**Mật mã học**

1. **4 mục tiêu cơ bản của mật mã học**

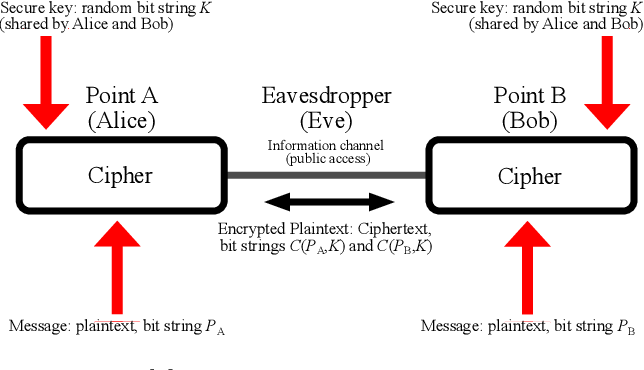
Đảm bảo tính bí mật : thông tin chỉ được tiết lộ cho những người được phép.

Tính toàn vẹn : thông tin không thể bị khi không có yếu tố ngoài tác động.

Tính xác thực : người gửi hoặc người nhân có thể chứng minh là chính họ.

Tính chống chối bỏ : người nhận hoặc gửi không thể chối bỏ họ đã thao tác với thông tin, hoặc phủ nhận liên quan đến thông tin.

1. **Nguyên tắc Kirchoff**



Trong môi trường truyền tin bằng điện toán thì sẽ phải truyền qua các kênh không an toàn (sóng radio và họ bắt được đúng tần số của mình), đối phương có thể biết được thông tin mã hóa và thậm chí là thuật toán dùng để mã hóa. Vậy cách bảo mật tối ưu nhất là bảo vệ key mà dùng để mã hóa.

**Nguyên tắc Kirchoff :** Toàn bộ cơ chế sinh mã và giải mã ngoại trừ thông tin về khóa đều được công khai với kẻ thù. Điều này chỉ ra độ an toàn không phụ thuộc vào thuật toán mà là cách quản lý và bảo vệ khóa.

1. **Secret key cryptography (Symmetric-key algorithm)**

Hay còn gọi là thuật toán khóa đối xứng, tức 2 bên nhận và gửi đều thống nhất chung với nhau một khóa để có thể giải mã và mã hóa thông tin.

Các thuật toán mã hóa đối xứng : DES, 3DES, AES

1. **Block cipher**

Là các khối có độ dài phụ thuộc vào thuật toán (64-128-256 bit) được tách nhỏ ra từ thông tin ban đầu và sau đấy được mã hóa cùng key

Do các khối có độ dài cố định mà thông tin thì không phải lúc nào cũng vậy nên phải thêm vào padding thông tin có độ dài là bội của số bit được quy định trong thuật toán.

Có nhiều cách để mã hóa từng khối :

Diagram

Description automatically generatedEBC (Electric CodeBlock): mã hóa độc lập từng khối với key. Nhưng nếu các khối giống nhau thì có thể tạo ra Cipher text giống nhau sau mỗi lần.

Diagram

Description automatically generatedCBC (Chain CodeBlock): mã hóa từng khối theo nguyên lý quy hồi, chúng dùng khổi cipher text của kết quả trước XOR với plaintext của khối hiện tại. Khối Initialization Vector sẽ được khởi tạo đầu (là một số ngãu nhiên) để làm cho việc sẽ đưa ra Cipher text khác nhau sau mỗi lần mã hóa.

Ngoài ra còn nhiều chế độ khác CTR, CFB, ...

Thuật toán mã hóa có thể lặp đi lặp lại quy trình encryption được gọi là các round.

Ứng dụng : khi thông tin đã đầy đủ, dùng trong các tình huống mà thông tin là dạng tin nhắn.

Các thuật toán dùng Ciphertext :

**DES (Data Encryption Standard)** :

Độ dài mỗi khối : 64bit

Key : 64bit

Số vòng : 16

**3DES (Triple Data Encryption Standard)** :

Là DES nhưng mỗi block được trải qua 3 vòng :

***EK3(DK2(EK1(PlainText))***

Mã hóa với key1 sau đấy giải mã nó với key2 và mã hóa với key3.

Các key có độ dài 56bit, chúng có thể độc (bảo mật nhất) hoặc trung nhau tất cả (kém nhất).

**AES (Advanced Encryption Standard)** **:**

Độ dài một khối : 128bit

Độ dài key : 128-192-256 bit

Số vòng : 10-12-14 (tương ứng độ dài key)

1. **Stream Cipher**

Khác với Block Cipher khi mã hóa từng khối của thông tin độ dài của khối phụ thuộc vào thuật toán. Stream Cipher sẽ mã hóa từng byte của thông tin tại một thời điểm. Thuật toán sẽ sử dụng key để tạo ra các giá trị ngẫu nhiên sau đó đưa keystream, keystream này sẽ XOR với plaintext để tạo ra giá trị encrypted.

Để decrypt cần phải có keystream, sau đó XOR nó với cipher text để đưa về plain text.

Vậy vấn đề bảo mật ở đây là tạo ra keystream ngẫu nhiên nhất có thể. Đối với pseudo random number thì bộ giá trị sinh ra có thể bị lặp lại sau một số lần lặp.

Stream Cipher có thể được sử dụng trong các hệ thống mà không biết độ dài tin nhắn, yêu cầu đơn giản như embed trong phần cứng, trong các kết nối không dây yêu cầu bảo mật, hoặc yêu cầu về tốc độ,

Các thuật toán ChaCha, RC4, A5/1, A5/2, ...

1. **Message authentication code**

Là đoạn mã được tạo ra để kiểm tra tính xác thực và toàn vẹn của thông tin. Đoạn mã có trách nhiệm đảm bảo thông tin chỉ có thể đến từ người gửi và thông tin nhận được không bị thiếu sót.

Một hệ thống MAC gồm có các thành phần :

+ Thuật toán sinh khóa sẽ lựa chọn ngẫu nhiên một khóa trong tập khóa

+ Thuật toán ký sẽ băm thông tin cùng với key tạo ra đoạn mã

+ Thuật toán sẽ dùng key để xác thực thông tin nhận đến và so sánh với đoạn mã MAC. Thông tin được chấp nhận khi kết quả là bằng nhau.

Ứng dụng :

Trong các hệ thống gửi tin mà yêu cầu cao về tính xác thực giữa người nhận và người gửi

Thuật toán :

CMAC (Chain MAC) : sử dụng nguyên lý giống CBC để tạo ra chuỗi được mã hóa.

HMAC : nối key và thông tin và với nhau và sử dụng một hàm băm để tạo ra đoạn mã.

1. **Public key cryptography**

Khác với Symmetric-key algorithm khi sử dụng 1 key trong cả việc mã hóa và giải mã,  Asymemrtric cryptography sử dụng 2 key, 1 key trong việc mã hóa và 1 key trong việc giải mã.

Cả người nhân và người gửi để có chung một public key, khi giao tiếp 2 bên sẽ trao đổi cái này cho nhau.

Thông tin khi gửi đi sẽ được mã hóa bằng public key, khi giải mã mỗi bên sẽ sử dụng private key để giải mã thông tin được mã hóa.

1. **Cryptographic hash function**

Là hàm băm mà nhận đầu vào là thông tin và đưa ra một chuỗi có độ dài cố định.

Hàm băm này cần có yêu cầu :

* Không thể đảo ngược, tức khi có chuỗi băm không thể tìm ra thôn tin ban đầu.
* Khuếch tán, trong thông tin đầu vào khi có thay đổi, dù chỉ nhỏ nhất sẽ dẫn đến sự thay đổi lớn về chuỗi kết quả sau khi băm.
* Nhất quán, thông tin đầu vào sẽ luôn luôn đưa ra một kết quả sau khi băm, không bị thay đổi sau số lần băm.
* Khó để tìm ra 2 chuỗi đầu vào khác nhau mà tạo ra một chuỗi băm giống nhau.

Thuật toán tiêu biểu

MD5 : lấy các khối đầu vào 512bit và đưa ra 128bit (nếu thông tin không đủ độ dài sẽ được padding thêm để tạo ra bội của 512 bit)

SHA-1 :ý tưởng giống MD5 đưa ra chuỗi băm có độ dài 160bit

SHA-256 : đưa ra chuỗi độ dài 256bit

1. **PKC (public key encryption)**

Là hệ thống mã hóa mà sử dụng cặp khóa. Trong cặp khóa có 1 public key và private key. 2 khóa này có quan hệ về mặt toán học với nhau, không thể tìm được khóa bí mật mà dựa trên khóa công khai.

* Sender yêu cầu cung cấp hoặc tự tìm khoá công khai của Receiver trên một Server chịu trách nhiệm quản lý khoá công khai.
* Sau đó hai phía thống nhất thuật toán dùng để mã hóa dữ liệu, Sender sử dụng khóa công khai của Receiver cùng với thuật toán đã thống nhất để mã hóa thông tin bí mật.
* Thông tin sau khi mã hóa được gửi tới Receiver, lúc này chính Sender cũng không thể nào giải mã được thông tin mà anh ta đã mã hóa (khác với mã hóa khóa riêng).
* Khi nhận được thông tin đã mã hóa, Receiver sẽ sử dụng khóa bí mật của mình để giải mã và lấy ra thông tin ban đầu.

Tính chất :

* Đảm bảo tính toàn vẹn cho dữ liệu
* Không thể tìm khóa bí mật khi dựa vào khóa công khai
* Gửi thông tin kèm public key trên đường truyền không tin cậy
* Private key sẽ được dữ lại ở mỗi bên
* Chậm hơn Symmetric-key

**RSA:**

Là thuật toán mã khóa công khai

* Chọn khóa:

Chọn 2 số nguyên tố lớn p và q, sau đó tính n = p.q

Tính giá trị hàm số Euler (số các số nguyên tố trong khoảng n) Ø(n)

Chọn số e sao cho e 1 < e < Ø(n) và là số nguyên tố

Tính d sao cho d.e đồng dư 1 khi chia cho Ø(n)

Khóa công khai gồm : n và e

Khóa bí mật gồm : d và e

**Ví dụ với RSA:**

Ứng dụng trong chữ ký số :

Khi một văn bản muốn được gửi đi và ký, người gửi sẽ hash văn bản đó kèm theo tính giá trị d mod n dựa vào chuỗi hash trên, kết quả cuối cùng là chữ ký số.

Người nhận khi nhận được sẽ kiểm tra chuỗi hash của văn bản, kèm theo đó là tính e từ chuỗi chữ ký, nếu e mod n = 1 và hash bằng nhau thì văn bản được công nhận.

1. **Public key infrastructure(PKI):**

PKI là hạ tầng mang tính tiêu chuẩn có trách nhiệm đảm bảo việc bảo mật thông tin trong môi trường không an toàn như internet. Thông tin có thể được trao đổi một cách an toàn dựa vào việc sử dụng một cặp mã bí mật và công khai được chứng nhận bởi một bên cung cấp chứng nhận CA (Certificate Authority). Nền tảng PKI cung cấp một chứng chỉ số dùng để xác minh cá nhân, tổ chức, dịch vụ, và có thể thu hồi chứng chỉ đó khi cần.

Do PKI cung cấp việc xác thực lẫn nhau nên một số ứng dụng có thể được sử dụng :

* + Mã hóa, giải mã văn bản.
  + Xác thực người dùng ứng dụng
  + Tạo chữ ký số.

PKI phải đảm bảo được các tính chất của mật mã học như đã nêu ở phần 1.

Các thành phần của PKI:

* + Timeline

    Description automatically generatedEE – End Entity (thực thể cuối) : là đối tượng sử dụng chứng nhận có thể là người hoặc hệ thống
  + CA – Certificate Authority : phát hành, quản lý và hủy bỏ chứng thư số. Là một mấu chốt quan trọng và được tín nhiệm bởi EE, bao gồm tập hợp người và hệ thống có độ an toàn và tin cậy cao.
  + Public Key Certificate – PKC (chứng nhận khóa công khai) :
    - Là sự ràng buọc của danh tinh và khóa công khai đối với thực thể cuối
    - Nó chứa đủ thông tin để người dùng khác có thể nhận biết và phân biệt mỗi EE
  + Tổ chức đăng ký chứng nhân (Registration Authority - RA) : là một phần của CA giảm tải cho CA có nhiệm vụ :
    - Xác thực cá nhân, chủ thể đăng ký PKC.
    - Kiểm tra tính hợp lệ do chủ thể cung cấp
    - Xác nhận quyền của chủ thể đối với những thuộc tính trong PKC
    - Tạo cặp khóa bí mật và công khai
    - Phân phối bí mật được chia sẻ đến EE
    - Trung gian đăng ký EE với CA
    - Lưu trữ khóa riêng
    - Tạo mới hoặc khôi phục khóa
    - Phân phối thành phần vật lý mang tính định danh đến EE
  + Kho lưu trữ chứng nhân (Certificate Repositories - CR) :
    - Là hệ thống lưu trữ chứng thư và danh sách cách chứng thư bị thu hồi.
    - Cung cấp cơ chế phân phối và danh sách thu hồi chứng thư.

1. **Digital Certificate**

Chứng thư số là một tài liệu điện tử dùng để xác nhận khóa công khai. Chứng thư bao gồm trong đó thông tin về khóa, thông tin về chủ sở hữu và chữ ký số. Phần mềm sử dụng chứng thư số sẽ kiểm tra chữ ký và độ tin cậy của thông tin về chủ sở hữu sau đó có thể dùng nó thiết lập một giao dịch an toàn.

Các thành phần trong chứng thư số :

* Số serial : là duy nhất với mỗi chứng chỉ tử CA
* Subject : là loại của thực thể sử hữu chứng thư
* Issuer : thực thể đã công nhận và ký vào chứng thư
* Not before : thời gian gần nhất mà chứng thư còn hiệu lực
* Not after : thời gian hết hạn
* Key Usage : thông tin liên quan đến public key
* Extended Key Usage : thông tin mà hứng chỉ có thể sử dụng (tùy chọn)
* Public Key : khóa công khai thuộc về loại đăng ký
* Signature Algorithm : chứa thông tin về thuật toán mã hóa đối với chữ ký
* Signature : chuỗi hash của certificate và chuỗi được mã hóa của nó với EE private key

1. **Quy trình chứng thực chứng thư số**

Nếu một người muốn chứng thực chữ thư số, họ sẽ lây thông tin về chứng thư đó và lấy được public key của người muốn giao tiếp.

Sau đó dùng private key của cá nhân để kiểm tra thông tin về người muốn giao tiếp.

Nếu cả 2 đối tượng cùng đăng ký chưng thư ở cùng CA thì có thể lấy ngay thông tin của nhau

Nhưng nếu 2 đối tượng đăng ký CA ở 2 chỗ khác nhau , thì người muốn chức thực phải biết đường dẫn tới CA của bên cần được chứng thực