TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA HỆ THỐNG THÔNG TIN

SEMINAR

AN TOÀN VÀ BẢO MẬT TRONG THƯƠNG MẠI ĐIỆN TỬ

Safety and Security in e-commerce

NHÓM 4 – LỚP IS334.P11

NHÓM 4

DANH SÁCH THÀNH VIÊN

22521303 - Nguyễn Đức Tấn

22520889 - Trần Giáp Minh

22520721 - Nguyễn Trí Tuấn Kiệt

22520097 - Đặng Quốc Bảo

24520003 - Trần Quốc Danh

19522192 - Nguyễn Thừa An Thái

NỘI DUNG THUYẾT TRÌNH

NGHIÊN CỨU VỀ AN TOÀN VÀ BẢO MẬT TRONG TMĐT

01

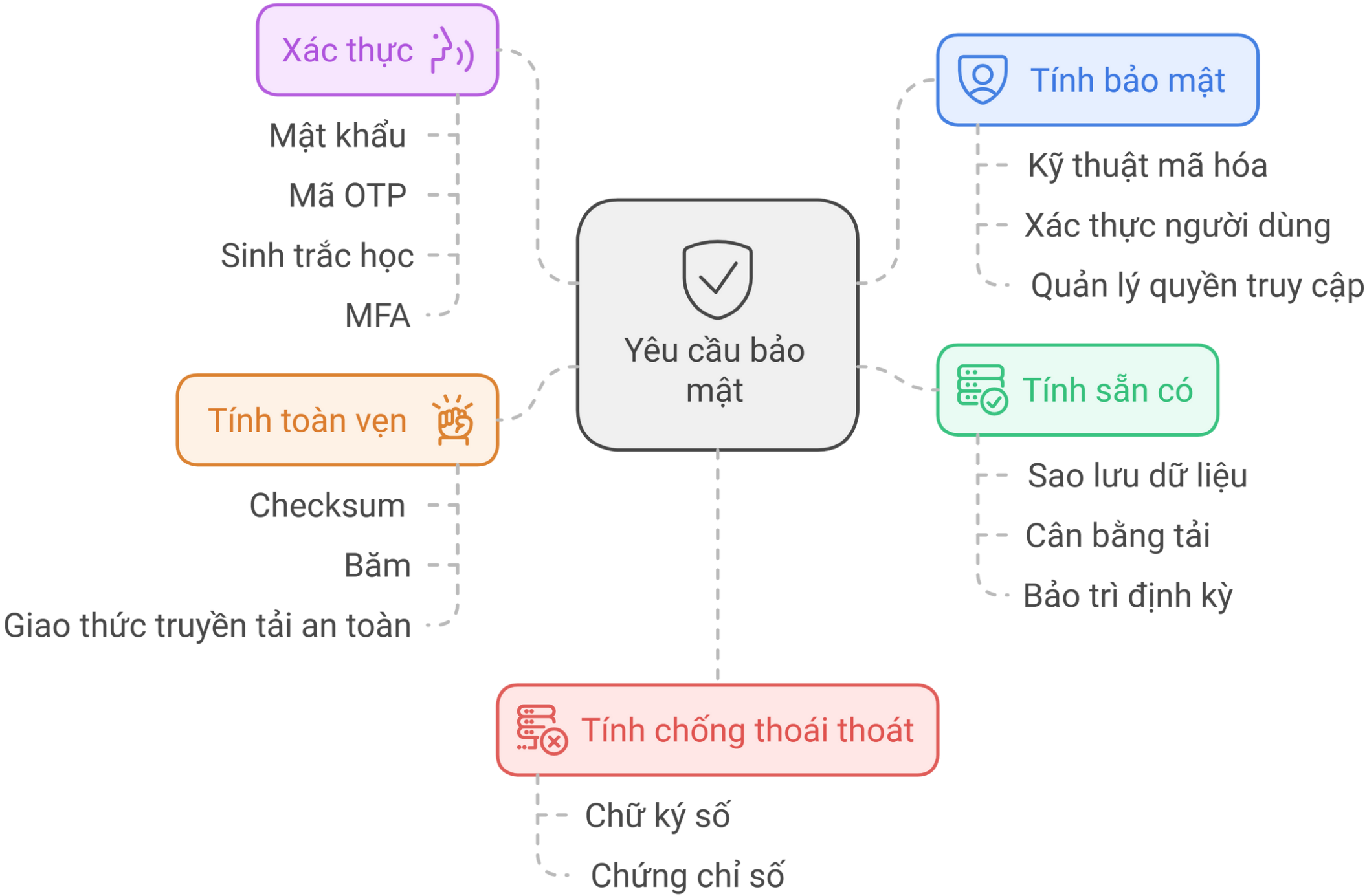
CÁC HÌNH THỨC TẤN CÔNG TRANG WEB TMĐT

02

BẢO MẬT THANH TOÁN DI ĐỘNG, CÁC MỐI ĐE DỌA VÀ THÁCH THỨC

03

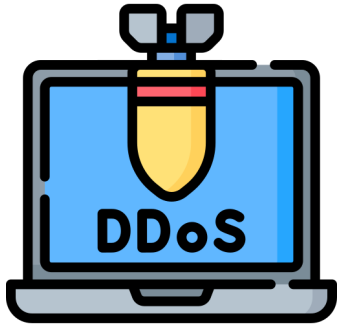
CÁC HÌNH THỨC BẢO MẬT VÀ AN TOÀN THÔNG TIN


Yêu cầu bảo mật
Xác thực
Mật khẩu
Mã OTP
Sinh trắc học
MFA
Tính bảo mật
Kỹ thuật mã hóa
Xác thực người dùng
Quản lý quyền truy cập
Tính toàn vẹn
Checksum
Băm
Giao thức truyền tải an toàn
Tính sẵn có
Sao lưu dữ liệu
Cân bằng tải
Bảo trì định kỳ
Tính chống thoái thoát
Chữ ký số
Chứng chỉ số

01

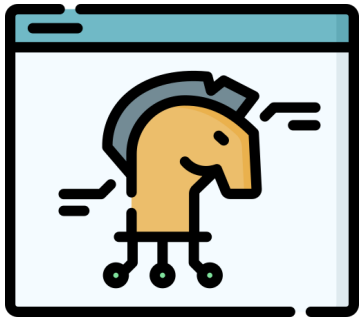
CÁC HÌNH THỨC TẤN CÔNG TRANG WEB TMĐT

Forms of attack on e-commerce websites



DDoS

"Distributed Denial of Service"



Trojan Horse

“Truyền thuyết con ngựa gỗ thành Troy”

Attack

Phishing

“Fishing” + “Phreaking”

SQL Injection

“Cấy ghép SQL, SQLi”

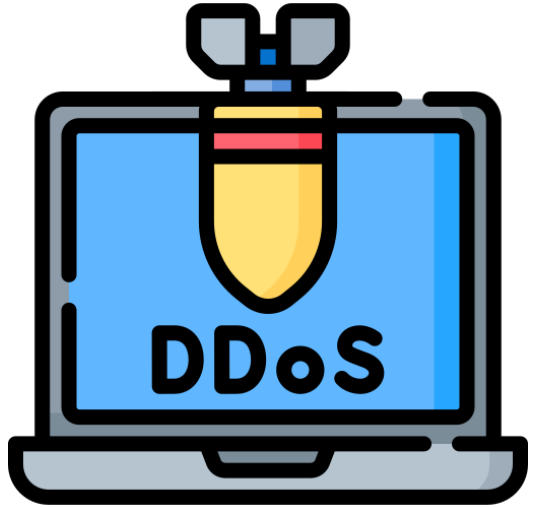
DISTRIBUTED DENIAL OF SERVICE

DDoS

Tấn công bởi lưu lượng truy cập đến từ rất nhiều hệ thống khác nhau thông qua nhiều địa chỉ IP khác nhau.

Làm hệ thống quá tải, gián đoạn dịch vụ hoàn toàn, mất rất nhiều thời gian để khôi phục.

=> Làm tiền đề cho những cuộc tấn công tiếp theo do server suy yếu, trì trệ.



Vào tháng 2/2020, dịch vụ AWS Shield của Amazon đã bị tấn công DDos, lưu lượng truy cập lên đến 2,3 Tbps(Terabits per second), đây là cuộc tấn công DDos lớn nhất được ghi nhận vào năm 2020

PHISHING

“Fishing” + “Phreaking”

Thực chất là tấn công giả mạo thông qua việc đính link giả và yêu cầu đăng nhập.

Kẻ tấn công giả mạo thành một đơn vị uy tín để lừa người dùng nhập thông tin đăng nhập qua các đường link giả được họ lập trình sẵn đính kèm trong email/tin nhắn

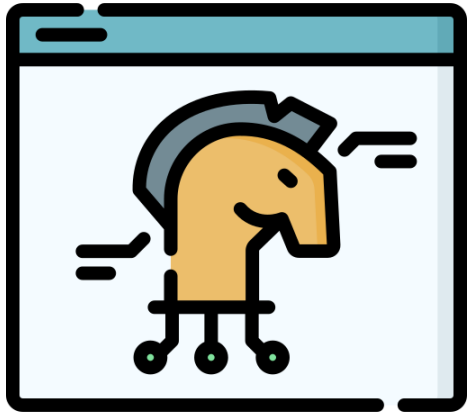
Nếu “mắc câu”, tin tặc sẽ có được thông tin ngay tức khắc.

Ví dụ: Đối tượng giả dạng nhân viên Shopee để thông báo chương trình trúng thưởng. Khách hàng không cần thanh toán khoản phí nào nhưng phải liên hệ với 1 tài khoản Telegram/Zalo để cung cấp và xác minh thông tin (thường là họ tên, ngày sinh, cccd,...).

TROJAN HORSE

“Truyền thuyết con ngựa gỗ thành Troy”

Là một phần mềm giả dạng thành một chương trình hợp pháp hoặc hữu ích, nhưng thực chất lại có mục đích phá hoại, ăn cắp dữ liệu hoặc kiểm soát hệ thống từ xa.



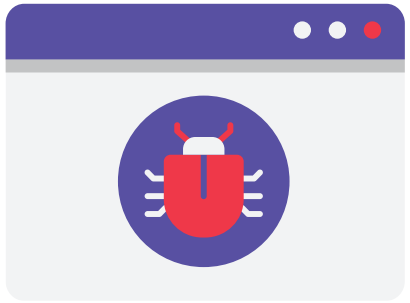
Nếu thiếu kiến thức về internet, cả admin và user trang web TMĐT đều có thể trở thành nạn nhân của Trojan Horse. Khi đó, hacker có toàn quyền điều khiển máy tính, dữ liệu của nạn nhân để thực hiện các hành vi nguy hại cho website thương mại điện tử.

Ví dụ: Năm 2014, eBay đã lên tiếng thúc giục người dùng đổi mật khẩu sớm nhất có thể sau khi bị hacker xâm nhập vào cơ sở dữ liệu trọng yếu.

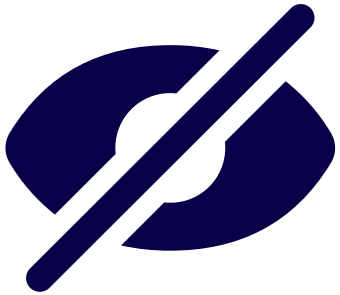
TROJAN HORSE

CÁCH THỨC HOẠT ĐỘNG

GIẢ MẠO



KÍCH HOẠT



ẨN GIẤU

Trojan có thể nhắm đến khách hàng lẫn hệ thống quản lý TMĐT

TROJAN HORSE

KỊCH BẢN TẤN CÔNG

Khách hàng TMĐT

Phát tán Trojan qua email Phishing

Gửi email giả mạo

Yêu cầu tải xuống các phần mềm giả mạo

Kích hoạt Trojan qua thiết bị người dùng

Hoạt động ngầm

Kích hoạt **keylogger***

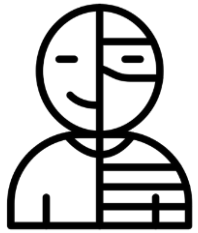
Chiếm tài khoản TMĐT

***Keylogger* :** *ứng dụng ghi lại các lần nhấn phím khi người dùng đăng nhập vào tài khoản TMĐT.*

TROJAN HORSE

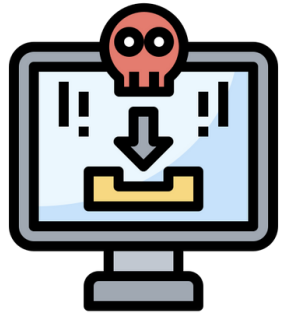
KỊCH BẢN TẤN CÔNG

Hệ thống TMĐT



Lừa nhân viên của sàn TMĐT tải Trojan

Gửi email giả mạo dưới danh nghĩa đối tác, nhà cung cấp hoặc khách hàng lớn



Nhân viên tải về phần mềm độc hại

Trojan này có thể tạo ra một **backdoor*** để hacker truy cập vào hệ thống mạng nội bộ của sàn TMĐT.

Xâm nhập và kiểm soát dữ liệu

Đánh cắp thông tin

Gián đoạn dịch vụ

Yêu cầu tiền chuộc

Tạo đơn hàng gian lận

Backdoor* *: một cách thức cho phép tin tặc luồng vào hệ thống mà không cần qua hệ thống an ninh như tường lửa.*

SQL Injection

SQLi

Là một cách thức vận dụng lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện đối với cơ sở dữ liệu của nó, cho phép kẻ tấn công xem được dữ liệu mà thông thường họ không thể truy xuất.

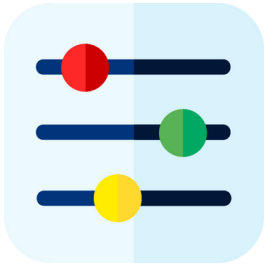
Trong nhiều trường hợp, kẻ tấn công có thể sửa đổi hoặc xóa dữ liệu này, gây ra những thay đổi lâu dài đối với nội dung hoặc hành vi của ứng dụng.

SQL Injection

SQLi

FORM

Do không thực hiện kiểm tra hoặc loại bỏ các ký tự đặc biệt như ' , - , hoặc ;



FILTER

Nếu các tham số lọc không kiểm tra bảo mật, kẻ tấn công có thể khai thác SQLi.

SEARCH

Hacker có thể nhập các đoạn mã SQL độc hại, cho phép kẻ tấn công khai thác.

URL THAM SỐ

Nếu tham số không được kiểm tra, hacker có thể thay giá trị tham số bằng một đoạn mã độc

SQL Injection thường cho phép hacker truy cập thông tin nhạy cảm như danh sách khách hàng, thông tin đơn hàng, hay thậm chí quyền quản trị trang web.

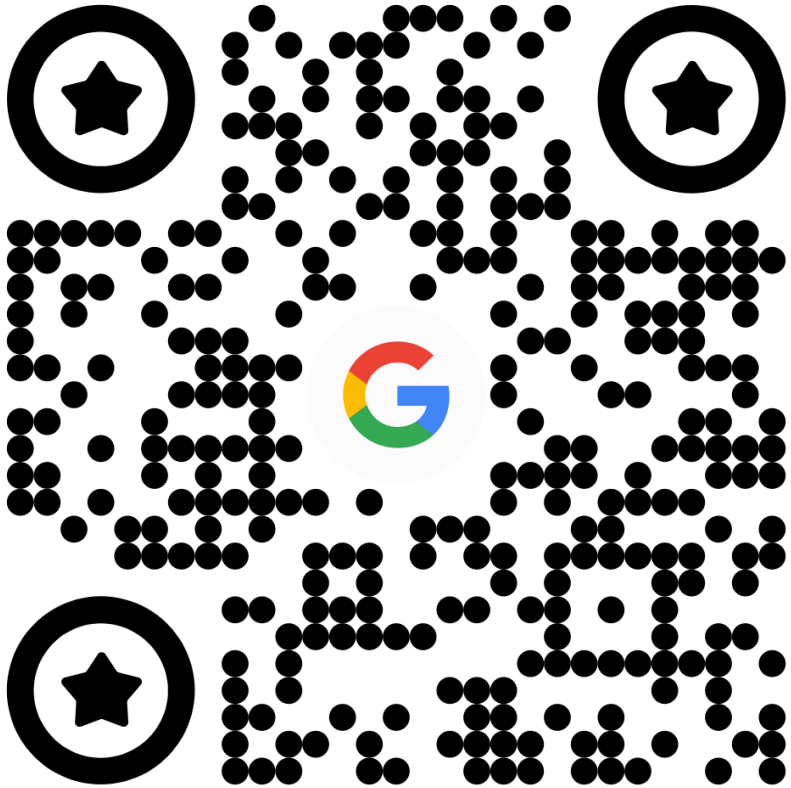
```
www.example.com/products.php?id=10

www.example.com/products.php?id=10' OR '1'='1'
```

- Cơ chế hoạt động của đa số URL tham số: tạo truy vấn ngược về bảng liên quan, tìm hàng dữ liệu có ID tương ứng (trong ví dụ đang đi tìm sản phẩm có ID = 10)
- Luận lý **‘1’ = ‘1’** luôn đúng, nếu thực thi truy vấn thành công, cơ sở dữ liệu trả lại toàn bộ các dòng và cột trong bảng đang được truy xuất

SQL Injection

DEMO



02

BẢO MẬT THANH TOÁN DI ĐỘNG, CÁC MỐI ĐE DỌA VÀ THÁCH THỨC

Mobile Payment Security, Threats, and Challenges

GIỚI THIỆU

CÁCH MẠNG HOÁ PHƯƠNG THỨC THANH TOÁN

THANH TOÁN DI ĐỘNG

SMS, NFC, …

PHỔ BIẾN, THUẬN TIỆN

→

MỐI ĐE DOẠ BẢO MẬT

HỆ THỐNG THANH TOÁN DI ĐỘNG

- **THANH TOÁN DI ĐỘNG**
  - Là dịch vụ thanh toán qua thiết bị di động, phổ biến trên iOS và Android.
  - Người dùng liên kết tài khoản ngân hàng hoặc thẻ tín dụng trước khi giao dịch.

5 loại chính:

TẠI ĐIỂM BÁN (POS)

Thanh toán bằng NFC, ví dụ Apple Pay, Samsung Pay.

NHƯ ĐIỂM BÁN (MOBILE POS)

Người bán sử dụng thiết bị di động làm POS, ví dụ Square Register.

NỀN TẢNG THANH TOÁN DI ĐỘNG

Dùng ví điện tử, ví dụ PayPal, Alipay.

HỆ THỐNG THANH TOÁN ĐỘC LẬP

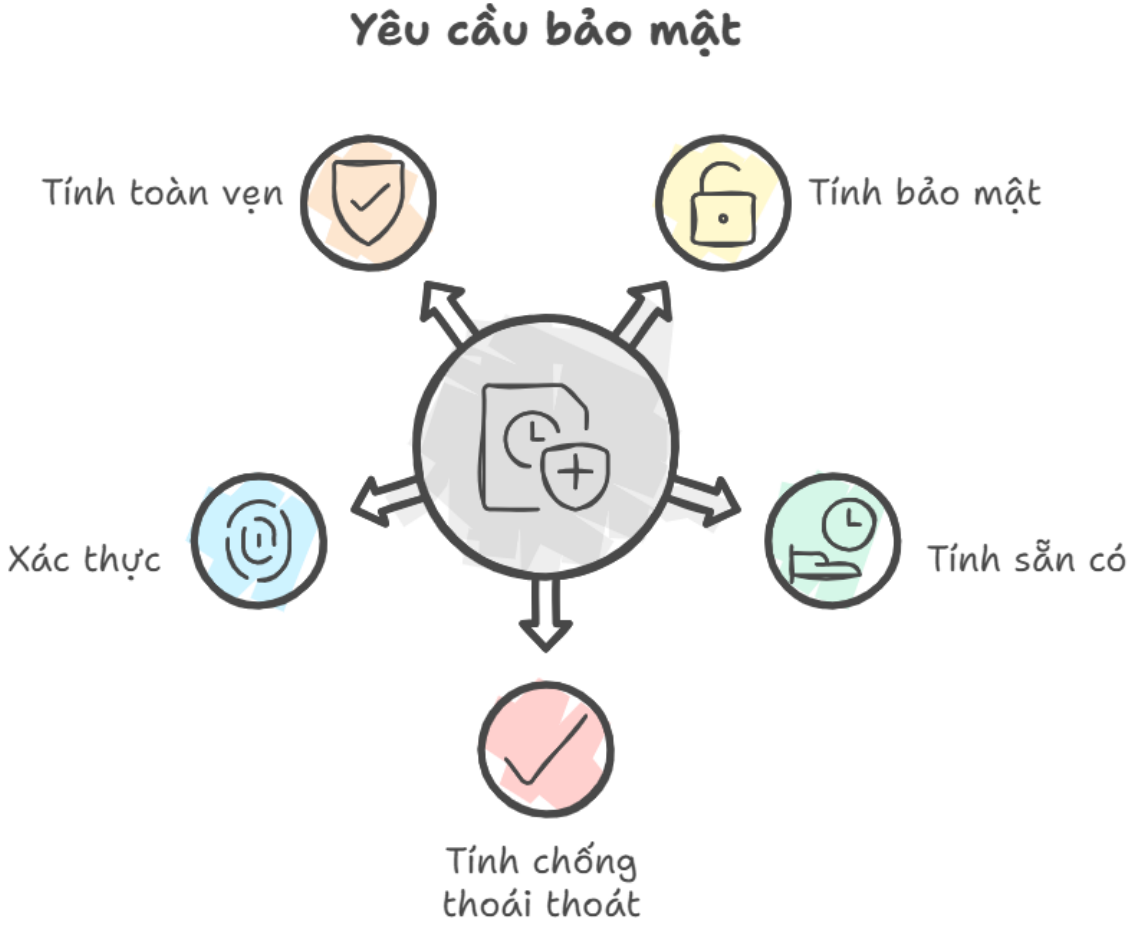
Ứng dụng của riêng công ty, ví dụ Starbucks.

THANH TOÁN QUA NHÀ MẠNG

Tính phí trực tiếp vào hóa đơn điện thoại, phổ biến với Boku ở châu Âu.

BẢO MẬT TRONG THANH TOÁN DI ĐỘNG

Dịch vụ bảo mật thanh toán di động



BẢO MẬT TRONG THANH TOÁN DI ĐỘNG

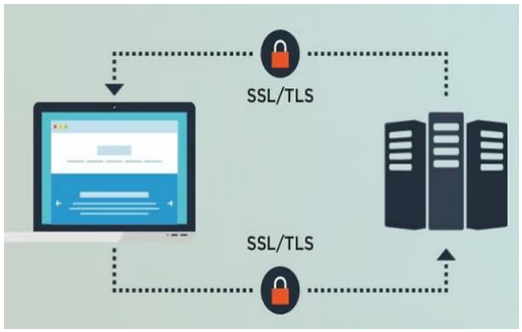
CƠ CHẾ

- **Dấu vân tay**: Sử dụng để xác thực giao dịch (Apple Pay, Samsung Pay).
- **Tên người dùng/mật khẩu**: Phương pháp xác thực phổ biến trên các hệ thống thanh toán.
- **Xác thực nhiều yếu tố**: Tăng cường bảo mật qua mã xác thực khi đăng nhập từ thiết bị mới.
- **SSL/TLS:** Bảo vệ dữ liệu thanh toán trong quá trình truyền tải trên Internet.
- **Yếu tố bảo mật:** Lưu trữ dữ liệu nhạy cảm và thực hiện hoạt động mật mã trên thiết bị (Apple Pay lưu trữ số tài khoản duy nhất).

MỐI ĐE DOẠ & GIẢI PHÁP

Phần mềm độc hại (Malware)

- Trojan Zeus/ZitMo đánh cắp thông tin xác thực giao dịch ngân hàng **qua tin nhắn SMS.**
- Phần mềm độc hại ghi lại và truyền dữ liệu cá nhân như nhật ký cuộc gọi, định vị GPS.



Lỗ Hổng SSL/TLS

- Lỗ hổng Heartbleed trong **OpenSSL** cho phép đánh cắp dữ liệu.
- Tấn công man-in-the-middle (MITM) có thể chặn dữ liệu thanh toán giữa khách hàng và máy chủ.

MỐI ĐE DOẠ & GIẢI PHÁP

Rò rỉ dữ liệu tại các hệ thống POS (Target, Home Depot) làm lộ thông tin cá nhân và thanh toán của hàng triệu khách hàng.

Quy trình thanh toán di động có nhiều bên tham gia, tạo cơ hội cho rủi ro về bảo mật dữ liệu , gây hậu quả lớn

NGƯỜI DÙNG

- Sử dụng mật khẩu/mẫu khóa mạnh.
- Nâng cấp hệ điều hành và cài bản vá bảo mật.
- Tránh tải phần mềm không rõ nguồn gốc và kết nối Wi-Fi không đáng tin cậy.

NHÀ CUNG CẤP DỊCH VỤ

- Áp dụng bảo mật SSL/TLS, xác thực chứng chỉ máy chủ.
- Ngăn chặn tấn công bằng cách cảnh báo người dùng khi có chứng chỉ không hợp lệ.

THÁCH THỨC TRONG THANH TOÁN DI ĐỘNG

PHÁT HIỆN PHẦN MỀM ĐỘC HẠI

XÁC THỰC ĐA YẾU TỐ

NGĂN CHẶN RÒ RỈ DỮ LIỆU

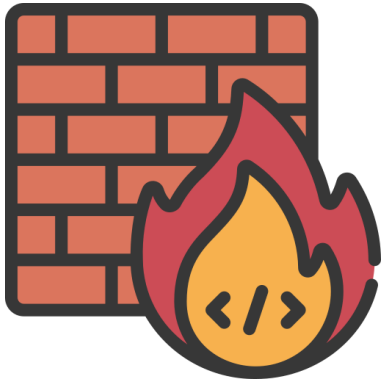
PHÁT HIỆN, BẢO VỆ VÀ CHỐNG GIAN LẬN

03

CÁC HÌNH THỨC BẢO MẬT VÀ AN TOÀN THÔNG TIN

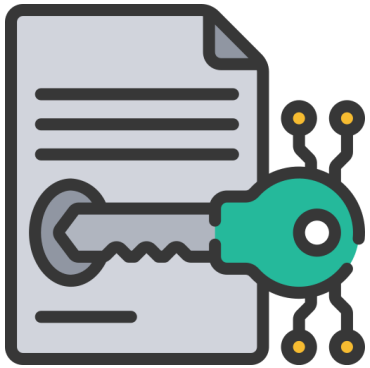
Forms of information security and safety

2FA



WAF

ENCRYPTION



DIGITAL SIGNATURE

SSL/TLS PROTOCOL

XÁC THỰC 2 YẾU TỐ

Yêu cầu người dùng xác nhận danh tính thông qua 2 yếu tố bảo mật khác nhau:

Yếu tố thứ nhất: Mật khẩu/mã PIN bạn đã tạo

Yếu tố thứ hai: Điện thoại, USB, Token bảo mật... dùng để tạo mã xác thực tạm thời, tạo dữ liệu sinh trắc học,...

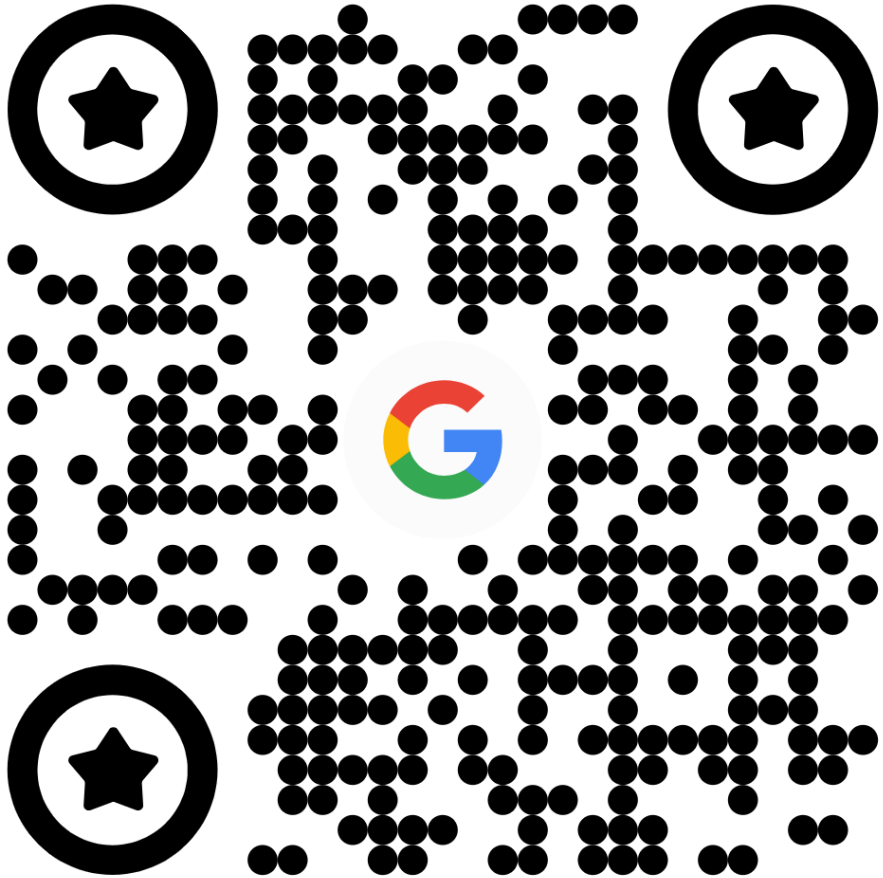
Ví dụ: đăng nhập Facebook sau một thời gian dài yêu cầu một mã OTP được gửi vào email tài khoản

Ưu: Tăng cường bảo mật, bảo vệ thông tin

Nhược: Gây mất trải nghiệm người dùng, khó khăn trong việc khôi phục tài khoản

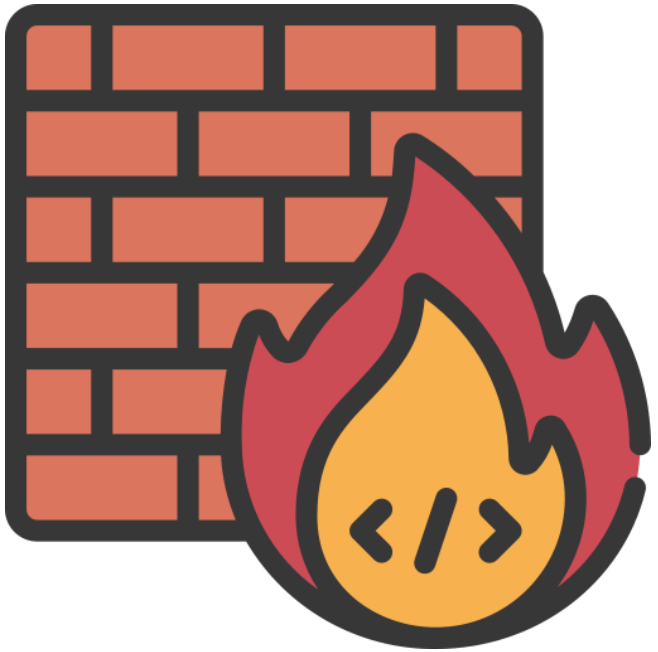
XÁC THỰC 2 LỚP

DEMO



TƯỜNG LỬA ỨNG DỤNG WEB (WAF)

Là một loại tường lửa chuyên dụng, được thiết kế để bảo vệ web khỏi các cuộc tấn công phổ biến nhằm vào các lỗ hổng bảo mật trong ứng dụng.



CHỨC NĂNG CHÍNH CỦA WAF:

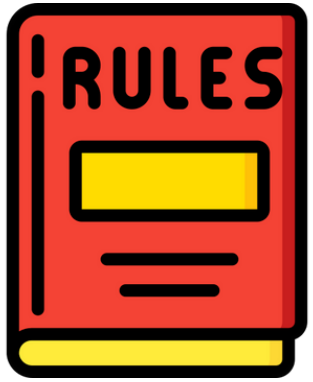
- Bảo vệ ứng dụng web (SQLi, XSS, CRFS)
- Giám sát lưu lượng HTTP/HTTPS
- Bảo vệ chống lại các tấn công Zero-day, các kiểu tấn công mới chưa được nhận diện trước đó

TƯỜNG LỬA ỨNG DỤNG WEB (WAF)

CƠ CHẾ HOẠT ĐỘNG

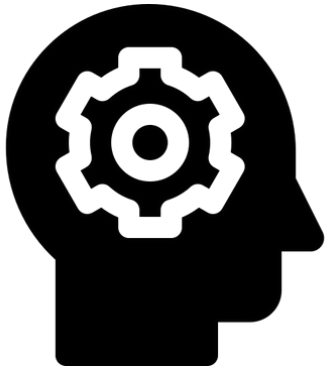
PHÂN TÍCH LƯU LƯỢNG

Phân tích từng yêu cầu và phản hồi HTTPS



RULE-BASED

Sử dụng các quy tắc bảo mật được cấu hình trước



BEHAVIORAL-BASED

Có khả năng học và phân tích hành vi lưu lượng hợp lệ

WAF hoàn toàn có thể ngăn chặn SQLi, Cross-Site Scripting (XSS) , Cross Site Request Forgery (CSRF) và Remote File Inclusion (RFI)/Local File Inclusion (LFI)

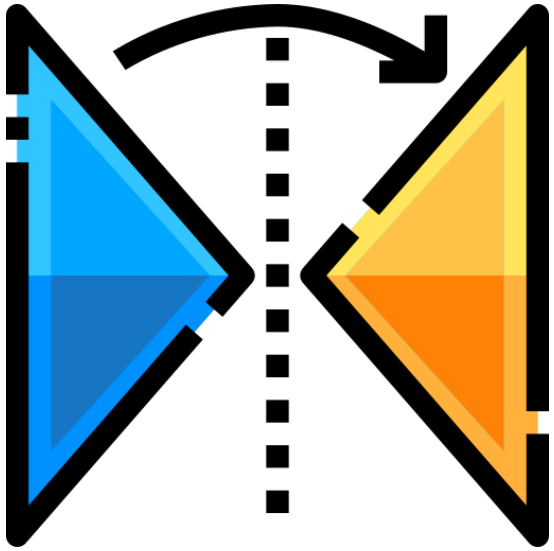
MÃ HOÁ CƠ BẢN

ENCRYPTION

Là kỹ thuật biến các đoạn chữ thuần thành những đoạn ký tự mà **người khác không thể đọc được**, dựa trên **hai nguyên tắc** cơ bản là **hoán vị và thay thế** để tạo ra các bản mã khác nhau.

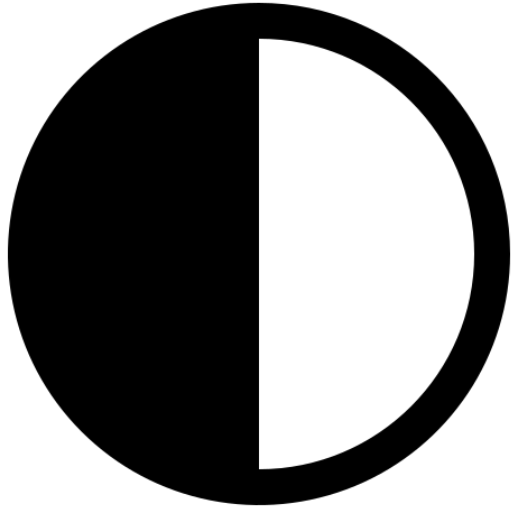
Các thuật ngữ cần biết:

- **Cipher text (CT)**: bản mã
- **Plain text**: bản rõ
- **Secret key**: Khoá bí mật
- **Public key**: khoá công khai
- **Private key**: Khoá riêng tư



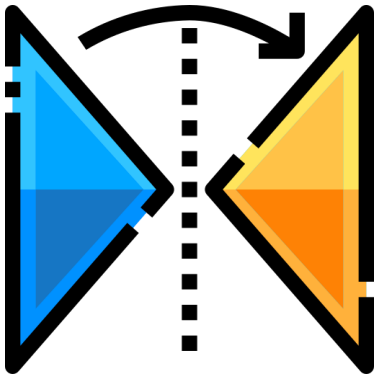
SYMMETRIC

DES, AES, 3DES



ASYMMETRIC

RSA, ElGamal, Curve



SYMMETRIC

DES, AES, 3DES

Là kiểu mã hóa sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã dữ liệu, ở đó người gửi lẫn nhận đều có chung một khóa bí mật.

Ưu điểm: đơn giản, nhanh, hiệu quả về tài nguyên

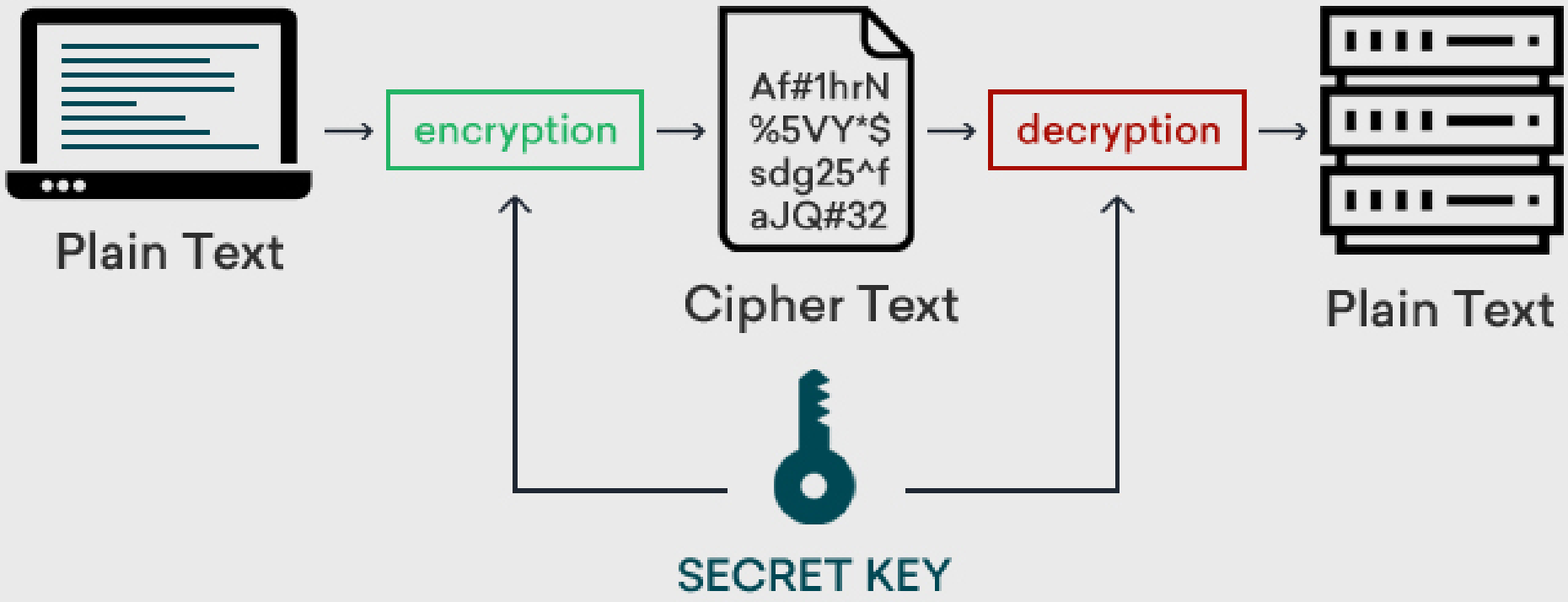
Nhược điểm: phân phối khóa chưa bảo mật, không chống thái thoát, rủi ro cao khi khóa lộ

Thường được kết hợp với mã hóa bất đối xứng trong các giao thức (SSL/TLS), tại đó:

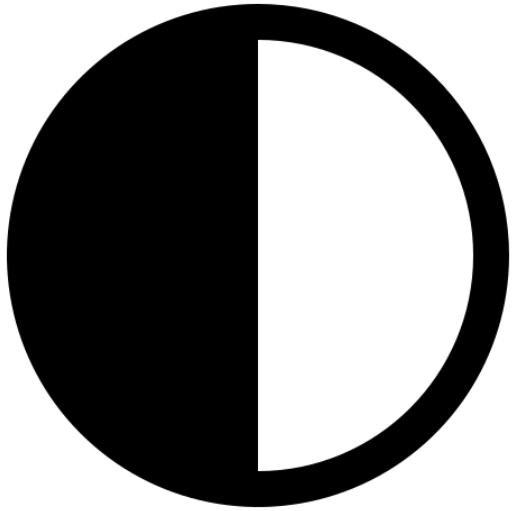
- Mã hóa đối xứng được dùng để mã hóa dữ liệu
- Mã hóa bất đối xứng được dùng để trao đổi khóa

=> SSL/TLS tận dụng được ưu điểm của cả hai loại mã hóa để tăng cường bảo mật tổng thể.

Symmetric encryption



Là kiểu mã hóa sử dụng **hai khóa riêng biệt:** khóa công khai (**public/encryption) key**) **để mã hóa** và khóa bí mật (**private/decryption key**) **để giải mã.**



Khóa công khai có thể được chia sẻ tự do, trong khi khóa bí mật được giữ kín.

Ưu điểm: phân phối khóa bảo mật, chống thoái thoát, bảo mật cao hơn mã hóa đồng bộ

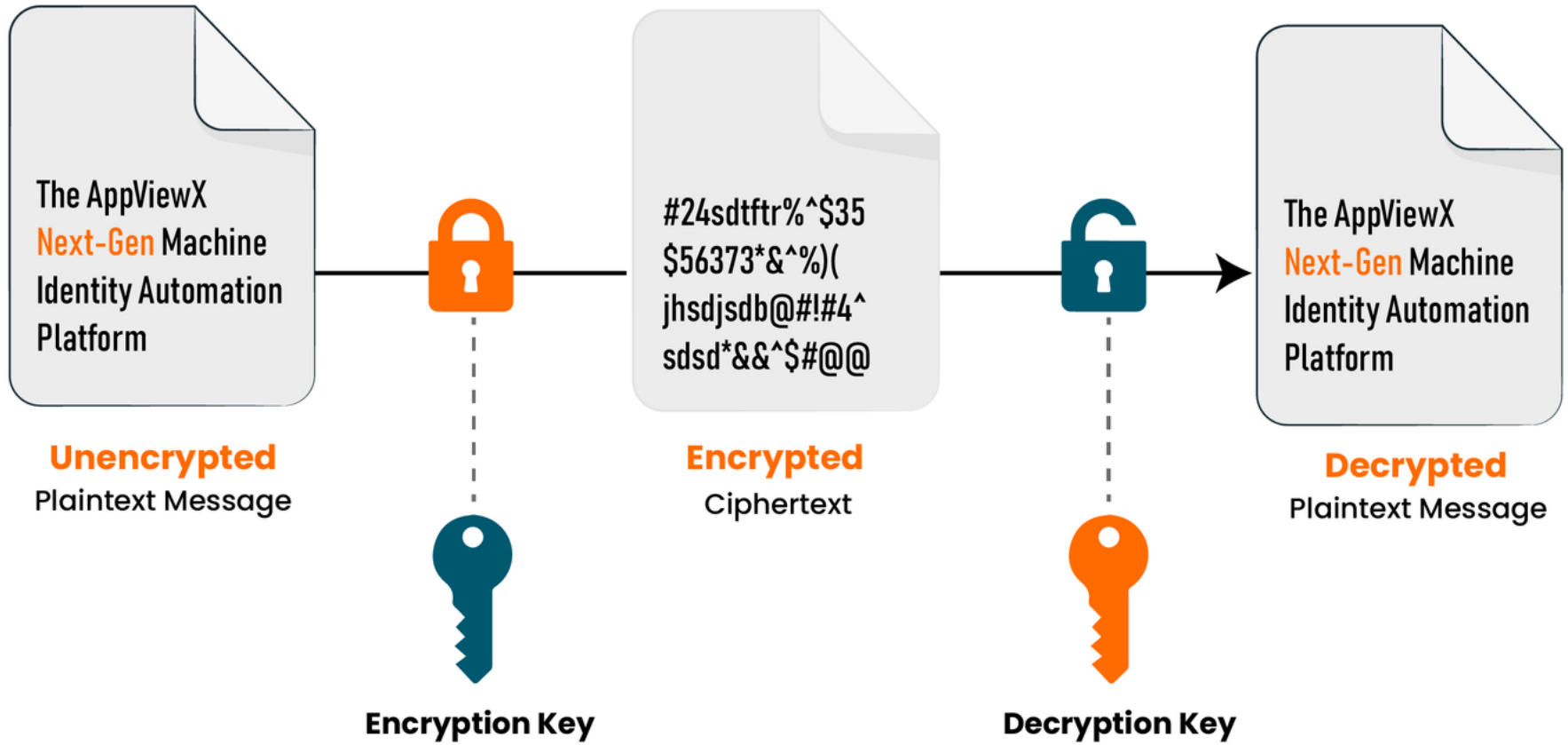
Nhược điểm: chậm hơn mã hóa đối xứng, yêu cầu tài nguyên cao hơn, phức tạp trong việc triển khai

ASYMMETRIC

RSA, ElGamal, Curve

appviewX

Asymmetric Encryption

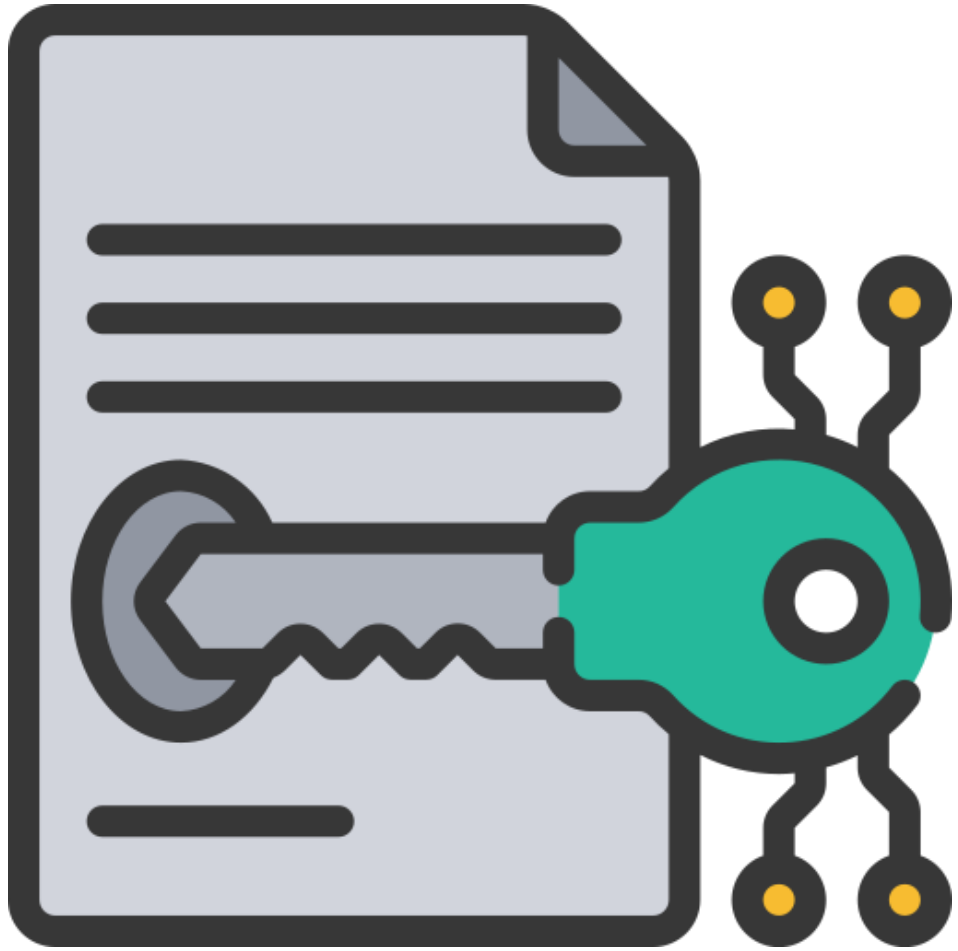


CHỮ KÝ SỐ

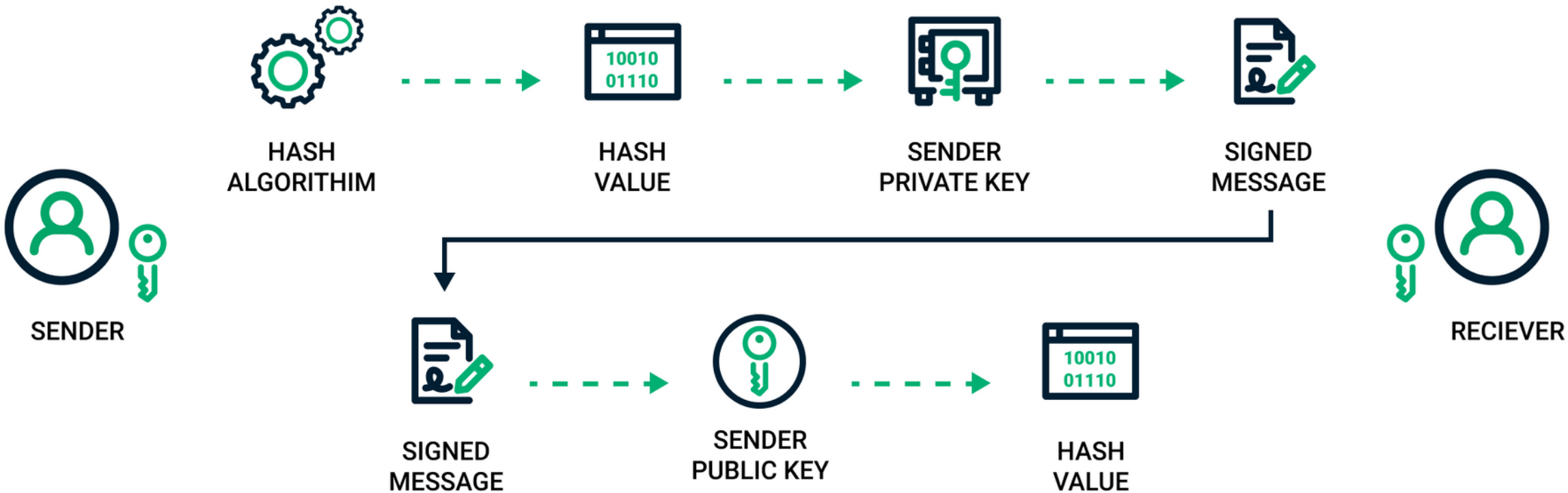
“Chữ ký số là chữ ký điện tử sử dụng thuật toán khóa không đối xứng, gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được dùng để ký số và khóa công khai được dùng để kiểm tra chữ ký số. Chữ ký số bảo đảm tính xác thực, tính toàn vẹn và tính chống chối bỏ nhưng không bảo đảm tính bí mật của thông điệp dữ liệu.”

- Điều 3 chương 1 luật Giao dịch điện tử năm 2023

Chữ ký số là sự kết hợp giữa mã hóa bất đồng bộ và các hàm băm.



How Does a Digital Signature Work?

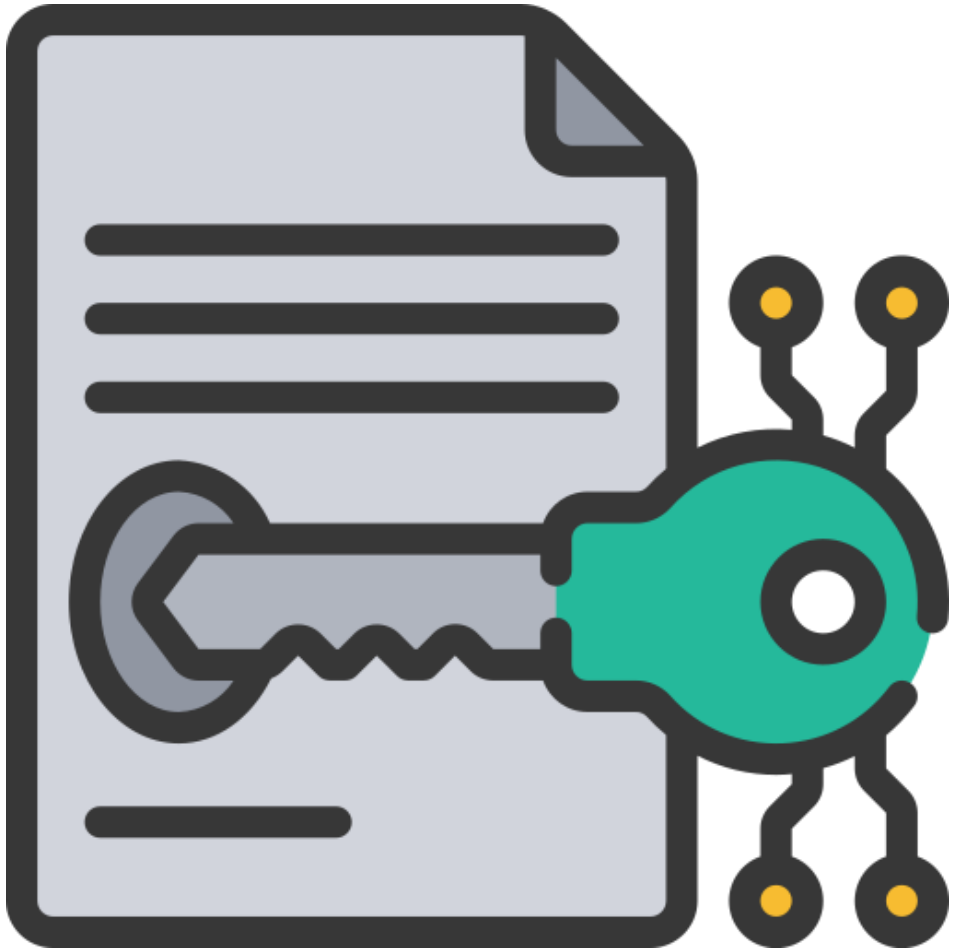


Các tính chất của chữ kí số:

- Mang tính **xác thực tuyệt đối**
- **Dữ liệu toàn vẹn**
- **Không thể chối bỏ**
- **Không thể làm giả**

Những tính chất này làm cho chữ kí số :

- Trở thành một cách thức **giao tiếp an toàn**
- **Không thể thiếu trong giao dịch tài chính**
- Trở thành một loại **tài liệu pháp lý** cho các thỏa thuận và hợp đồng



Chữ ký số có nhiều ứng dụng quan trọng trong TMĐT, giúp đảm bảo tính bảo mật, xác thực và toàn vẹn của các giao dịch trực tuyến:

- Xác thực và Bảo mật Giao dịch
- Xác nhận và Ký Hợp đồng Điện tử
- Quản lý Đơn hàng và Thanh toán
- Xác thực Thông tin và Hồ sơ...

SSL/TLS

Là một phiên bản bảo mật của giao thức HTTP. HTTPS kết hợp HTTP với TLS (trước đó là SSL) để đảm bảo rằng dữ liệu được truyền giữa trình duyệt và máy chủ được mã hóa và bảo mật.

TLS/SSL hoạt động dựa trên sự kết hợp của private key và public key:

1. Bắt tay (Handshake)
2. Mã hóa dữ liệu
3. Kiểm tra tính toàn vẹn (qua MAC / HMAC)
4. Xác thực danh tính (qua CA)

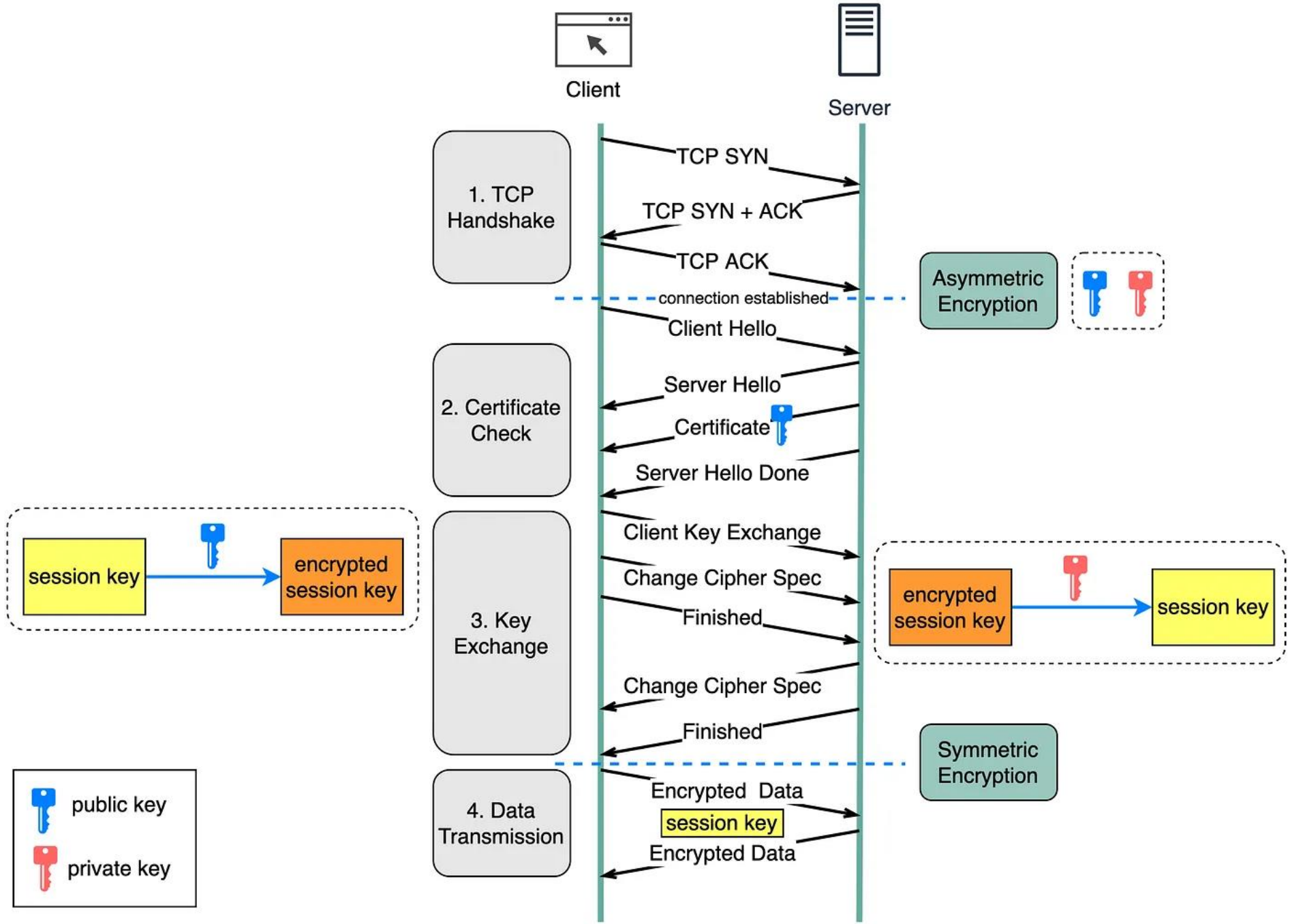
B1. Trình duyệt yêu cầu HTTPS: Khi bạn truy cập vào một trang web bằng HTTPS, trình duyệt của bạn sẽ **yêu cầu máy chủ thiết lập một kết nối bảo mật bằng HTTPS**.

B2. Máy chủ gửi chứng chỉ số (SSL/TLS Certificate): Máy chủ phản hồi bằng cách gửi chứng chỉ số, bao gồm **khóa công khai** của máy chủ và **thông tin xác nhận** từ một tổ chức chứng thực **(Certificate Authority - CA),** để xác thực danh tính của nó.

B3. Xác thực chứng chỉ: Trình duyệt kiểm tra tính hợp lệ của chứng chỉ số bằng cách xác thực nó với CA. **Nếu chứng chỉ hợp lệ, trình duyệt tiếp tục quá trình.**

B4. Thiết lập phiên mã hóa: Trình duyệt và máy chủ thỏa thuận về thuật toán mã hóa, tạo ra một **khóa phiên (session key)** để mã hóa dữ liệu truyền suốt phiên làm việc.

Sau khi khóa phiên được tạo, **tất cả dữ liệu truyền giữa trình duyệt và máy chủ sẽ được mã hóa và bảo mật** cho đến khi kết nối đóng.


Client
Server
1. TCP Handshake
TCP SYN
TCP SYN + ACK
TCP ACK
connection established
Asymmetric Encryption
2. Certificate Check
Client Hello
Server Hello
Certificate
Server Hello Done
3. Key Exchange
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Symmetric Encryption
4. Data Transmission
Encrypted Data
session key
Encrypted Data
session key
encrypted session key
encrypted session key
session key
public key
private key

Tiêu chí	HTTP	HTTPS
Bảo mật	Không mã hóa, dễ bị đọc trộm	Được mã hóa, khó đọc trộm
Cổng mặc định	Port 80	Port 443
Xác thực	Không cung cấp cơ chế	Sử dụng chứng chỉ số để xác thực
Tốc độ	Nhanh hơn do không mã hóa	Chậm hơn một chút do quy trình
Chứng chỉ SSL	Không yêu cầu	Yêu cầu chứng chỉ SSL/TLS

Fun fact: Nếu muốn cải thiện SEO và lên top tìm kiếm, HTTPS là bắt buộc!

DEMO

XEM VÀ THIẾT LẬP CHỨNG CHỈ HTTPS