Phúc*

*Sinh viên thực hiện : Bùi Hoàng Long - 99096*

*Hải Phòng, 2024*

Mục lục

[CHƯƠNG 1: Giới thiệu 2](#_Toc182425762)

[1.1 Sự ra đời của SSL 2](#_Toc182425763)

[1.2 SSL và TLS 3](#_Toc182425764)

[CHƯƠNG 2: Kiến trúc 4](#_Toc182425767)

[2.1 Vị trí hoạt động 4](#_Toc182425768)

[2.2 Cấu trúc 6](#_Toc182425769)

[2.3 Record Protocol 7](#_Toc182425770)

[2.4 Handshake Protocol 8](#_Toc182425771)

[2.5 Change Cipher Spec Protocol 9](#_Toc182425772)

[2.6 Alert Protocol 10](#_Toc182425773)

[CHƯƠNG 3: Hoạt động của SSL/TLS 13](#_Toc182425775)

[3.1 Mã hóa đối xứng 13](#_Toc182425776)

[3.2 Mã hóa bất đối xứng 14](#_Toc182425777)

[3.3 Truyền dữ liệu qua SSL/TLS trong thực tế 16](#_Toc182425778)

CHƯƠNG 4: Ứng dụng và kết luận…………………………...18

[4.1](#_Toc182425777) Ứng dụng………………………………………………...18

[4.2](#_Toc182425777) Kết luận……………………………………………….....22

[4.3](#_Toc182425777) Tài liệu tham khảo…………………………………….....23

# Chương 1 : Giới thiệu

## Sự ra đời của SSL

Trong thời kỳ đầu của Internet, việc trao đổi dữ liệu được trao đổi dưới dạng bản rõ, điều này khiến cho các thông tin nhạy cảm có thể bị đánh cắp bởi những kẻ xấu trên đường truyền.

SSL (Secure Sockets Layer) được sinh ra để giải quyết vấn đề này bằng cách cung cấp một kênh truyền đảm bảo các thuộc tính sau:

**Tính xác thực**: Phía máy chủ luôn được xác thực; phía máy khách có thể tùy chọn xác thực.

**Tính bảo mật**: Dữ liệu được gửi sau khi thiết lập kênh chỉ hiển thị với các điểm cuối (endpoint).

**Tính toàn vẹn**: Dữ liệu được gửi sau khi thiết lập kênh nếu bị kẻ tấn công sửa đổi thì sẽ luôn phát hiện được.

Để sử dụng SSL, các website cần có chứng chỉ SSL (hay chứng chỉ TLS) được cấp bởi các cơ quan chứng nhận. Chứng chỉ này hoạt động như một dấu hiệu xác nhận rằng website đó đã được xác thực và được bảo vệ bởi SSL. Việc sử dụng SSL sẽ giúp tăng tính an toàn cho dữ liệu truyền qua mạng, tránh được các mối đe dọa an ninh và bảo vệ thông tin cá nhân của người dùng.

## SSL và TLS

SSL là tiền thân của một giao thức khác là TLS (Transport Layer Security). Việc thay đổi tên gọi chỉ do vấn đề pháp lý nên thuật ngữ "SSL/TLS" vẫn được sử dụng luân phiên để chỉ giao thức này.

Hiện nay đã có những phiên bản SSL/TLS sau đây được phát triển:

SSL 1.0: Không được phát hành.

SSL 2.0: Phát hành năm 1995, ngưng sử dụng.

SSL 3.0: Phát hành năm 1996, ngưng sử dụng.

TLS 1.0: Phát hành năm 1999, ngưng sử dụng.

TLS 1.1: Phát hành năm 2006, ngưng sử dụng.

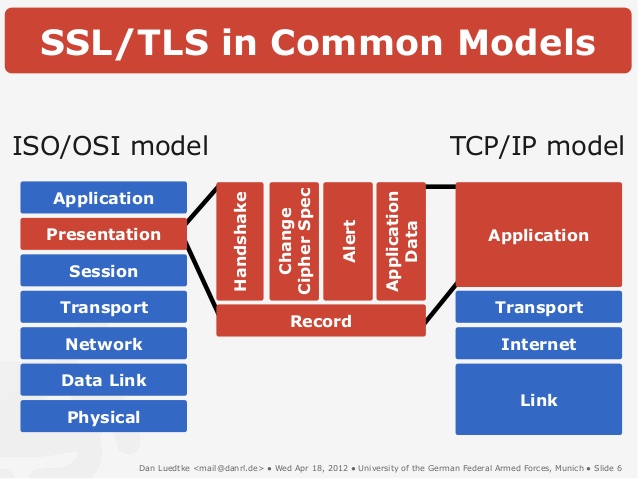
TLS 1.2: Phát hành năm 2008, đang được sử dụng.

TLS 1.3: Phát hành năm 2018, đang được sử dụng.

Các phiên bản của SSL/TLS liên tiếp được cho ra mắt để bắt kịp với sự phát triển của phần cứng, phần mềm cùng các phương thức tấn công. Phiên bản mới nhất TLS 1.3 được ra mắt năm 2018 và đang được sử dụng rộng rãi.

# Chương 2 : Kiến trúc

### Vị trí hoạt động



SSL (Secure Sockets Layer) và TLS (Transport Layer Security) là các giao thức bảo mật quan trọng đảm bảo tính bảo mật, tính toàn vẹn, và khả năng xác thực cho dữ liệu truyền tải qua mạng. Được thiết kế để hoạt động trên các giao thức truyền tải như TCP, SSL/TLS đóng vai trò như một lớp bảo vệ nằm giữa tầng Giao vận (Transport Layer) và tầng Ứng dụng (Application Layer). Điều này khiến việc xác định vị trí chính xác của SSL/TLS trong mô hình OSI hay TCP/IP trở nên khó khăn, vì nó có khả năng "giao thoa" giữa các tầng để đáp ứng mục tiêu bảo mật.

**Vị trí hoạt động trong mô hình OSI và TCP/IP**

SSL/TLS hoạt động ngay trên tầng Giao vận, nơi các giao thức như TCP và UDP quản lý việc truyền tải dữ liệu giữa các thiết bị. Các giao thức này thiết lập và quản lý kết nối truyền tải, cung cấp khả năng tin cậy cho việc gửi và nhận dữ liệu. SSL/TLS, nằm giữa tầng Giao vận và tầng Ứng dụng, mã hóa dữ liệu trước khi nó được gửi qua mạng, đảm bảo rằng dữ liệu không thể bị đọc hoặc sửa đổi trong quá trình truyền.

Trong khi mô hình OSI có cấu trúc gồm 7 tầng và chia các chức năng rõ ràng từ tầng vật lý đến tầng ứng dụng, mô hình TCP/IP chỉ có 4 tầng. Tuy nhiên, trong cả hai mô hình, SSL/TLS không nằm hoàn toàn trong một tầng cụ thể mà có vai trò như một lớp bảo mật bổ sung. Điều này có nghĩa là SSL/TLS không gói gọn vào tầng Giao vận hay tầng Ứng dụng, mà thay vào đó, nó cung cấp cơ chế bảo mật cho các giao thức ở tầng Ứng dụng như HTTP, SMTP, hoặc FTP, thường được sử dụng trong các hoạt động trao đổi thông tin nhạy cảm.

**Cách SSL/TLS cung cấp bảo mật**

Khi một kết nối SSL/TLS được thiết lập, một quá trình bắt tay (handshake) sẽ diễn ra để xác thực danh tính của các bên, trao đổi khóa mã hóa và thỏa thuận thuật toán mã hóa. Sau đó, các dữ liệu truyền tải sẽ được mã hóa để ngăn chặn việc bị đánh cắp hoặc can thiệp bởi những kẻ tấn công trong quá trình truyền. SSL/TLS cũng sử dụng các hàm băm để đảm bảo tính toàn vẹn của dữ liệu, giúp phát hiện mọi thay đổi xảy ra với dữ liệu trong quá trình truyền tải.

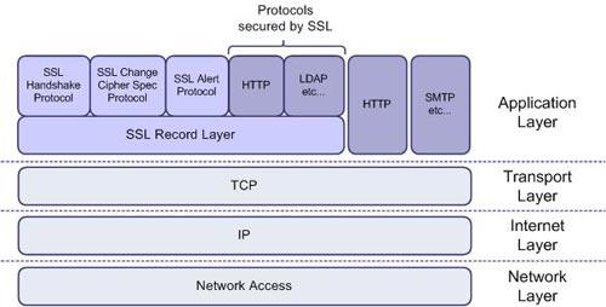
**Ứng dụng thực tiễn của SSL/TLS**

SSL/TLS được áp dụng rộng rãi trên internet, đặc biệt trong các giao dịch ngân hàng, thanh toán trực tuyến, và bảo vệ thông tin người dùng trên các trang web. Giao thức HTTPS (Hypertext Transfer Protocol Secure), một phiên bản bảo mật của HTTP, sử dụng SSL/TLS để mã hóa và bảo vệ dữ liệu người dùng trên các trang web, đảm bảo rằng thông tin nhạy cảm như mật khẩu và thông tin thẻ tín dụng không bị lộ.

**Lợi ích của cách triển khai SSL/TLS**

Sự linh hoạt của SSL/TLS cho phép nó dễ dàng tích hợp vào các tầng trên của mô hình OSI và TCP/IP, giúp bảo mật hầu hết các ứng dụng và giao thức phổ biến trên mạng. Điều này mang lại khả năng bảo mật mạnh mẽ mà vẫn giữ nguyên hiệu quả và hiệu suất của quá trình truyền tải dữ liệu. Nhờ đó, SSL/TLS vẫn là một lựa chọn phổ biến và hiệu quả trong lĩnh vực bảo mật mạng.

### Cấu trúc



SSL/TLS gồm 4 thành phần chính: Record Protocol (Giao thức bản ghi), Handshake Protocol (Giao thức bắt tay), Change Cipher Spec Protocol (Giao thức thay đổi bộ mã hóa), Alert Protocol (Giao thức cảnh báo).

Record Protocol giúp đảm bảo tính toàn vẹn và bảo mật cho dữ liệu bằng cách sử dụng các thuật toán mã hóa đối xứng và bất đối xứng để mã hóa dữ liệu và các hàm băm để đảm bảo tính toán vẹn của dữ liệu.

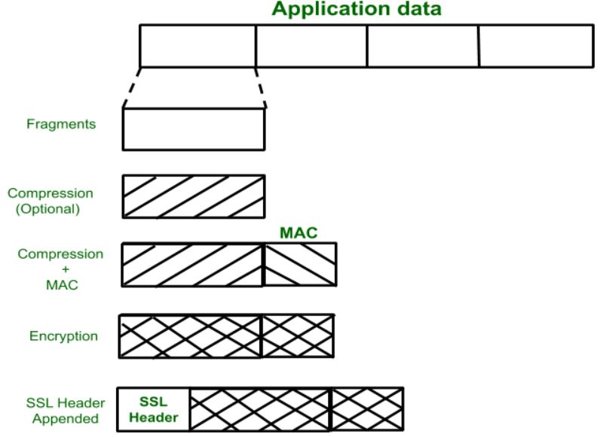
Handshake Protocol dùng để tạo một kênh truyền an toàn cho việc trao đổi thông tin qua các cơ chế xác thực và mã hóa.

Change Cipher Spec Protocol dùng để thông báo với các bên bộ mã hóa sẽ được sử dụng.

Alert Protocol dùng để cảnh báo các bên về các lỗi hoặc các sự cố bảo mật.

Sau đây là chi tiết về từng giao thức và cách chúng vận hành.

### Record Protocol



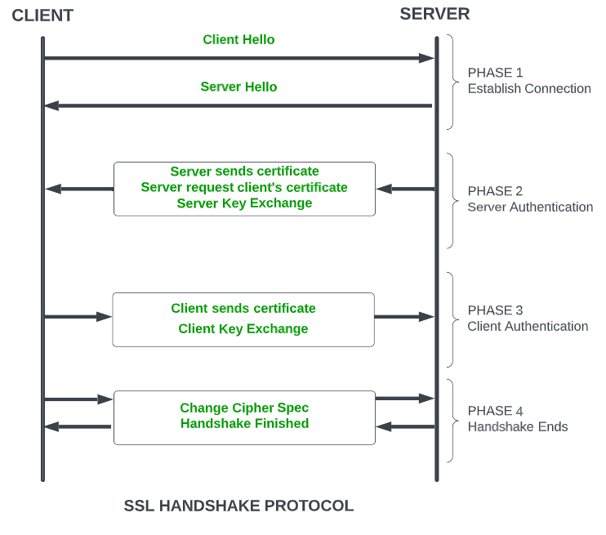
Record Protocol chịu trách nhiệm xác định các định dạng truyền dữ liệu, kiểm soát luồng dữ liệu

Dữ liệu từ tầng ứng dụng sau khi được đưa vào Record Protocol sẽ phải trải qua các bước sau:

* + Dữ liệu được chia thành các mảnh.
  + Các mảnh đó sau đó được nén (nếu cần) và đính kèm với MAC được sinh ra từ các hàm băm.
  + Các mảnh được mã hóa bằng khóa đã được thỏa thuận từ Handshake Protocol
  + Mỗi mảnh được đính thêm header chứa các thông tin tổng quan về mảnh đó.

Ngược lại khi nhận được dữ liệu từ tầng vận chuyển gửi tới Record Protocol sẽ làm ngược lại các bước giải mã, kiểm tra tính toàn vẹn, giải nén và kết hợp lại để tái tạo được dữ liệu ban đầu.

### Handshake Protocol



Handshake Protocol gồm 4 giai đoạn sau:

* Khởi tạo kết nối, trao đổi các gói tin “Hello”: Các gói tin này sẽ giúp client và server trao đổi được các thông tin như phiên bản SSL/TLS, các bộ mã hóa được hỗ trợ, số xác thực phiên của phiên trước (nếu có) và các thông tin phục vụ việc mã hóa.
* Server gửi chứng chỉ của mình cho client xác nhận cùng khóa công khai phục vụ việc mã hóa khóa phiên.
* Sau khi kiểm tra chứng chỉ của server, client tạo ra một khóa phiên và mã hóa nó bằng khóa công khai vừa nhận được. Cuối cùng client gửi khóa phiên đã được mã hóa cùng với chứng chỉ của mình nếu được yêu cầu cho server.
* Sau khi nhận được khóa phiên từ client, server sẽ sử dụng khóa bí mật để giải mã khóa phiên được gửi bởi client, sau đó server gửi thông điệp Change Cipher Spec cho client để thông báo rằng server sẽ bắt đầu sử dụng khóa phiên mới để mã hóa và giải mã các gói tin dữ liệu trong phiên tiếp theo. Sau khi client nhận được thông điệp này, nó cũng sẽ bắt đầu sử dụng khóa phiên mới để mã hóa và giải mã các gói tin dữ liệu.

### Change Cipher Spec Protocol

Change Cipher Spec Protocol là một phần quan trọng trong quá trình thiết lập và duy trì bảo mật cho phiên kết nối giữa hai bên trong giao thức SSL/TLS. Giao thức này được thiết kế để giúp các bên tham gia đồng thuận về bộ mã hóa sẽ sử dụng để bảo vệ các gói tin trong suốt phiên truyền tải, đảm bảo rằng mọi thông tin trao đổi sẽ được mã hóa theo cách đã thống nhất.

**Cách thức hoạt động của Change Cipher Spec Protocol**

Giao thức Change Cipher Spec Protocol gửi một tin nhắn đặc biệt có tên **Change Cipher Spec** mỗi khi có sự thay đổi về bộ mã hóa hoặc khi hai bên đã đồng ý về một bộ mã hóa nhất định. Tin nhắn này có kích thước rất ngắn, chỉ gồm **1 byte** với giá trị là **1**. Dù ngắn gọn, nhưng tin nhắn Change Cipher Spec lại mang ý nghĩa quan trọng trong việc thông báo cho bên còn lại biết rằng mọi gói tin được truyền qua kênh này từ thời điểm này sẽ được mã hóa bằng bộ mã hóa mới.

Quy trình này thường diễn ra như sau:

1. Một trong hai bên tham gia phiên kết nối, chẳng hạn như máy chủ, gửi một tin nhắn Change Cipher Spec tới bên kia, thường là máy khách, để thông báo rằng từ lúc này, bộ mã hóa mới sẽ được áp dụng.
2. **Máy khách nhận** được tin nhắn Change Cipher Spec, tiến hành chuẩn bị để sử dụng bộ mã hóa mới cho các dữ liệu tiếp theo.
3. Sau khi chuẩn bị xong, **máy khách cũng gửi lại** một tin nhắn Change Cipher Spec tương tự về phía máy chủ để xác nhận rằng nó đã nhận được yêu cầu thay đổi bộ mã hóa và cũng đã sẵn sàng áp dụng bộ mã hóa này.
4. Khi cả hai bên đã gửi và nhận tin nhắn Change Cipher Spec của nhau, phiên kết nối sẽ chính thức chuyển sang sử dụng bộ mã hóa mới để bảo vệ tất cả các gói tin trong suốt quá trình truyền tải.

**Ý nghĩa và vai trò của Change Cipher Spec Protocol**

Việc sử dụng Change Cipher Spec Protocol giúp các bên tham gia kết nối biết chính xác thời điểm bắt đầu sử dụng bộ mã hóa mới. Điều này giúp ngăn chặn những sự cố có thể xảy ra nếu một bên không nhận thức được về sự thay đổi trong việc mã hóa dữ liệu. Nhờ giao thức này, kết nối giữa hai bên được đảm bảo tính toàn vẹn và tính bảo mật ở mức độ cao hơn, vì mọi dữ liệu trao đổi sẽ tuân theo một chuẩn mã hóa thống nhất đã được xác thực từ cả hai phía.

**Ứng dụng thực tế**

Giao thức Change Cipher Spec Protocol đóng vai trò quan trọng trong các giao dịch nhạy cảm như thanh toán trực tuyến, giao dịch ngân hàng, hay bảo mật thông tin cá nhân trên các trang web sử dụng HTTPS.

.

### Alert Protocol

Alert Protocol là một thành phần quan trọng trong giao thức SSL/TLS, được thiết kế để gửi thông báo cảnh báo giữa client và server về các sự cố hoặc vấn đề bảo mật trong quá trình kết nối. Nhờ Alert Protocol, các bên tham gia phiên kết nối có thể nhanh chóng nhận diện và xử lý các vấn đề tiềm ẩn, giúp đảm bảo tính bảo mật và độ tin cậy của hệ thống.

**Cấu trúc của một cảnh báo**

Mỗi thông báo cảnh báo do Alert Protocol gửi đi bao gồm **2 byte** với ý nghĩa như sau:

1. **Byte thứ nhất** thể hiện **mức độ nghiêm trọng** của cảnh báo. Có hai mức độ là:
   * **Cảnh báo mức độ cao**: Dành cho các sự cố nghiêm trọng liên quan đến bảo mật như lỗi xác thực, lỗi chứng chỉ, hoặc các nguy cơ tiềm ẩn có thể dẫn đến mất an toàn thông tin.
   * **Cảnh báo mức độ thấp**: Dành cho các tình huống ít nghiêm trọng hơn, như thiếu tài nguyên hoặc các yêu cầu cần kết nối lại nhưng không làm ảnh hưởng trực tiếp đến bảo mật của kết nối.
2. **Byte thứ hai** thể hiện **mô tả chi tiết** của cảnh báo, cung cấp thông tin về loại lỗi hoặc vấn đề cụ thể xảy ra.

**Các loại cảnh báo và mức độ ảnh hưởng**

* **Cảnh báo mức độ cao**: Khi một cảnh báo mức độ cao được gửi đi, nó biểu thị một lỗi nghiêm trọng không thể bỏ qua. Các loại cảnh báo phổ biến ở mức độ này bao gồm:
  + **Lỗi bảo mật**: Khi phát hiện nguy cơ bảo mật, như dấu hiệu của một cuộc tấn công hoặc chứng chỉ không hợp lệ.
  + **Lỗi xác thực**: Khi không thể xác thực được danh tính của một bên trong kết nối, cảnh báo này sẽ được gửi và dẫn đến việc ngắt kết nối ngay lập tức để đảm bảo tính an toàn.

Khi nhận được cảnh báo mức độ cao, client hoặc server sẽ **ngay lập tức ngắt kết nối** nhằm bảo vệ dữ liệu và ngăn chặn các truy cập trái phép tiềm ẩn.

* **Cảnh báo mức độ thấp**: Những cảnh báo ở mức độ thấp thường chỉ ra các vấn đề nhẹ hơn và không yêu cầu ngắt kết nối ngay lập tức. Các tình huống phổ biến bao gồm:
  + **Hết tài nguyên**: Hệ thống có thể gặp vấn đề như bộ nhớ đầy hoặc giới hạn tài nguyên tạm thời.
  + **Yêu cầu kết nối lại**: Nếu một bên yêu cầu kết nối lại để khắc phục lỗi hoặc thay đổi cấu hình, một cảnh báo mức độ thấp sẽ được gửi.

Khi nhận cảnh báo mức độ thấp, kết nối vẫn có thể được duy trì. Tuy nhiên, các bên tham gia có thể phải xử lý các gián đoạn hoặc thực hiện các điều chỉnh để kết nối hoạt động mượt mà hơn.

**Vai trò của Alert Protocol trong bảo mật**

Alert Protocol đóng vai trò quan trọng trong việc giữ an toàn cho kết nối giữa client và server, giúp các bên nhanh chóng nhận diện, xử lý, và phản ứng với các tình huống có thể gây ảnh hưởng đến bảo mật. Việc phân loại rõ ràng giữa cảnh báo mức độ cao và thấp giúp hệ thống dễ dàng đưa ra phản hồi phù hợp, ngăn chặn các sự cố bảo mật kịp thời hoặc giảm thiểu gián đoạn không cần thiết. Alert Protocol là một phần không thể thiếu để đảm bảo tính toàn vẹn và tin cậy của các kết nối an toàn trong môi trường mạng.

# Chương 3 : Hoạt động của SSL/TLS

Hoạt động của SSL/TLS dựa vào hai kỹ thuật mã hóa là: Mã hóa đối xứng và mã hóa đối xứng

### Mã hóa đối xứng

Mã hóa đối xứng là phương pháp mã hóa được sử dụng rộng rãi trong các hệ thống bảo mật nhờ tính đơn giản và tốc độ. Với mã hóa đối xứng, chỉ cần một khóa duy nhất, được gọi là "khóa bí mật," cho cả hai quá trình mã hóa và giải mã. Điều này khác với mã hóa bất đối xứng, trong đó có hai khóa riêng biệt (khóa công khai và khóa bí mật).

**1.1. Nguyên lý hoạt động của mã hóa đối xứng**

Quá trình mã hóa đối xứng bắt đầu khi một thông điệp ban đầu (plaintext) được mã hóa bằng khóa bí mật để tạo ra dữ liệu đã mã hóa (ciphertext). Ciphertext này gần như không thể đọc hiểu nếu không có khóa giải mã. Để khôi phục thông tin ban đầu, người nhận chỉ cần sử dụng cùng một khóa bí mật để giải mã ciphertext về lại dạng plaintext.

**1.2. Ưu và nhược điểm của mã hóa đối xứng**

Một ưu điểm lớn của mã hóa đối xứng là tốc độ: do chỉ sử dụng một khóa và các phép toán đơn giản, mã hóa đối xứng có tốc độ xử lý cao, thích hợp cho các ứng dụng yêu cầu truyền tải dữ liệu nhanh và có lưu lượng lớn. Tuy nhiên, nhược điểm là việc bảo mật khóa bí mật trở nên quan trọng và phức tạp. Khi nhiều người dùng cần truy cập, việc chia sẻ và quản lý khóa một cách an toàn là một thách thức.

**1.3. Các thuật toán phổ biến**

Một số thuật toán mã hóa đối xứng nổi tiếng bao gồm:

* **DES (Data Encryption Standard)**: Đây là một trong những thuật toán mã hóa đối xứng đầu tiên được sử dụng rộng rãi, dù hiện nay đã không còn an toàn do độ dài khóa ngắn.
* **AES (Advanced Encryption Standard)**: Là chuẩn mã hóa hiện đại thay thế DES, với khả năng bảo mật cao hơn và các kích thước khóa linh hoạt (128, 192 hoặc 256 bit).
* **Blowfish và Twofish**: Các thuật toán mã hóa nhanh và được sử dụng rộng rãi trong các ứng dụng yêu cầu hiệu suất cao.

**1.4. Ứng dụng của mã hóa đối xứng**

Mã hóa đối xứng thường được sử dụng trong các giao thức bảo mật mạng như SSL/TLS để bảo vệ thông tin trong quá trình truyền tải trên internet, các ứng dụng bảo mật file và ổ đĩa, và trong một số hệ thống ngân hàng điện tử để bảo vệ dữ liệu giao dịch.

### Mã hóa bất đối xứng

Mã hóa bất đối xứng (asymmetric encryption) là một phương pháp mã hóa hiện đại và phức tạp, thường được ứng dụng rộng rãi trong các hệ thống bảo mật nhờ vào tính an toàn cao và khả năng ngăn chặn việc xâm nhập không mong muốn. Kỹ thuật này sử dụng một cặp khóa bao gồm hai khóa khác nhau: **khóa công khai** (public key) và **khóa bí mật** (private key). Khóa công khai có thể được chia sẻ công khai và bất kỳ ai cũng có thể truy cập. Ngược lại, khóa bí mật phải được giữ kín và chỉ chủ sở hữu mới có quyền tiếp cận. Nhờ đó, ngay cả khi khóa công khai bị người khác biết, chỉ có người giữ khóa bí mật mới có thể giải mã dữ liệu.

**Nguyên lý hoạt động của mã hóa bất đối xứng**

Trong mã hóa bất đối xứng, quá trình mã hóa và giải mã dữ liệu được thực hiện bằng cách sử dụng cặp khóa công khai và khóa bí mật. Cụ thể:

* Khi một đối tượng muốn gửi tin nhắn được mã hóa cho đối tượng khác, người gửi sẽ sử dụng **khóa công khai** của người nhận để mã hóa tin nhắn.
* Tin nhắn đã mã hóa (ciphertext) sau đó được gửi đi và chỉ có người nhận - người sở hữu **khóa bí mật** tương ứng - mới có thể giải mã và đọc được nội dung tin nhắn.

Điều này mang lại một lợi ích lớn về bảo mật, vì không cần phải chia sẻ khóa bí mật qua mạng. Dù khóa công khai có thể bị lộ ra, dữ liệu vẫn an toàn bởi vì chỉ có khóa bí mật mới có thể giải mã được dữ liệu đã mã hóa bằng khóa công khai.

**Ứng dụng thực tế của mã hóa bất đối xứng**

Mã hóa bất đối xứng là nền tảng của nhiều hệ thống bảo mật trong thực tế. Nó được sử dụng trong:

* **Chữ ký số**: Một tài liệu hoặc thông điệp có thể được ký bởi khóa bí mật của người gửi để xác nhận danh tính và tính toàn vẹn của nội dung. Người nhận sau đó có thể sử dụng khóa công khai của người gửi để xác thực chữ ký.
* **Giao dịch trực tuyến và chứng chỉ SSL/TLS**: Các trình duyệt web sử dụng mã hóa bất đối xứng trong giao thức SSL/TLS để bảo vệ kết nối giữa người dùng và máy chủ, đảm bảo rằng thông tin không thể bị xâm nhập hoặc thay đổi bởi các bên thứ ba.
* **Mạng riêng ảo (VPN)** và các ứng dụng yêu cầu kết nối an toàn.

**Lợi ích và hạn chế của mã hóa bất đối xứng**

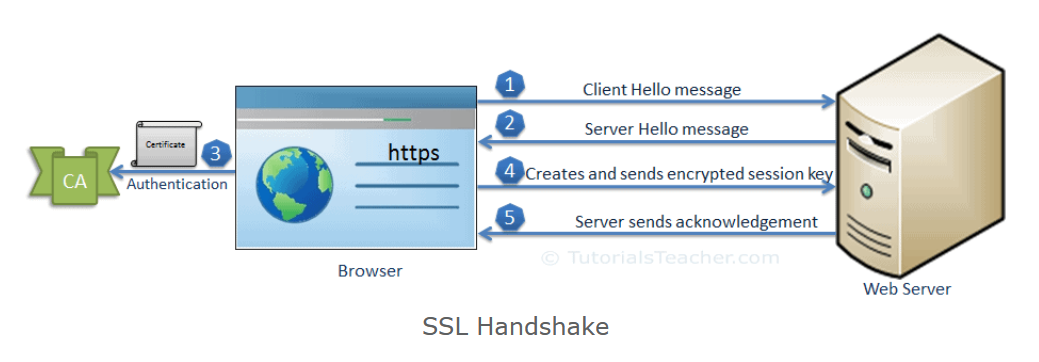
Mã hóa bất đối xứng mang lại khả năng bảo mật cao nhờ không cần chia sẻ khóa bí mật qua mạng. Tuy nhiên, nó đòi hỏi hiệu suất tính toán lớn hơn nhiều so với mã hóa đối xứng, dẫn đến thời gian xử lý chậm hơn. Vì vậy, mã hóa bất đối xứng thường được kết hợp với mã hóa đối xứng để đảm bảo tính bảo mật và hiệu quả cho các hệ thống hiện đại.

### Truyền dữ liệu qua SSL/TLS trong thực tế

Ảnh có chứa văn bản

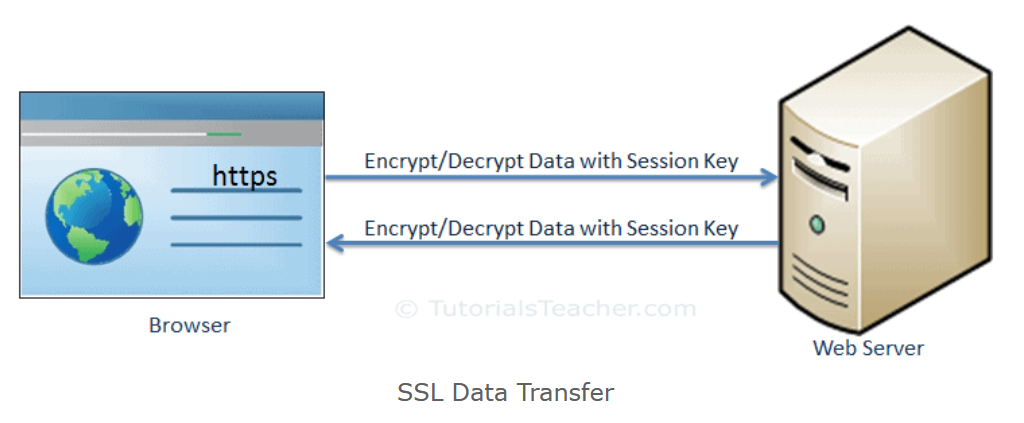
Mô tả được tạo tự động Giao tiếp SSL giữa trình duyệt và Server (hoặc bất kỳ hai hệ thống nào khác) được chia thành giai đoạn chính:

* Bắt tay SSL (SSL Handshake)
* Truyền dữ liệu thực tế (Data Transfer)



**SSL Handshake:**

* Ở giai đoạn này Handshake Protocol được thực thi, kỹ thuật mã hóa bất đối xứng sẽ được áp dụng cho việc trao đổi khóa phiên giữa Client và Server.
* Server sẽ tạo ra khóa công khai và khóa bí mật, khóa công khai sẽ được gửi đến client, client sẽ dùng khóa công khai đấy để mã hóa khóa phiên nó vừa tạo rồi gửi lại Server, Server dùng khóa bí mật để giải mã khóa phiên.



**Data Transfer:**

Ở giai đoạn này, kỹ thuật mã hóa đối xứng (symmetric encryption) được áp dụng để bảo vệ sự an toàn của dữ liệu trong quá trình truyền tải giữa Client và Server. Trong mô hình mã hóa đối xứng, cả hai bên đều sử dụng chung một khóa phiên (session key), khóa này đã được tạo ra trong giai đoạn trước của quá trình giao tiếp. Khóa phiên này đóng vai trò quan trọng trong việc mã hóa dữ liệu trước khi gửi đi từ Client và giải mã khi dữ liệu đến Server, cũng như ngược lại.

Điều này có nghĩa là mỗi khi có dữ liệu cần trao đổi giữa Client và Server, dữ liệu sẽ được mã hóa bằng khóa phiên duy nhất, giúp bảo vệ tính toàn vẹn và sự bảo mật của thông tin trong suốt quá trình truyền tải. Vì cả hai bên (Client và Server) đều biết và sử dụng chung một khóa phiên, quá trình mã hóa và giải mã diễn ra nhanh chóng và hiệu quả. Tuy nhiên, sự an toàn của hệ thống phụ thuộc vào việc bảo vệ khóa phiên này khỏi các mối đe dọa tiềm ẩn từ bên ngoài. Nếu khóa phiên bị lộ ra, các dữ liệu trao đổi sẽ có nguy cơ bị xâm phạm, làm mất tính bảo mật của hệ thống.

Thông qua việc sử dụng kỹ thuật mã hóa đối xứng, dữ liệu truyền tải không chỉ được bảo vệ khỏi các cuộc tấn công nghe lén mà còn giúp đảm bảo rằng chỉ có những bên có quyền truy cập hợp pháp mới có thể đọc và hiểu được thông tin trao đổi.

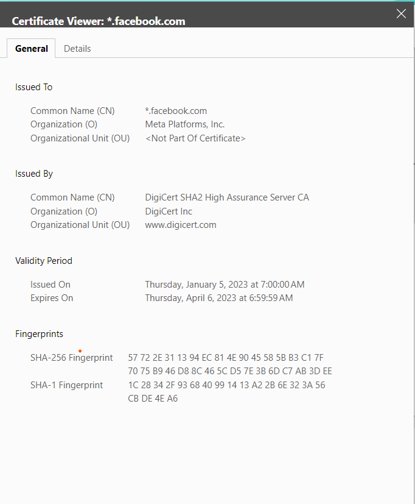
# Chương 4 : Ứng dụng và Kết Luận

SSL/TLS được sử dụng rộng rãi trong các ứng dụng truyền thông trên Internet như web, email, chat và file transfer. Cụ thể, SSL/TLS được sử dụng trong các ứng dụng sau:

* HTTPS (Hypertext Transfer Protocol Secure) cho truyền thông trên web
* SMTPS (Simple Mail Transfer Protocol Secure) và POP3S/IMAPS (Secure Post Office Protocol/Internet Mail Access Protocol) cho truyền thông trên email
* FTPS (File Transfer Protocol Secure) cho truyền thông trên file transfer.
* VPN (Virtual Private Network) cho truyền thông trên mạng riêng ảo.

Tuy nhiên ứng dụng nổi bật nhất của SSL/TLS chính là HTTPS. Khi chúng ta duyệt web, nếu để ý thì có thể thấy trong đường dẫn của nhiều website có biểu tượng khóa và trong URL của website đó bắt đầu bằng “https” (HTTP Secure). Đó là dấu hiệu cho việc Website đó đã được cấp một chứng chỉ SSL/TLS.

Chứng chỉ SSL/TLS là một chứng chỉ kỹ thuật số dùng để bảo mật và xác minh danh tính của trang web hoặc dịch vụ trực tuyến. Chứng chỉ được cấp bởi một bên thứ 3 đáng tin cậy có tên là “Tổ chức phát hành chứng chỉ”. Tổ chức này sẽ xác minh danh tính của trang web hoặc dịch vụ trước khi cấp chứng chỉ.

 Ở đây ta có thể thấy trang facebook.com được cấp chứng chỉ SSL/TLS từ tổ chức DigiCert.

Một trang Web có chứng chỉ SSL/TLS sẽ đảm bảo các đặc điểm sau:

* **Encryption**: Chứng chỉ SSL/TLS sử dụng thuật toán mã hóa để bảo mật thông tin liên lạc giữa trang web hoặc dịch vụ và người dùng. Điều này đảm bảo rằng thông tin nhạy cảm, chẳng hạn như thông tin đăng nhập và thông tin thẻ tín dụng, được bảo vệ khỏi bị chặn và đọc bởi các bên trái phép.
* **Authentication**: Chứng chỉ SSL/TLS xác minh danh tính của trang web hoặc dịch vụ, đảm bảo rằng người dùng đang giao tiếp với bên dự định chứ không phải với kẻ mạo danh. Điều này cung cấp sự đảm bảo cho người dùng rằng thông tin của họ đang được truyền đến một thực thể đáng tin cậy.
* **Integrity**: Chứng chỉ SSL/TLS sử dụng mã xác thực thông báo (MAC) để phát hiện bất kỳ hành vi giả mạo dữ liệu nào trong quá trình truyền. Điều này đảm bảo rằng dữ liệu được truyền đi không bị sửa đổi theo bất kỳ cách nào, bảo toàn tính toàn vẹn của nó.
* **Non-repudiation**: Chứng chỉ SSL/TLS cung cấp tính năng không từ chối dữ liệu, nghĩa là người nhận dữ liệu không thể phủ nhận việc đã nhận được dữ liệu đó. Điều này rất quan trọng trong các tình huống cần thiết lập tính xác thực của thông tin, chẳng hạn như trong các giao dịch thương mại điện tử.
* **Public-key Cryptography**: Chứng chỉ SSL/TLS sử dụng mật mã khóa công khai để trao đổi khóa an toàn giữa máy khách và máy chủ. Điều này cho phép máy khách và máy chủ trao đổi khóa mã hóa một cách an toàn, đảm bảo rằng thông tin được mã hóa chỉ có thể được giải mã bởi người nhận dự định.
* **Session Management**: Chứng chỉ SSL/TLS cho phép quản lý các phiên bảo mật, cho phép nối lại các phiên bảo mật sau khi bị gián đoạn. Điều này giúp giảm chi phí thiết lập kết nối an toàn mới mỗi khi người dùng truy cập trang web hoặc dịch vụ.
* **Chứng chỉ do các CA đáng tin cậy cấp**: Chứng chỉ SSL/TLS được cấp bởi các CA đáng tin cậy, những người chịu trách nhiệm xác minh danh tính của trang web hoặc dịch vụ trước khi cấp chứng chỉ. Điều này mang lại mức độ tin cậy và đảm bảo cao cho người dùng rằng trang web hoặc dịch vụ mà họ đang liên lạc là xác thực và đáng tin cậy.

Ngoài các đặc điểm chính này, chứng chỉ SSL/TLS còn có nhiều cấp độ xác thực khác nhau, bao gồm Xác thực tên miền (DV), Xác thực tổ chức (OV) và Xác thực mở rộng (EV). Mức độ xác thực xác định lượng thông tin được CA xác minh trước khi cấp chứng chỉ, với chứng chỉ EV cung cấp mức độ đảm bảo và tin cậy cao nhất cho người dùng.

# 

# Kết luận

Nhìn chung, SSL/TLS là một thành phần quan trọng của bảo mật trực tuyến, cung cấp khả năng mã hóa, xác thực, tính toàn vẹn, chống thoái thác và các tính năng chính khác nhằm đảm bảo việc truyền thông tin nhạy cảm an toàn và đáng tin cậy qua internet.

Tuy nhiên, SSL/TLS vẫn không hoàn hảo và có thể bị tấn công bởi một số kỹ thuật như khai thác lỗ hổng của các phiên bản cũ, tấn công giả mạo chứng chỉ, và tấn công kết nối giữa máy khách và máy chủ. Do đó, việc ứng dụng SSL/TLS đòi hỏi sự cẩn trọng và các biện pháp bảo mật phù hợp.

Tóm lại, SSL/TLS là một công nghệ quan trọng để bảo vệ thông tin truyền tải trên internet. Tuy nhiên, để đảm bảo tính bảo mật, các tổ chức cần triển khai các biện pháp bảo mật đầy đủ và cập nhật SSL/TLS lên các phiên bản mới nhất và phù hợp.

**Tài liệu tham khảo**

1. [RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 (rfc-editor.org)](https://www.rfc-editor.org/rfc/rfc8446)
2. [Secure Socket Layer (SSL) - GeeksforGeeks](https://www.geeksforgeeks.org/secure-socket-layer-ssl/)
3. Giáo trình AT&BM – HTTT PTIT