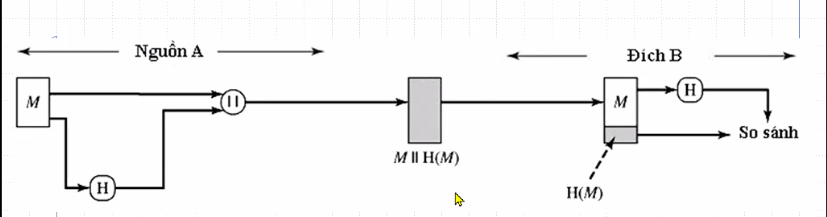
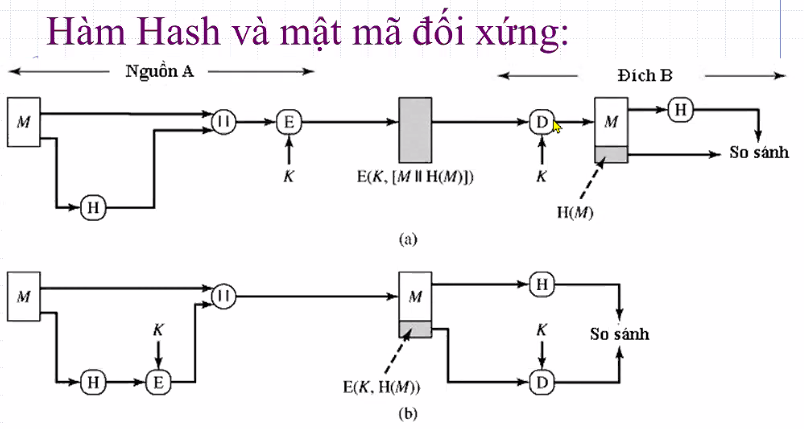
## **Các hàm Hash**

| Khái niệm | Là một công cụ quan trọng trong chứng thực |
| --- | --- |
| Nhiệm vụ | Tác động lên thông điệp đầu vào M (có kích thước bất kì) để thu được một khối dữ liệu nhỏ H(M) có kích thước cố định ở đầu ra. H(M) được gọi là mã hash của M.  -H(M) đặc trưng cho M, nhưng thường có kích thước nhỏ hơn M, sẽ được sử dụng làm giá trị chứng thực. |
| Ứng dụng | -Mã hash thường được đính kèm và gửi cùng với thông điệp, nhằm mục đích chứng thực cho thông điệp đó là chính xác về mặt nội dung và nguồn gốc.  -Mã hash thường được dùng kết hợp với các mật mã khoá công khai hoặc đối xứng. |
|  |  |



* Sơ đồ này dễ bị giả mạo phải phối hợp với mật mã



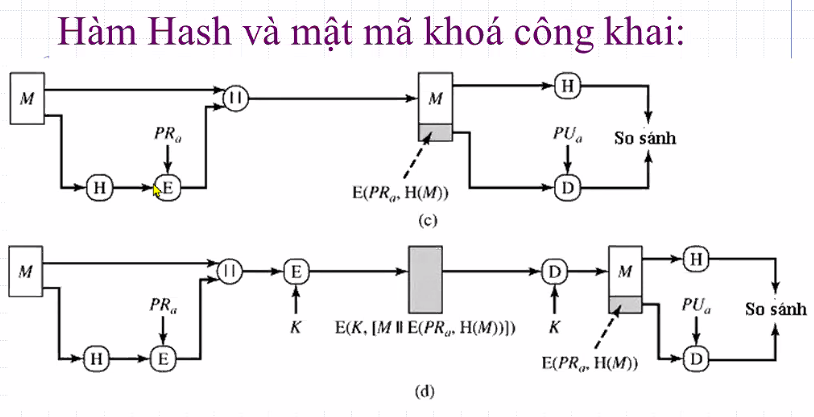
Sơ đồ A ⇒ (Bảo mật thông điệp và Chứng thực nd thông điệp

* (Bảo mật thông điệp)Thông điệp M qua hàm H đưa đến bộ ghép đưa đến hàm mã hóa E với khóa K ==> dữ liệu đều ra E(K,[M || H(M)])
* a,(Chứng thực nd thông điệp)THông điệp đã đc mã hóa E(K,[M || H(M)]) truyền đến ng nhận ,ng nhận giải mã bằng khóa K ra thông điệp và hàm H(M) và hàm H so sánh nếu giống nhau thì thông điệp M ng gửi

Sơ đồ B ⇒ Xác thực ND thông điệp dùng khi k cần bí mật(dùng mật mã đối xứng)

* THông điệp M qua hàm Hask đc mã hóa bằng hàm E với khóa K thu đc bộ ghép truyền đi (có thể bị kẻ địch đọc (nhưng k sửa đc vì k biết khóa K) ND) thông điệp M đã đã đc mã hóa E(K,H(M)) đầu ra hàm H và giải mã D với khóa K so sánh với nhau nếu trên đc truyền bị kẻ địch xâm nhập đọc mà sửa thì ở giai đoạn này sẽ bị phát hiện

| Sơ đồ A | Sơ đồ B |
| --- | --- |
| -Khối lg tính toán nhiều  -Bảo mật thông điệp  -Chứng thực nd thông điệp | -Giảm khối lượng tính toán  - k có khả năng giử bí mật ND thông điệp  -Có khả năng xác thực nd thông điệp  -Dùng khoá mm đối xứng |
| Sơ đồ C | Sơ đồ D |
| -Xác thực ND thông điệp trên đg truyền  -Xác thực nguồn gốc thông điệp  -Dùng khoá mm bất đối xứng  -K có khả năng bảo mật  ⇒ Cơ sở của kỹ thuật số | -Tổng hợp mm đối xứng và mm bất đối xứng và hàm Hask  -Bảo mật thông điệp trên đg truyền  -Xác thực ND thông điệp trên đg truyền  -Xác thực nguồn gốc thông điệp  -Tốc độ tính toán lâu |



Sơ đồ C : M || E(PR(A),H(M))

* Nguồn A: PR(a) khóa riêng,PU khóa công khai/ thông điệp M qua hàm H(M) mã hóa bằng khóa riêng của ng gửi ,ND trên đg truyền gửi đến bên nhận
* Đích B:(dùng mm bất đối xứng) thông điệp tách ra mã H của thông điệp M bằng khóa riêng đưa đến giải mã D bằng khóa công khai PU(a) của ng gửi đầu ra H(M) so sánh H bên thu nếu giống thì thông điệp M k bị thay đổi trên đg truyền

Sơ đồ D

* Nguồn A: E(K,[M|| E(PR(a),H(M)))]) ⇒ Thông điệp M qua hàm H đem mã hóa hàm E với khóa PR(a) riêng của ng gửi A => E[PR(a),H(M)] đến bộ ghép lại mã hóa tiếp hàm E với khóa K gửi trên đg truyền đên ng nhận B
* Đích B: đến ng nhận giải mã D(K,M) mm đối xứng rồi tách (thông điệp M và hàm H) và giải mã E(PR(a),H(M)) bằng D(PU,H(M)) thu đc H(M) so sánh vs H ở trên

## **MAC**

### 

| **Khái niệm** | -MAC (Message Authentication Code - Mật mã chứng thực thông điệp) là một kĩ thuật mã hoá nhằm biến đổi thông điệp đầu vào M (có kích thước bất kì) thành một khối dữ liệu nhỏ có kích thước cố định ở đầu ra.  Khối dữ liệu đầu ra đó được gọi là mã MAC của thông điệp M. Nếu M bị thay đổi thì mã MAC của nó cũng sẽ thay đổi theo. |
| --- | --- |
|  | **-**k thể làm giả mã MAC vì k biết khóa K  -có thể sử dụng độc lập k cần sd mật mã |
|  | **Sơ đồ 1:**   * Xác thực ND thông điệp nhờ mã MAC * Bảo mật ND thông điệp nhờ hàm mm đối xứng * Phải mã hóa cả mã MAC và M nên tốc độ thực hiện lâu hơn   **Sơ đồ 2:**   * Xác thực ND thông điệp nhờ mã MAC * Bảo mật ND thông điệp nhờ hàm mm đối xứng * Mã hóa thông điệp rồi ms tính mã MAC Tốc độ thực hiện nhanh hơn |
|  |  |

**So sánh MAC và HASH**

|  | **MAC** | **HASH** |
| --- | --- | --- |
| Giống | -mã MAC thường được đính kèm và gửi cùng với thông điệp, nhằm mục đích chứng thực cho thông điệp đó là chính xác về mặt nội dung và nguồn gốc. | -mã HASH thường được đính kèm và gửi cùng với thông điệp, nhằm mục đích chứng thực cho thông điệp đó là chính xác về mặt nội dung và nguồn gốc. |
| Khác | **-**k thể làm giả mã MAC vì k biết khóa K  -có thể sử dụng độc lập k cần sd mật mã  Kĩ thuật mã hoá của MAC có sử dụng mật khoá *K(PR)*:  ***MAC* = C(*K*, *M*)**  *M* = Thông điệp đầu vào.  C = Hàm MAC.  *K* = Mật khoá chia sẻ giữa bên gửi và bên nhận.  *MAC* = Mã chứng thực thông điệp (Mã MAC). | -Trên đg truyền dễ bị giả mạo phải sd thêm mm đê bảo mật thông điệp |

# **Chữ ký số và chứng thực**

## **Chữ ký số**

| Khái niệm | - Là một cơ chế chứng thực cho phép tác giả thông điệp gắn thêm một đoạn mã vào thông điệp. Đoạn mã này đóng vai trò như một chữ ký.  -Chữ ký được tạo ra bằng cách tính giá trị hash của thông điệp và mã hóa nó bằng khóa riêng của tác giả.  -Chữ ký bảo đảm về nguồn gốc và tính toàn vẹn của thông điệp |
| --- | --- |
| Tính chất | - Phải xác minh được tác giả cùng thời gian của chữ ký.  - Phải chứng thực được nội dung thực sự vào thời gian ký.  - Phải kiểm tra được bởi một bên thứ ba, để giải quyết các tranh chấp. |
| Chữ kí số trực tiếp | SĐ a   * Xác thực ND thông điệp (so sánh)   SĐ b   * Xác thực ND thông điệp(so sánh) * Hiệu xuất truyền tin tốt hơn * Vì TĐ M vs mã HASH(ngắn) đem đi mã hóa -chuỗi mã hóa ngắn ghép vs thông điệp gưi đi trên đg truyền ngắn     SĐ c:   * Bảo mật thông điệp * Xác thực ND TĐ   SĐ d:   * Bảo mật thông điệp * Xác thực ND TĐ |
| chữ ký số trực tiếp | * Chỉ có tác dụng khi hai bên tin tg nhau chống ng thứ 3 trên đg truyền   Nhược điểm   * Chưa ghi thời gian phát sinh chữ kí * Thiếu cơ chế xử lí khi xảy ra tranh chấp(cần phải có trọng tài giải quyết) |

## **Chữ ký trọng tài**

| VD | Mã hóa | Ưu nhược điểm |
| --- | --- | --- |
| VD1:Mã hóa đối xứng, trọng tài thấy ND thông điệp | (1) X→ A: ID*X*|| *M*||E(*Kxa*, [*IDX*||H(*M*)])  (2) A → Y: E(*Kay*, [ID*X*||*M*||E(*Kxa*, [*IDX*||H(*M*)])||*T*]) | -Cả người gửi và người nhận đều phải tin tưởng tuyệt đối vào trọng tài A  -Nếu A không công tâm, anh ta có thể sửa đổi thông điệp, hoặc thông đồng với X để phủ nhận thông điệp đã kí, hoặc thông đồng với Y để giả mạo chữ kí của X. |
| VD2: Mã hóa đối xứng, trọng tài không thấy ND thông điệp | (1) X→ A: *ID*X||E(*K*xy, *M*)||E(*K*xa, [*ID*X||H(E(*K*xy, *M*))])  (2) A → Y: E(*K*ay,[*ID*X||E(*K*xy, *M*)])||  E(*K*xa, [*ID*X||H(E(*K*xy, *M*))||*T*]) | -Cả người gửi và người nhận đều phải tin tưởng tuyệt đối vào trọng tài A  -A không có khả năng sửa đổi thông điệp, nhưng vẫn có thể thông đồng với X để phủ nhận thông điệp đã kí, hoặc thông đồng với Y để giả mạo chữ kí của X. |
| VD3: Mã hóa khoá-công-khai, trọng tài thấy nội dung thông điệp | (1) X → A: ID*X*|| *M*||E(*PR*x, [*IDX*||H(*M*)])  (2) A → Y: E(*PR*a, [ID*X*||*M*||E(*PR*x, [*IDX*||H(*M*)])||*T*]) | -A biết nội dung thông điệp, nhưng không thể sửa đổi thông điệp hay làm giả chữ kí |
| VD4: Mã hóa khoá-công-khai. Trọng tài không thấy nội dung thông điệp | (1) X→A: *ID*X||E(*PR*x, [*ID*X||E(*PU*y, E(*PR*x, *M*))])  (2) A → Y: E(*PR*a, [*ID*X||E(*PU*y, E(*PR*x, *M*))||*T*]) | A không biết nội dung thông điệp, không thể sửa đổi thông điệp hay làm giả chữ kí |

## **Các giao thức chứng thực**

| Khái niệm | -Giao thức là tập hợp các quy tắc để các bên tham gia liên lạc trao đổi thông tin với nhau  -Các giao thức chứng thực cho phép các bên tham gia liên lạc tự nhận dạng lẫn nhau và chuyển giao khoá phiên |  |  |
| --- | --- | --- | --- |
| Giao thức chứng thực dùng mã hóa đối xứng | Giữa hai bên liên lạc A và B cần có một bên thứ ba gọi là KDC (Key Distribution Center - Trung tâm phân phối khóa tin cậy)  Bên A sẽ chia sẻ khoá Ka với KDC  Bên B sẽ chia sẻ khoá Kb với KDC  KDC sẽ sinh ra khoá phiên Ks (session key). Ks chỉ tồn tại trong một thời gian ngắn để A và B thực hiện phiên liên lạc. |  |  |
| Giao thức Needham-Schroeder(trực tiếp-mh đối xứng) | 1.A → KDC: *ID*A||*ID*B||*N*1  2.KDC → A: E(*K*a, [*K*s||*ID*B||*N*1||E(*K*b, [*K*s||*ID*A])])  3.A → B: E(*K*b, [*K*s||*ID*A])  4.B → A: E(*K*s, *N*2)  5.A → B: E(*K*s, *f*(*N*2)) | -Có khả năng bị tấn công nhại  N1, N2 là các giá trị nonce (lời gọi), có tác dụng chống tấn công nhại (đối phương chặn một thông điệp, sao chép thông tin, và sau đó gửi nhại chính thông điệp đó đến đích)  1.Khi A gửi cho KDC một nonce (N1), theo quy ước  2.KDC sẽ phải trả lời A bằng một giá trị tương ứng với N1, nếu không có nghĩa là thông điệp trả lời đã bị giả mạo  KDC sinh ra khóa phiên Ks rồi gửi cho A  3.A gửi thông điệp đã mã hóa (có chứa Ks) cho B  4.B gửi lại A một nonce (N2), chứng tỏ B đã nhận được Ks, và muốn kết nối với A  5.A trả lời B bằng một thông điệp có chứa N2. Phiên kết nối giữa A và B hình thành. Sau đó A và B có thể trao đổi các thông tin được mã hóa bởi Ks | Nhược điểm:  Nếu kẻ tấn công (bằng cách nào đó) có được một khóa phiên Ks cũ, anh ta có thể dùng nó để đóng giả A nhằm lừa gạt B  =>Giải pháp khắc phục  Cần gắn thêm nhãn thời gian T để thiết lập thời hạn sử dụng cho khóa phiên (xem giao thức Denning sau đây) |
| Giao thức Denning  (trực tiếp-mm đối xứng) | 1.A → KDC: *ID*A||*ID*B  2.KDC → A: E(*K*a, [*K*s||*ID*B||*T*||E(*K*b, [*K*s||*ID*A||*T*])])  3.A → B: E(*K*b, [*K*s||*ID*A||*T*])  4.B → A: E(*K*s, *N*1)  5.A → B: E(*K*s, *f*(*N*1)) | Khóa phiên Ks được gắn kèm với nhãn thời gian T  B chỉ chấp nhận thông điệp (chứa khóa phiên Ks) ở bước 3 nếu giá trị của nhãn thời gian T đủ gần với thời gian hiện hành của B, bao gồm độ trễ mạng và sai số cho phép  Đồng hồ của các bên tham gia liên lạc phải được đồng bộ hóa với nhau |  |
| Lưu ý | Các giao thức trên chỉ áp dụng cho trường hợp các bên tham gia liên lạc đồng thời online trên mạng (ví dụ dịch vụ Chat)  Nếu một bên tham gia liên lạc không online (ví dụ dịch vụ Email) thì cần có giải pháp khác |  |  |
| TH A,B k đồng thời trực tuyến đc(Chứng thực 1 chiều) cho email | 1.A → KDC: *ID*A||*ID*B||*N*1  2.KDC → A: E(*K*a, [*K*s||*ID*B||*N*1||E(*K*b, [*K*s||*ID*A])])  3.A → B: E(*K*b, [*K*s||*ID*A])||E(*K*s, *M*) |  | Phương pháp này không sử dụng nhãn thời gian T nên vẫn có nguy cơ bị tấn công nhại.  Tuy nhiên, việc xử lý email thường không tức thời, nên người nhận B chủ yếu dùng khoá phiên Ks để giải mã thông điệp M, chứ không dùng Ks để tiếp tục giao tiếp với A. |
| Dùng mã hóa công khai(của Denning) | Giữa hai bên liên lạc A và B cần có một bên thứ ba gọi là AS (Authentication Server – Server chứng thực)  AS không sinh ra khoá phiên Ks mà sẽ đưa ra “chứng chỉ” khoá công khai  Khóa phiên được chọn và mã hóa bởi A  1. A →AS: *IDA*||*IDB*  2. AS→ A: E(*PRas*, [*IDA*||*PUa*||*T*])||E(*PRas*, [*IDB*||*PUb*||*T*])  3. A→ B: E(*PRas*, [*IDA*||*PUa*||*T*])||E(*PRas*, [*IDB*||*PUb*||*T*])||E(*PUb*, E(*PRa*, [*Ks*||*T*])) | AS sinh ra chứng chỉ khoá công khai (chứa khoá công khai của người dùng), mỗi chứng chỉ chỉ có hiệu lực trong khoảng thời gian T  Khi A nhận được chứng chỉ do AS gửi, A sẽ biết được khoá công khai của B, và dùng nó để chuyển giao khoá phiên Ks cho B  Khoá phiên được mã hoá 2 lần: Lần 1 bởi PRa để chứng thực, lần 2 bởi PUb để giữ bí mật |  |