**LÝ THUYẾT**

**AN TOÀN BẢO MẬT THÔNG TIN - CT204**

**&-&**

1. **Mật mã đối xứng:**

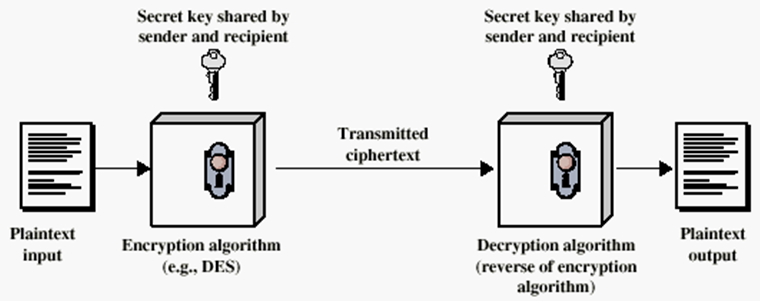
- 4 tiêu chí attt:

+ Thông tin tin cậy: Bí mật, Toàn vẹn.

+ Đối tác tin cậy: Chứng thực, không thoái thác.

- Bản rõ: Dữ liệu ban đầu. Bản mật (Ciphertext): Dữ liệu được mã hóa. Bản mật được giải mật (Decrypttext).

- Mô hình tạo mật mã:



- Mục tiêu: Tạo bản mật có phân bố bit hoàn toàn ngẫu nhiên.

- Chỉ có thể đoán khóa = Vét cạn.

- AES:

+ Đơn vị dữ liệu: 1 byte = 8 bit.

+ Từ mã: W = 4 byte.

+ Bản rõ: P = Nb \* W là 1 khối dữ liệu.

++ Nb: Số từ mã.

++ AES lấy Nb = 4 => P = 16 byte.

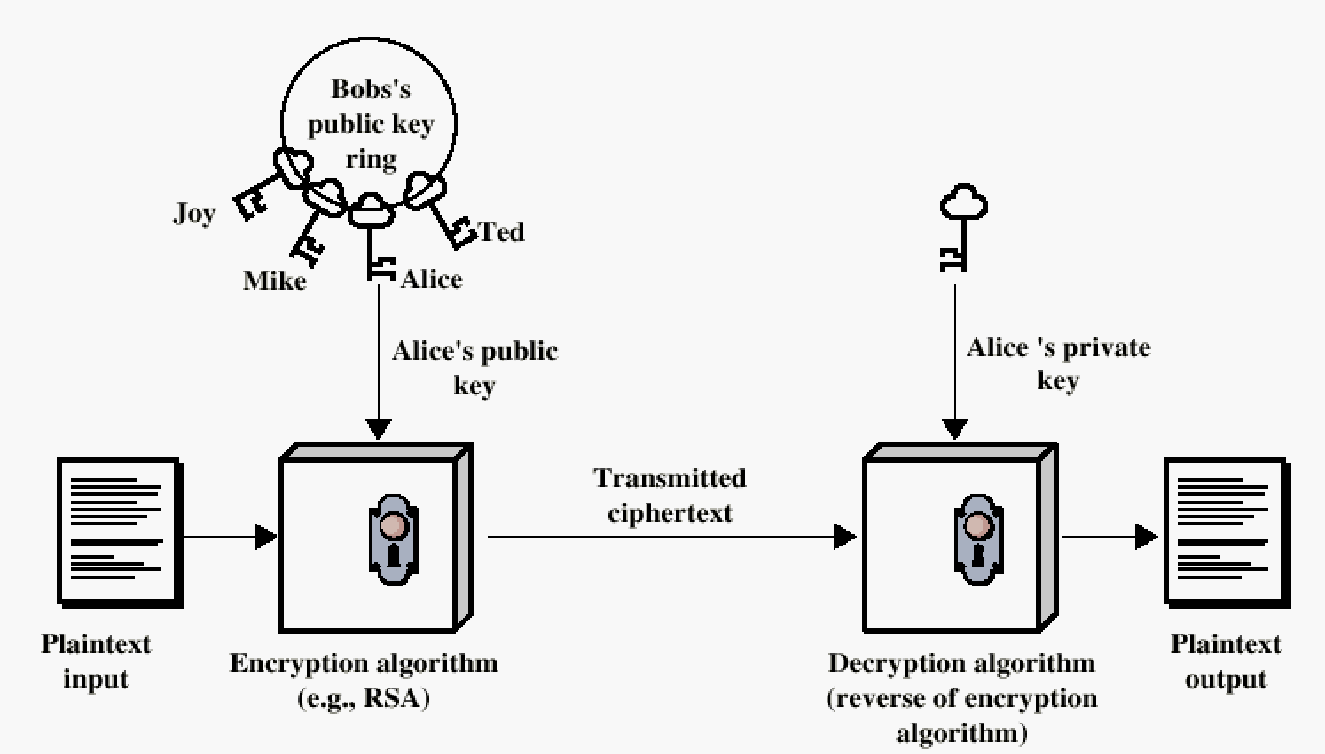
+ Ma trận trạng thái: (Trên xuống dưới, trái qua phải).

+ Vòng xử lí: Thay đổi trạng thái. Một vòng tương ứng với một **khóa phụ**. => Biến đổi ma trận trạng thái qua nhiều vòng để đạt trạng thái **Ngẫu nhiên hoàn toàn.**

+ Các phiên bản AES:

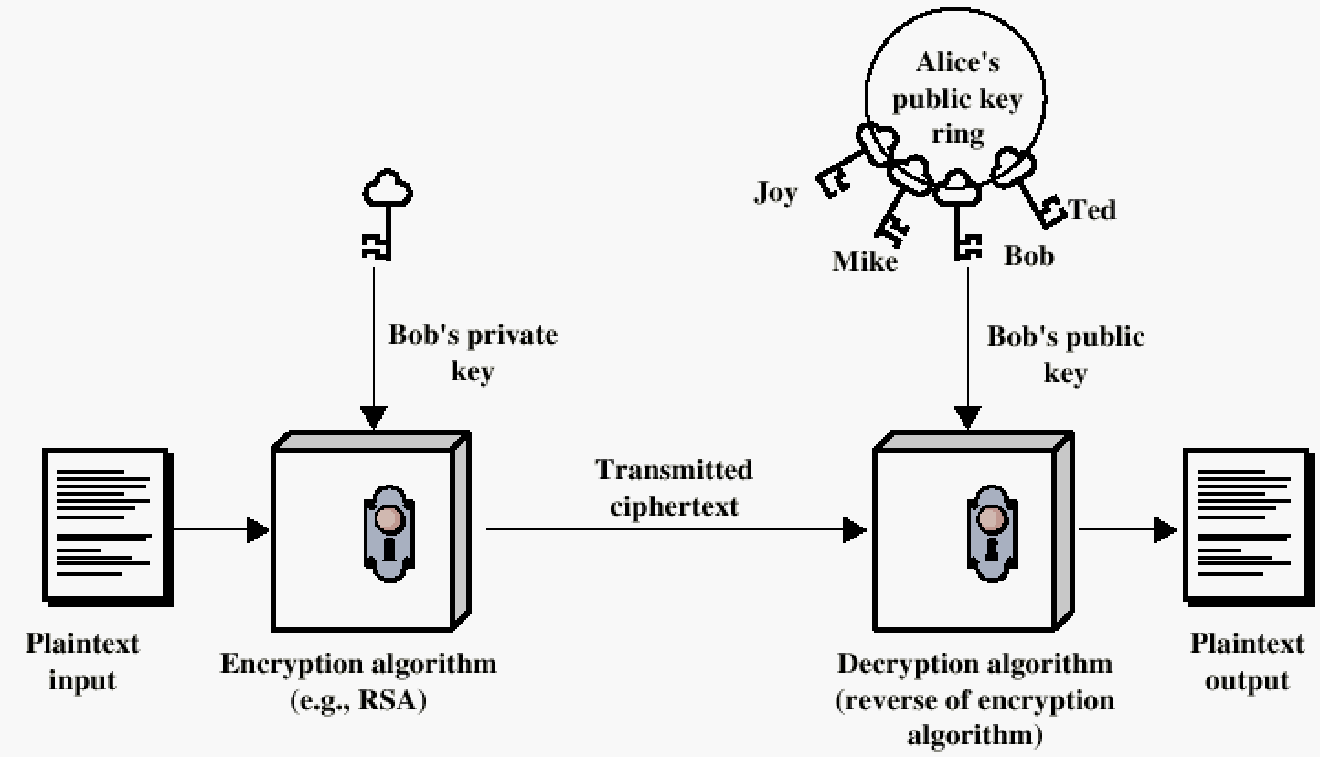
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  | **Parameters** | | | | **Variant** | **Nb** | **Nk** | **Nr** | | **AES-128** | 4 | 4 | 10 | | **AES-192** | 4 | 6 | 12 | | **AES-256** | 4 | 8 | 14 | | - Variant: Các phiên bản.  - Nb: Kích cỡ khối.  - Nk: Độ dài khóa.  - Nr: Số vòng xử lý. |

1. **Mật mã bất đối xứng:**



Hình 1

- Giải thích hình 1: Mật mã với khóa công khai và giải mật với khóa cá nhân. => Đảm bảo chỉ người nhận có thể giải mã thông tin. => Đảm bảo tính bí mật.



Hình 2

- Giải thích hình 2: Mật mã với khóa cá nhân và giải mật với khóa công khai. => Chống thoái thác (chữ ký số), đảm bảo tính xác thực của thông tin. => Đảm bảo xác thực, toàn vẹn, và chống thoái thác.

- RSA:

+ Chức năng chính: Trao đổi khóa, chữ ký điện tử.

+ Chức năng phụ: Tạo mật mã cho khối data nhỏ như mật mã khóa phiên.  
 + Nguyên lý tạo mật mã:

++ Bản rõ P là M.

++ Tạo bản mật với khóa công khai (n, e): C = Me mod n.

++ Giải mật mã với khóa cá nhân (n, d): M = Cd mod n.

+ Quá trình sinh khóa:

++ Chọn p và q: Hai số nguyên tố rất lớn.

++ Tính n = p \* q.

++ Tính phi-euler của n: Φ(n) = (p - 1)\*(q - 1).

++ Chọn e trong dãy: [1, Φ(n)] sao cho (Φ(n), e) nguyên tố cùng nhau, hay: gcd(Φ(n), e) = 1.

++ Tính d: d \* e = 1 mod Φ(n) (hay: d = e-1 mod Φ(n)).

++ Sinh khóa công khai Kpublic = {e, n}.

Sinh khóa cá nhân Kprivate = {d, n}.  
 **Ví dụ:** Sinh khóa với p = 7, q = 11:

- Tính n = 7\*11 = 77.

- Tính Φ(n) = (7 - 1)\*(11 - 1) = 60

- Chọn e trong [1, 60] để gcd(e, Φ(n)) = 1 => e = 13. (chọn một số nguyên tố kh trùng p, q)

- Tính d: d = e-1 mod Φ(n) = 13-1 mod 60 = 37.

+ Làm tay: Sử dụng Euclid mở rộng.

+ Bấm máy tính: (Phương trình gốc: 13x + 60y = 1. Bấm máy

tính f(x) = (1 - 13x) / 60. f(x) là số nguyên => x là nghịch đảo modulo của 13 theo modulo 60.)

- Khóa công khai: Kpub = {e, n} = {13, 77}; Kpri = {d, n} = {37, 77}.

1. **Hàm băm:**

- Là hàm một chiều. => Đo tính toàn vẹn của tập tin gốc.

- Giả sử file gốc x và giá trị hàm băm h = H(x), khi đó:

+ x có độ dài bất kỳ và H(x) có độ dài cố định.

+ Cho trước h: Rất khó (hầu như không thể) có thể tìm được x sao cho H(x) = h.

+ Đối với x cho trước, hầu như không thể tính được y để H(y) = H(x), y khác x.

- Các hàm băm: MD (MD2, MD4, và MD5 có 128 bit) và SHA (SHA-1 (160 bit), SHA-224, SHA-256, SHA-384 và SHA-512).

1. **Chữ ký số:**

- Là phương pháp chống thoái thác, tương tự chữ ký.

- Tạo chữ ký số:

+ Băm nội dung cần gửi.

+ Tạo mật mã bất đối xứng cho giá trị băm: Sử dụng khóa cá nhân.

- Kiểm tra chữ ký số.

+ P’: Nội dung kèm chữ ký số C của cá nhân có Kpub.

+ Băm P’ nhận được H’.

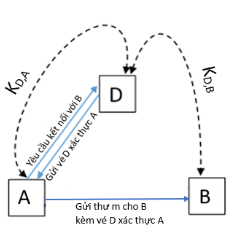
+ Giải mật mã bất đối xứng C với Kpub.

+ Đối chiếu H’ và H:

++ H’ == H: Xác nhận C là chữ ký của người có Kpub và P’ là bản gốc P.

++ Otherwise, bác bỏ P’.

1. **Vé xác thực:**



2

3

1

**Hình. Mô hình Sever-Client**

- D: Server Xác thực có tài khoản của client A và B. D đã gửi khóa mật chủ (Master Key).

+ KD, A cho A.

+ KD, B cho B.

- A và B đã đăng nhập thành công tại D.

- Vé “D xác thực A” cho B = EK D,B (KS, IDA) là mật mã AES với khóa

KD, B gồm:

+ Khóa phiên KS.

+ ID của A.

**\*\*Vé xác thực văn bản**

- A yêu cầu D cấp vé xác thực kết nối với B: E.

+ D gửi A:

++ Vé “D xác thực A” cho B.

++ Mật mã AES của khóa phiên KS và ID của A.

+ KS: Mật mã trao đổi tin giữa A và B trong thời gian quy định.

+ IDA -> B xác nhận A kèm thông tin gửi A: EK(D, A) (KS).

- A gửi văn bản m cho B:  
 + A giải mật khóa phiên KS.

+ A tạo EKs (m, IDA): Mật mã AES của m và ID của A với khóa phiên.

+ Gửi B:

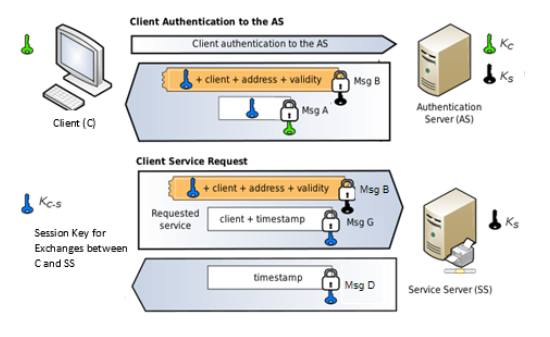
++ Thư mật mã EKs (m, IDA).

++ Vé “D xác thực A” cho B.

- B nhận gói tin từ A:

+ B giải mật E = EK(D, B) (KS, IDA) => KS, IDA.

+ B đối chiếu IDA từ m và IDA từ E.



- Các khóa:

+ KC: Khóa phiên giữa KH và Authentication Server.

+ KS: Khóa phiên giữa KH và Service Server.

+ Kc-S: Khóa phiên để trao đổi dữ liệu giữa KH và Service Server sau khi xác thực thành công, chỉ KH mới giải mã được.

- Quy trình:  
 1. KH gửi yêu cầu đến AS để y/c chứng thực danh tính.

1. AS gửi vé dịch vụ đã mã hóa và khóa phiên AS về cho KH (Msg B).
2. KH gửi vé và y/c dịch vụ đến SS (Msg G).
3. SS xác thực vé, trả lại dấu thời gian (Msg D), và phiên giao tiếp an toàn bắt đầu với khóa KC-S.
4. **Chứng thư số:**

- Xác thực đối tác tin cậy và trao đổi khóa phiên.

- Chức năng đặc biệt:

+ Thiết lập định danh: Xác nhận khóa pub của người có chứng thư.

+ Ấn định thẩm quyền: Thiết lập hoạt động được phép.

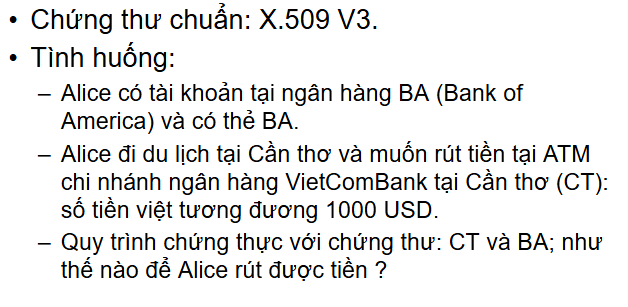
+ ATTT mật: Trao đổi khóa phiên để đọc tt mật.

- Phải có phần mềm dùng chung để tự sinh khóa công khai.

- Chứng thư chuẩn:

|  |
| --- |
| Content of an X.509 V3 Certificate |
| 1. Số phiên bản X.509 2. STT chứng thư 3. Tên và định danh duy nhất của tổ chức cấp chứng thư 4. Thời gian hiệu lực 5. Tên và định danh duy nhất của khách hàng 6. Định danh giải thuật chữ ký số 7. Thông tin về khóa công khai của KH 8. Đường dẫn chứng thực: Từ KH đến tổ chức cấp 9. Giá trị băm 1 -> 8 10. Kí tên |

- Tình huống:



+ Hồ sơ BA:

1. BA tạo cặp khóa pub và pri RSA.
2. BA xin công chứng khóa pub tại dịch vụ Công chứng uy tín.
3. Công chứng viên xác thực khóa pub BA và gửi hồ sơ -> Verisign.
4. Verisign sử dụng khóa pri của mình kí lên chứng thư để xác nhận khóa pub của BA -> Đáng tin.

+ Hồ sơ VCB: Tương tự của BA.

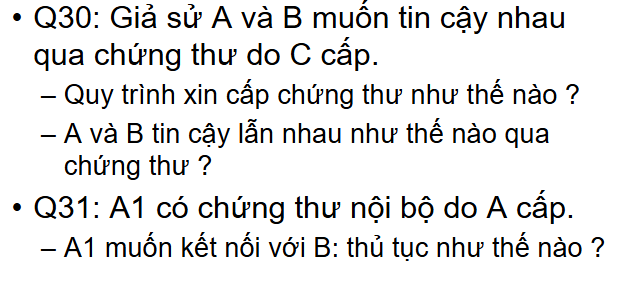
+ Hồ sơ của chi nhánh Cần Thơ:  
 1. Chi nhánh tạo cặp khóa Pub và pri.

1. VCB sử dụng khóa pri kí lên chứng thư để xác nhận khóa pub của CT đáng tin trong nội bộ VCB.

+ Rút tiền tại CT:

1. CT yêu cầu kết nối với BA với chứng thư của CT.
2. BA kiểm tra chứng thư của CT:
   1. Xác định đường dẫn của CT có VCB.
   2. Kiểm tra khóa pub của VB qua chứng thư của VB.
   3. Nếu tin cậy, BA tin vào khóa công khai của VB.
   4. Kiểm tra chữ ký số của VB trên CT.
3. Nếu chứng thư CT tin cậy, BA chấp nhận kết nối với CT.
4. BA tạo khóa phiên K và chuyển cho CT bằng RSA vs khóa pub của CT.
5. CT sử dụng K chuyển thông tin mật cho BA.
6. BA sử dụng khóa K giải mật thông báo và kiểm tra tính hợp lệ của hóa đơn.
7. BA chuyển số tiền từ tài khoản của Alice -> VCB (VCB sẽ thanh toán nội bộ với CT).
8. CT đồng ý cho Alice rút tiền.

- Kết nối qua chứng thư:



+ A và B xin cấp chứng thư bởi C theo quy trình như BA.

+ A và B trao đổi chứng thư với nhau.

+ A và B tin khóa pub của nhau.

+ A1 xin cấp chứng thư từ A do A ký vs khóa pri và có đường dẫn: A1 -> A -> C.

+ A1 gửi chứng thư cho B.

+ B kiểm tra chứng thư của A1 tương tự BA kiểm tra của CT (chi nhánh VCB).

1. **Phân loại cấp độ ATTT:**

- 3 loại thông tin:

+ L1: Cá nhận / Tập thể độc lập.

+ L2: Cộng đồng/Xã hội/Tập thể có cá nhân liên quan đến cộng đồng, xã hội.

+ L3: Quốc phòng, An ninh Quốc gia.

- 3 mức độ tổn hại:

+ M1: Tổn hại

+ M2: Tổn hại nghiêm trọng.

+ M3: Tổn hại rất nghiêm trọng.

- Tóm tắt 5 cấp độ:

+ L1 + M1 -> C1.

+ (L1+M2) và (L2+M1) → C2.

+ (L2+M2) và (L3+M1) → C3.

+ (L2+M3) và (L3+M2) → C4.

+ (L3+M3) → C5.

1. **Hồ sơ đề xuất cấp độ:**

- Các HTTT cần được thẩm định cấp độ:

+ HTTT được phê duyệt chủ trương xây dựng mới

+ HTTT đang vận hành nhưng chưa được phê duyệt cấp độ ATTT

+ HTTT đang vận hành và đã được phê duyệt cấp độ ATTT, nhưng được nâng cấp hoặc mở rộng.

- Quy trình thẩm định được quy định theo NĐ 85.

1. **Mô hình 4 lớp ATTT:**

- Lực lượng tại chỗ:

+ Cách làm: xây dựng một bộ phận chuyên trách về ATTT mạng chuyên: Ứng cứu sự cố; Tham mưu, tổ chức, đôn đốc việc tuân thủ quy định pháp luật về ATTT mạng.

+ Yêu cầu: Tối thiểu phải có 5 chuyên gia về ATTT mạng (có thể thuê ngoài).

- Lực lượng giám sát bảo vệ chuyên nghiệp:

+ Cách làm: Tự thực hiện hoặc thuê tổ chức ngoài có đủ năng F.

+ Yêu cầu: Giám sát 4 lớp skill: Mạng, ứng dụng, CSDL, và thiết bị đầu cuối.

- Lực lượng kiểm tra đánh giá độc lập:

+ Lựa chọn hoặc thuê tổ chức doanh nghiệp độc lập với tổ chức doanh nghiệp giám sát bảo vệ.

+ Yêu cầu:

++ HTTT cấp 3 trở lên: Kiểm tra đánh giá đột xuất theo yêu cầu.

++ HTTT 3 và 4: Kiểm tra dianh1 giá hàng năm.

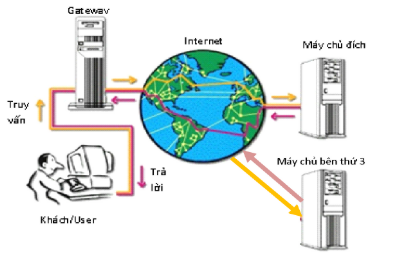
++ HTTT 5: Kiểm tra đánh giá 6 tháng / lần.

- Lực lượng quốc gia:

+ Tập trung thông tin và công nghệ về TT Giám sát An toàn mạng Quốc gia (NCSC).

+ Chia sẻ và kết nối thông tin với NCSC; Cung cấp dải IP public của các HTTT thuộc quyền quản lý cho NCSC.

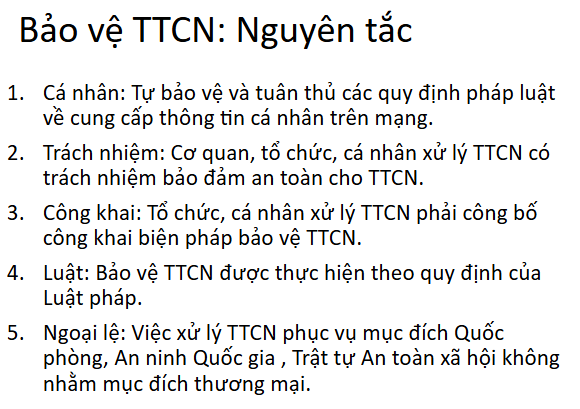
1. **Bên thứ 3:**

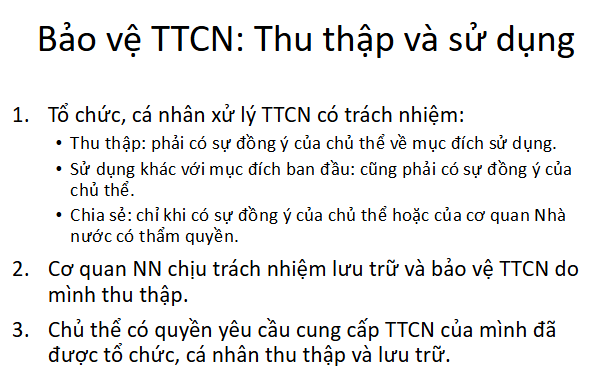


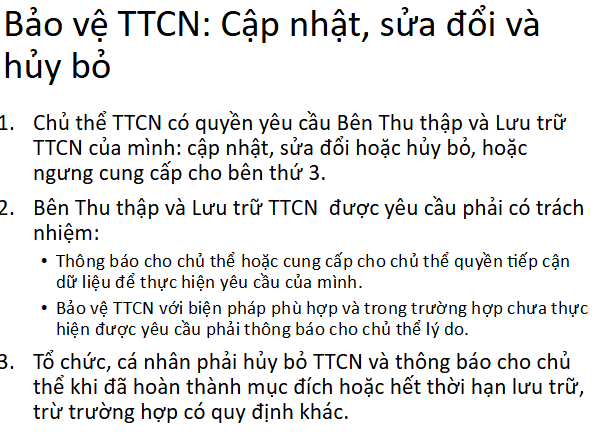
- Bên thứ 3: Uy tín, tin cậy và luôn kiểm soát được các KH của mình.

- KH của bên thứ 3 đều phải đăng ký tài khoản trước đó.

1. **Bảo vệ thông tin cá nhân (TTCN):**

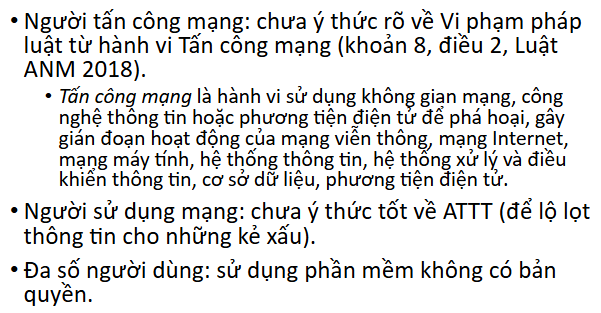




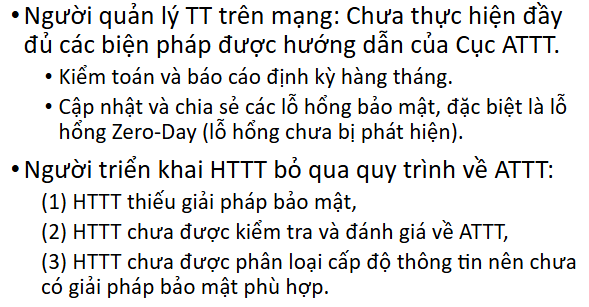


1. **Nguyên nhân mất ATTT:**

- Cá nhân:



- Quản lý:



1. **Chuyển đổi số: Tính tất yêu và thách thức (Trong tập)**

**ĐỀ THI ATBMTT**

Để tăng cường kỹ năng nhận biết về cấp độ An Toàn Thông tin (ATTT), tính bền vững trong phòng chống tấn công mạng và mối quan hệ tin cậy trong lưu thông sản phẩm nông nghiệp, Chính quyền Tỉnh X thực hiện một thử nghiệm : xây dựng Hệ thống thông tin (HTTT) nội bộ cho doanh nghiệp NTTS (Nuôi Trồng Thủy Sản). Mục tiêu của thử nghiệm là : Đánh giá khả năng đảm bảo ATTT của một doanh nghiệp.

**Câu 1: Đánh giá về ATTT cho HTTT của doanh nghiệp NTTS.**

* 1. Cấp độ 2 là cấp độ phù hợp cho HTTT của doanh nghiệp.
  2. Phân tích mực độ nguy hại nếu bị tấn công:
* **Ảnh hướng đến doanh nghiệp:** Làm rò rỉ, mất mát các thông tin quan trọng như dữ liệu sản phẩm, dữ liệu khách hàng, dliệu đối tác, dẫn đến tổn hại nghiêm trọng về mặt kinh tế và giảm sút uy tín.
* **Tác động đến lợi ích công cộng:** Nếu hệ thống có các dữ liệu về sản lượng và kế hoạch nuôi trồng bị thay đổi hoặc xâm nhập, việc cung cấp sản phẩm ra thị trường có thể bị ảnh hưởng, dẫn đến tổn hại lợi ích công cộng, như chuỗi cung ứng bị gián đoạn hoặc thiếu hụt nguồn cung.
* **Khả năng gián đoạn hoạt động sản xuất:** Nếu hệ thống bị chiếm quyền điều khiển hoặc bị phá hoại, các hoạt động vận hành sẽ bị ngưng trệ, gây thiệt hại nghiêm trọng trong quá trình khắc phục và phục hồi.
* **Thiệt hại tài chính:** Tốn chi phí khắc phục, bồi thường, mất doanh thu do ngừng hoạt động.
* **Không gây tổn hại tới Quốc phòng và An ninh quốc gia:** Tính chất của hệ thống doanh nghiệp NTTS chủ yếu liên quan đến sản xuất và kinh doanh thủy sản, không tác động trực tiếp đến an ninh quốc phòng.
* **Tác động lâu dài:** mất niềm tin từ đối tác, khác hàng.

**Câu 2: Chính quyền Tinh đề nghị doanh nghiệp NTTS thực hiện các nhiệm vụ sau : (1) thành lập nhóm ATTT, (2) hợp đồng với Viettel để giám sát vận hành HTTT, (3) lên kế hoạch kiểm tra định kỳ ATTT cho HTTT của doanh nghiệp, (4) nối kết với Trung ương để báo cáo các nguy cơ về mất ATTT.**

**2.1 Phân tích các nhiệm vụ của doanh nghiệp NTTS thuộc mô hình nào về ATTT. Trình bày mục tiêu của từng nhiệm vụ.**

**- Các nhiệm vụ của doanh nghiệp NTTS thuộc mô hình 4 lớp ATTT:**

* **(1) Thành lập nhóm ATTT**
  + Mô hình: Thuộc lớp 1: Lực lượng tại chỗ
  + Mục tiêu: Nhóm ATTT nội bộ chịu trách nhiệm triển khai và duy trì các biện pháp an ninh mạng tại doanh nghiệp. Họ đóng vai trò quan trọng trong việc giám sát hàng ngày, xử lý sự cố, và tham mưu, tổ chức, đôn đốc việc đảm bảo hệ thống tuân thủ các quy định về ATTT.
* **(2) Hợp đồng với Viettel để giám sát vận hành HTTT**
  + Mô hình: Thuộc lớp 2: Lực lượng giám sát bảo vệ chuyên nghiệp.
  + Mục tiêu: Viettel, với tư cách là một đơn vị giám sát bảo vệ chuyên nghiệp, cung cấp dịch vụ giám sát an ninh mạng 24/7, phát hiện và ứng phó nhanh chóng với các mối đe dọa tiềm ẩn. Điều này giúp doanh nghiệp đảm bảo hoạt động HTTT luôn được bảo vệ trước các cuộc tấn công phức tạp.
* **(3) Lên kế hoạch kiểm tra định kỳ ATTT cho HTTT của doanh nghiệp**
  + Mô hình: Thuộc lớp 3: Lực lượng kiểm tra đánh giá độc lập.
  + Mục tiêu: Việc kiểm tra định kỳ giúp phát hiện sớm các lỗ hổng trong hệ thống, đánh giá hiệu quả của các biện pháp bảo vệ hiện có và đề xuất các biện pháp cải tiến. Việc này giúp duy trì tính sẵn sàng và an toàn của hệ thống.
* **(4) Nối kết với Trung ương để báo cáo các nguy cơ về mất ATTT**
  + Mô hình: Thuộc lớp 4: Lực lượng quốc gia.
  + Mục tiêu: Việc kết nối với Trung ương để chia sẻ thông tin và báo cáo các nguy cơ giúp doanh nghiệp NTTS có thể nhận được cảnh báo và hướng dẫn kịp thời từ cơ quan an ninh mạng quốc gia. Điều này tăng cường khả năng phòng thủ và giảm thiếu tác động của các sự cố an ninh thông tin trên phạm vị lớn.

**2.2 Nhóm ATTT của doanh nghiệp có các nhiệm vụ cụ thể sau:**

* Ứng cứu và xử lý sự cố.
* Giám sát an toàn thông tin.
* Tham mưu cho lãnh đạo.
* Tổ chức và triển khai các biện pháp bảo vệ.
* Đôn đốc và đảm bảo tuân thủ pháp luật.
* Đào tạo và nâng cao nhận thức.
* Báo cáo và liên kết với các cơ quan quản lý.

**Câu 3: Cấp Chứng thư.**

**Doanh nghiệp NTTS cần các đối tác tin cậy trong cung ứng sản phẩm nông nghiệp cũng như tiêu thụ sản phẩm thủy sản. Giả sử doanh nghiệp NTTS cần tiêu thụ sản phẩm của mình thông qua đối tác A.**

**3.1 Doanh nghiệp NTTS và đối tác cần có chứng thư từ Cục ATTT. Vậy quy trình cấp chứng thư cho doanh nghiệp NTTS phải dựa trên điều kiện nào ? Tại sao**

* **Dựa trên điều kiện:** 
  + Xác minh danh tính và tính hợp pháp của doanh nghiệp.
  + Tạo cặp khóa công khai và khóa cá nhân.
  + Nộp hồ sơ và yêu cầu cấp chứng thư.
  + Kiểm tra và xác minh của Cục ATTT.
  + Phí cấp chứng thư và các cam kết tuân thủ.
* **Tại vì:**
  + Nó đảm bảo độ tin cậy cao và đáp ứng tiêu chuẩn bảo mật cần thiết.
  + Đảm bảo tính an toàn và tính toàn vẹn của giao dịch giữa doanh nghiệp NTTS và đối tác.

**3.2 Trong quy trình lập hồ sơ Chứng thư có bước Sinh khóa công khai RSA. Tính khóa công khai nếu p = 7 và q = 11.**

- Tính khóa công khai là Tìm e,n.

+ Tính n = p\*q = 7 \* 11 = 77

+ Tính phi-Euler ϕ(n) = (p-1)\*(q-1) = (7-1)\*(11-1) = 60

+ Chọn 1 < e < ϕ(n) sao cho gcd(ϕ(n),e) = 1: (e là số nguyên tố)

+ GCD(60,e) = 1 -> Chọn e = 17

* Khóa công khai (e,n) là (3, 77) hoặc (17,77)

+ Tính d: d\*e = 1 (hay d = e^-1 mod ϕ(n))

d\*17 = 1 (mod 60)

17 \* d – 60 \* k = 1

Chia 60 cho 17, tìm dư

60 = 3 \* 17 + 9

17 = 1 \* 9 + 8

9 = 1 \* 8 + 1

8 = 8 \* 1 + 0

1 = 9 – 1 \* 8

Thay 8 = 17 – 1 \* 9 vào, ta có

1 = 9 – 1 \* (17 – 1 \* 9) = 2 \* 9 – 1 \* 17

Thay 9 = 60 – 3 \* 17 vào, ta có

1=2 \* (60 – 3 \* 17) – 1 \* 17= 2 \* 60 – 7 \* 17

* + - d = - 7

Vì d là số nguyên dương, ta cộng thêm 60 => d = 53

* Khóa riêng (d,n) là (53, 77)

**VD: Hiệp hội Du lịch là Tổ chức liên kết các công ty Du lịch trong cả nước hướng tới mục tiêu chia sẻ thông tin du lịch ở mọi nơi và được phép cấp Chứng thư Du lịch cho khách hàng của mình.**

**Chứng thư Du lịch có thể giúp người có thẻ tìm Khách sạn, Nhà hàng, Điểm du lịch, Thuê/ Gọi xe dịch vụ hoặc tìm Hướng dẫn viên online với giá ưu đãi và thanh toán hoặc ghi nợ không lãi suất có thời hạn một cách dễ dàng.**

**Hiệp hội Du lịch sở hữu một phần mềm riêng có tên «Du lịch chất » và đã phân phối cho khách hàng trên các App Store và Google Play.**

**Yêu cầu:**

1. **Cấp Chứng Thư X.509 V3. Giả sử Công ty A là một doanh nghiệp Khách sạn muốn có Chứng thư Du lịch (X.509 V3) của Hiệp hội. Việc đầu tiên là Công ty A phải công chứng Khóa Công khai của mình.**

**- Liệt kê các bước thực hiện công chứng Khóa Công khai một cách tuần tự và giải thích ý nghĩa mỗi bước:**

Bước 1: Công ty A phải tạo Khóa công khai và khóa cá nhân cho mình. Giải thích: Đây là bước nền tảng để Công ty A đảm bảo an toàn trong giao tiếp, đồng thời chuẩn bị cho việc cấp chứng thư số. Ngoài ra, Khóa cá nhân (Private Key): Được giữ bí mật, dùng để ký số và bảo vệ dữ liệu.Khóa công khai (Public Key): Được chia sẻ với các bên thứ ba, dùng để xác thực và mã hóa thông tin.

Bước 2: Hiệp hội Du lịch sử dụng khóa cá nhân của mình ký lên chứng thư X.509 V3 để xác nhận Khóa công khai của Công ty A: Khóa Công khai của Công ty A đáng tin trong nội bộ Hiệp hội Du lịch. Giải thích: Việc Hiệp hội Du lịch ký chứng thư số bằng khóa cá nhân của mình đảm bảo rằng: Khóa công khai của công ty A là hợp lệ và có thể sử dụng trong các giao dịch an toàn. Chứng thư số X.509 V3 chứa thông tin chi tiết, giúp bên thứ ba xác thực danh tính Công ty A một cách tự động và đáng tin cậy.

Cách 2:

**Các bước công chứng Khóa Công khai (X.509 V3):**

1. **Công ty A tạo cặp khóa cá nhân và khóa công khai:**
   * **Ý nghĩa:** Cặp khóa đảm bảo giao tiếp an toàn, với khóa cá nhân để bảo mật và khóa công khai để xác thực.
2. **Công ty A tạo yêu cầu chứng thực khóa công khai (CSR):**
   * **Ý nghĩa:** CSR chứa thông tin khóa công khai và danh tính Công ty A, gửi đến Hiệp hội Du lịch.
3. **Hiệp hội Du lịch xác minh thông tin trong CSR:**
   * **Ý nghĩa:** Đảm bảo Công ty A hợp lệ và đáng tin cậy.
4. **Hiệp hội Du lịch ký chứng thư X.509 V3 bằng khóa cá nhân của mình:**
   * **Ý nghĩa:** Chứng nhận khóa công khai của Công ty A là hợp lệ và được bảo chứng bởi Hiệp hội.
5. **Công ty A nhận chứng thư X.509 V3:**
   * **Ý nghĩa:** Chứng thư xác thực danh tính Công ty A, giúp thực hiện giao dịch an toàn.

**3.Cấp độ An toàn thông tin (ATTT).**

**Công ty A cần xây dựng Hệ thống Thông tin (HTTT) với các thông tin về thuê phòng, hướng dẫn du lịch, thuê xe và giới thiệu danh sách các Hướng dẫn viên du lịch và các dịch vụ khác của Khách sạn, trong đó có thông tin về khách hàng thuê phòng.**

* **Phân tích Cấp độ ATTT của HTTT này (cho phép biên độ là 2 cấp độ).**

Phân tích cấp độ ATTT sẽ dựa trên 3 Loại thông tin và 3 mức độ Tổn hại.

* + Loại 1: Cá nhân/ Tập thể độc lập đó là danh sách hướng dẫn viên và dịch vụ du lịch.
  + Loại 2 Cộng đồng/Xã hội/ Tập thể có cá nhân liên quan đến cộng đồng, xã hội là thông tin thuê phòng và khách hàng, bên cạnh đó là thông tin liên quan đến dịch vụ thuê xe.
  + Loại 3: Không có tồn tại vì nó không liên quan đến Quốc phòng, An ninh Quốc gia.
  + Mức độ 1: Có tổn hại nhẹ. VD: Lộ thông tin danh sách dịch vụ hoặc hướng dẫn viên gây tổn hại nhẹ đến uy tín công ty, nhưng không gây hậu quả nghiệm trọng.
  + Mức độ 2: Tổn hại nghiệm trọng. VD: Lộ thông tin khách hàng, đặc biệt dữ liệu thanh toán, có thể gây mất niềm tin và thiệt hại lớn hơn về kinh tế và danh tiếng.
  + Mức độ 3: Tổn hại rất nghiêm trọng. VD: Nếu toàn bộ hệ thống bị tấn công, có thể dẫn đến mất khả năng vận hành và thiệt hai nghiêm trong.
* Đề xuất cấp độ ATTT cho hệ thống của Công ty A là cấp độ 2. (L1 + M2) và (L2 + M1) -> C2. VD: Lộ thông tin khách thuê phòng hoặc hướng dẫn viên có thể gây tổn hại nghiêm trọng đến danh tiếng.
  + - Biên độ cho phép: C1 đến C3
      * C1: Trong trường hợp hệ thống chỉ xử lý dữ liệu đơn giản.
      * C3: Nếu có thông tin nhạy cảm.

1. **Xác thực Khóa Công khai**

**Giả sử khách hàng có thẻ Du lịch do Công ty Du lịch B cấp (khác Công ty A) và cả hai công ty này đã có chứng thư của nhau. Khách hàng thuê Hướng dẫn viên Du lịch của Cty A nhưng theo mức giá ưu đãi của Cty B, nên Cty B phải xác thực Khóa Công khai của Cty A để có thể đồng ý kết nối với Cty A.**

**- Phân tích các bước chính (không cần trình bày giải thuật) xác thực Khóa Công khai này.**

Bước 1: Công ty A phải gửi cho công ty B chứng thư của Công ty A

Bước 2: Công ty B kiểm tra: khóa công khai của công ty A là tin cậy

* + B Kiểm tra chữ ký của Hiệp hội du lịch trên chứng thư của Công ty A.

Bước 3: Nếu đúng, tin khóa công khai của Công ty A và chấp nhận kết nối.