**1. Anh/chị hãy giải thích tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?**

Đảm bảo an toàn cho thông tin và hệ thống thông tin là vô cùng quan trọng với nhiều lý do sau:

- Bảo vệ dữ liệu cá nhân: Thông tin cá nhân của cá nhân và tổ chức cần được bảo vệ để tránh việc lộ thông tin cá nhân, đặc biệt là trong các lĩnh vực như y tế, tài chính, luật pháp.

- Bảo vệ thông tin nhạy cảm: Nhiều tổ chức lưu trữ thông tin nhạy cảm như thông tin tài chính, kế hoạch kinh doanh, và sơ đồ vận hành. Nếu thông tin này bị rò rỉ, có thể gây ra thiệt hại về mặt tài chính hoặc danh tiếng.

- Bảo vệ khỏi tấn công mạng: Hệ thống thông tin thường là mục tiêu của các hacker và tin tặc muốn đánh cắp thông tin giúp ngăn chặn các cuộc tấn công mạng và giữ cho hệ thống hoạt động một cách trơn tru.

- Tuân thủ các quy định và luật pháp: Nhiều lĩnh vực có các quy định nghiệm ngặt về bảo vệ thông tin, chẳng hạn như GDPR ở Châu Âu hoặc HIPAA trong lĩnh vực y tế tại Hoa Kỳ. Tuân thủ các quy định này không chỉ là một nghĩa vụ pháp lý mà còn giúp xây dựng niềm tin từ phía khách hàng và đối tác.

- Bảo vệ trước mất mát dữ liệu: Mất mát dữ liệu có thể xảy ra từ các sự cố như lỗi phần cứng, lỗi phần mềm, hoặc tấn công malware. Đảm bảo an toàn thông tin giúp ngăn chặn hoặc giảm thiểu nguy cơ mất mát dữ liệu.

**2. Anh/chị hãy giải thích các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA?**

Mô hình CIA(Confidentiality, Integrity, Availability) là một trong những khái niệm cơ bản trong lĩnh vực bảo mật thông tin. Nó bao gồm ba thuộc tính chính mà mọi hệ thống thông tin cần phải đảm bảo để được coi là an toàn:

- Confidentiality(Tính bảo mật): Đảm bảo rằng thông tin chỉ có thể được truy cập và xem bởi những người có quyền truy cập. Các biện pháp bảo mật như mã hóa dữ liệu, xác thực và quản lý quyền truy cập được sử dụng để đảm bảo tính bảo mật của thông tin.

- Integrity(Tính chính xác): Bảo vệ khỏi sự sửa đổi trái phép hoặc không được ủy quyền cùa thông tin. Điều này đảm bảo rằng thông tin không bị thay đổi một cách không đáng kể, giữ cho nó đáng tin cậy và chính xác. Các biện pháp như kiểm tra tính toàn vẹn dữ liệu và chữ ký số được sử dụng để bảo vệ tính chính xác của thông tin.

- Availability(Tính khả dụng): Đảm bảo rằng thông tin có sẵn và có thể truy cập khi cần thiết cho những người được ủy quyền. Điều này đảm bảo rằng hệ thống thông tin luôn hoạt động và sẵn sàng phục vụ người dùng, tráng tình trạng bị tấn công từ chối dịch vụ (DDoS) hoặc các vấn đề kỹ thuật khác gây ra sự cố khả dụng.

**3. Anh chị hãy so sánh 2 loại phần mềm độc hại: virus và worm?**

Virus: là một loại phần mềm độc hại có khả năng tự sao chép bằng cách gắn kết vào các tập tin hoặc chương trình khác

Cách hoạt động: Virus thường cần sự can thiệp từ người dùng để lan truyền, ví dụ như thông qua mở tệp tin bị nhiễm virus hoặc cài đặt phần mềm chứa virus.

Đặc điểm: Virus có thể gây ra sự cố bảo mật như xóa dữ liệu, thay đổi hoặc mã hóa tập tin, lây nhiễm các hệ thống khác qua các tập tin được chia sẻ.

Worm: là một loại phần mềm độc hại có khả năng tự phát tán và lây qua mạng máy tính mà không cần sự can thiệp của người dùng.

Cách hoạt động: Worm thường sử dụng các lỗ hổng bảo mật trong hệ điều hành hoặc các ứng dụng để tự động sao chép và lây nhiễm sang các máy tính khác mà không cần sự tương tác của người dùng.

Đặc điểm: Worm có thể lan rộng rất nhanh trong mạng máy tính, gây ra tình trạng quá tải hệ thống, giảm hiệu suất mạng, hoặc thậm chí gây ra các cuộc tấn công phủ định dịch vụ (DoS) trên quy mô lớn.

So sánh:

Phương thức lây lan: Virus cần sự can thiệp từ người dùng hoặc cơ chế lây nhiễm thông qua các tập tin, trong khi worm có khả năng tự động lây lan qua mạng mà không cần sự can thiệp.

Tốc độ lây lan: Worm thường lan rộng nhanh hơn virus do khả năng tự động và không cần sự tương tác của người dùng.

Tác hại: Cả virus và worm đều có thể gây ra thiệt hại nghiêm trọng cho hệ thống thông tin, nhưng worm có thể lan rộng và gây ra tác hại rộng lớn hơn do tính tự động lây lan của nó

**4. Anh/chị hãy trình bày sơ đồ phân loại và cách phòng chống các phần mềm độc hại?**

Sơ đồ phân loại các phần mềm độc hại

- Theo cách thức lây lan:

+ Virus: Sử dụng các tập tin hoặc chương trình để tự sao chép và lây nhiễm qua các hoạt động của người dùng

+ Worm: Lây lan qua mạng máy tính mà không cần sự can thiệp của người dùng, sử dụng các lỗ hổng bảo mật của hệ thống

- Theo mục đích tấn công:

+ Malware: Phần mềm độc hại tổng quát, bao gồm virus, worm, trojan, spyware, ransomware, ...

+ Spyware: Thu thập thông tin người dùng mà không được sự cho phép của họ

+ Ransomware: Mã hóa dữ liệu của người dùng và yêu cầu tiền chuộc để giải mã

+ Trojan Horse: Phần mềm giả mạo, thường làm người dùng tin tưởng và cài đặt, sau đó có thể cho phép kẻ tấn công kiểm soát từ xa.

- Theo vùng tấn công:

+ Client-side: Tấn công từ phía người dùng, thông qua mail, web, ...

+ Server-side: Tấn công trực tiếp vào hệ thống máy chủ

Các biện pháp phòng chống:

1. Phòng chống trước khi bị lây nhiễm

- Cập nhật hệ thống và phần mềm: Đảm bảo các bản vá bảo mật mới nhất được cài đặt để bảo vệ khỏi các lỗ hổng bảo mật.

- Sử dụng phần mềm bảo mật: Cài đặt và duy trì phần mềm diệt virus, tường lửa và các công cụ bảo vệ khác để ngăn chặn và phát hiện sớm các phần mềm độc hại

- Chỉ tải xuống từ nguồn tin cậy: Tránh tải xuống phần mềm từ các nguồn không tin cậy hoặc không được kiểm tra.

2. Phát hiện và xử lý sau khi bị nhiễm

- Quét và xóa: Thực hiện quét hệ thống bằng phần mềm diệt virus để phát hiện và loại bỏ phần mềm độc hại

- Khôi phục dữ liệu từ sao lưu: Đảm bảo có sao lưu dữ liệu thường xuyên để có thể khôi phục khi bị mã hóa bởi ransomware

- Ngắt kết nối mạng: Điều này có thể ngăn chặn worm hoặc ransomware khỏi lan ra ngoài và gây thiệt hại lớn hơn

**5. Anh/chị hãy giải thích các lớp phòng vệ điển hình trong mô hình bảo đảm an toàn hệ thống thông tin có chiều sâu Defence in Depth?**

- Lớp phòng vệ vật lý:

+ Đảm bảo an toàn của các thành phần vật lý của hệ thống như máy chủ, thiết bị mạng, phòng máy, và các trung tâm dữ liệu

+ Bao gồm việc áp dụng các biện pháp như kiểm soát truy cập vật lý, hệ thống camera giám sát, hệ thống báo động, và các biện pháp bảo vệ vật lý khác

- Lớp phòng vệ mạng:

+ Bảo vệ dữ liệu và hệ thống thông qua các biện pháp như tường lửa, IDS/IPS, VPN, và các kỹ thuật chống phá hoại mạng

- Lớp phòng vệ hệ điều hành và ứng dụng:

+ Bảo vệ hệ điều hành và các ứng dụng được triển khai trên hệ thống

+ Bao gồm các biện pháp như cập nhật hệ điều hành và ứng dụng, cấu hình an toàn, giám sát và bảo vệ chống lại các lỗ hổng bảo mật phần mềm

- Lớp phòng vệ dữ liệu:

+ Đảm bảo an toàn cho dữ liệu quan trọng của tổ chức

+ Bao gồm các biện pháp mã hóa dữ liệu, giám sát và phát hiện xâm nhập vào dữ liệu, quản lý quyền truy cập dữ liệu, và các chiến lược sao lưu và phục hồi dữ liệu

- Lớp phòng vệ người dùng:

+ Tăng cường nhân thức và kiến thức về bảo mật người dùng hệ thống thông qua đào tạo, chương trình giáo dục về bảo mật thông tin

+ Giúp người dùng nhận biết các mối đe dọa tiềm ẩn và hành vi không an toàn, từ đó giảm thiểu nguy cơ bảo mật do hành vi người dùng

**6. Anh/chị hãy giải thích tấn công giả mạo địa chỉ và nêu cách phòng chống?**

**Tấn công giả mạo địa chỉ và cách phòng chống**

* **Tấn công giả mạo địa chỉ (IP Spoofing):**

**+ Định nghĩa:** Tấn công giả mạo địa chỉ là kỹ thuật tấn công trong đó kẻ tấn công thay đổi địa chỉ nguồn trong các gói tin IP để che giấu danh tính thật của mình hoặc để thực hiện các cuộc tấn công từ chối dịch vụ (DoS). Kẻ tấn công có thể gửi các gói tin với địa chỉ IP nguồn giả mạo để trông như chúng đến từ một nguồn đáng tin cậy.

**+ Mục đích:** Che giấu danh tính thật của kẻ tấn công, vượt qua các biện pháp kiểm tra bảo mật dựa trên IP, hoặc làm cho các gói tin phản hồi đến một địa chỉ khác. Các cuộc tấn công DoS thường sử dụng giả mạo địa chỉ để gửi lượng lớn gói tin đến một mục tiêu, làm cho hệ thống không thể đáp ứng được các yêu cầu hợp pháp.

**- Cách phòng chống tấn công giả mạo địa chỉ:**

1. **Lọc gói tin (Packet Filtering):**
   * **Ingress Filtering:** Các bộ định tuyến hoặc tường lửa ở rìa mạng nên được cấu hình để loại bỏ các gói tin có địa chỉ IP nguồn không hợp lệ hoặc không thuộc dải địa chỉ IP được phép.
   * **Egress Filtering:** Các bộ định tuyến hoặc tường lửa nội bộ nên kiểm tra và loại bỏ các gói tin gửi ra ngoài với địa chỉ IP nguồn không hợp lệ hoặc không thuộc mạng nội bộ.
2. **Sử dụng ACLs (Access Control Lists):**
   * Cấu hình ACLs trên các bộ định tuyến và tường lửa để chỉ cho phép lưu lượng mạng từ các địa chỉ IP nguồn hợp lệ và chặn các địa chỉ IP giả mạo.
3. **Áp dụng BCP 38/BCP 84:**
   * Best Current Practice 38 (BCP 38) và BCP 84 cung cấp hướng dẫn về việc lọc gói tin để ngăn chặn các gói tin giả mạo rời khỏi mạng.
4. **Xác thực IP (IP Authentication):**
   * Sử dụng các phương pháp xác thực IP để đảm bảo rằng các gói tin đến từ các nguồn đáng tin cậy. Ví dụ, IPSec có thể được sử dụng để mã hóa và xác thực lưu lượng IP, đảm bảo tính toàn vẹn và xác thực nguồn gốc.
5. **Kiểm tra tính hợp lệ của gói tin (Packet Validation):**
   * Sử dụng các công cụ và hệ thống phát hiện xâm nhập (IDS) hoặc hệ thống ngăn chặn xâm nhập (IPS) để giám sát và kiểm tra tính hợp lệ của các gói tin, phát hiện các gói tin có địa chỉ IP giả mạo.
6. **Sử dụng công nghệ chống giả mạo (Anti-Spoofing Technology):**
   * Sử dụng các công cụ và phần mềm chống giả mạo để phát hiện và ngăn chặn các cuộc tấn công giả mạo địa chỉ. Các giải pháp này thường kết hợp nhiều kỹ thuật như phân tích hành vi, lọc gói tin và kiểm tra tính hợp lệ của gói tin.
7. **Đào tạo và nhận thức bảo mật:**
   * Đào tạo nhân viên về nhận thức bảo mật và các dấu hiệu của cuộc tấn công giả mạo địa chỉ để họ có thể phản ứng kịp thời và thông báo cho đội ngũ bảo mật khi phát hiện hoạt động đáng ngờ.

**7. Anh/chị hãy giải thích về các dạng tấn công vào mật khẩu và nêu cách phòng tấn công vào mật khẩu?**

**Các dạng tấn công vào mật khẩu và cách phòng chống**

**Các dạng tấn công vào mật khẩu:**

1. **Brute Force Attack (Tấn công vét cạn):**
   * **Mô tả:** Kẻ tấn công thử mọi khả năng kết hợp của các ký tự cho đến khi tìm ra mật khẩu đúng.
   * **Hạn chế:** Tốn nhiều thời gian và tài nguyên, nhưng có thể thành công nếu mật khẩu ngắn hoặc đơn giản.
2. **Dictionary Attack (Tấn công từ điển):**
   * **Mô tả:** Kẻ tấn công sử dụng một danh sách các mật khẩu phổ biến hoặc các từ thông dụng để thử.
   * **Hạn chế:** Hiệu quả với các mật khẩu đơn giản hoặc phổ biến, nhưng không hiệu quả với mật khẩu phức tạp hoặc ngẫu nhiên.
3. **Phishing (Lừa đảo):**
   * **Mô tả:** Kẻ tấn công lừa người dùng cung cấp mật khẩu qua email hoặc trang web giả mạo.
   * **Hạn chế:** Dựa vào việc lừa người dùng, không yêu cầu nhiều kỹ thuật phức tạp.
4. **Keylogging:**
   * **Mô tả:** Kẻ tấn công sử dụng phần mềm hoặc phần cứng để ghi lại các phím bấm của người dùng, từ đó thu thập mật khẩu.
   * **Hạn chế:** Cần cài đặt phần mềm hoặc thiết bị keylogger trên máy tính của nạn nhân.
5. **Social Engineering (Kỹ thuật xã hội):**
   * **Mô tả:** Kẻ tấn công sử dụng các kỹ thuật tâm lý để lừa người dùng tiết lộ mật khẩu.
   * **Hạn chế:** Dựa vào việc khai thác lòng tin hoặc sự thiếu cảnh giác của người dùng.
6. **Credential Stuffing:**
   * **Mô tả:** Kẻ tấn công sử dụng thông tin đăng nhập bị lộ từ các vụ vi phạm dữ liệu khác để thử đăng nhập vào các dịch vụ khác.
   * **Hạn chế:** Hiệu quả nếu người dùng tái sử dụng mật khẩu trên nhiều dịch vụ.
7. **Rainbow Table Attack:**
   * **Mô tả:** Kẻ tấn công sử dụng bảng tra cứu (rainbow table) chứa các giá trị băm (hash) và mật khẩu tương ứng để giải mã mật khẩu.
   * **Hạn chế:** Yêu cầu nhiều tài nguyên và có thể bị hạn chế bằng cách sử dụng các kỹ thuật bảo vệ như salting.

**Cách phòng chống tấn công vào mật khẩu:**

1. **Sử dụng mật khẩu mạnh và phức tạp:**
   * **Mô tả:** Sử dụng mật khẩu dài, chứa sự kết hợp của chữ hoa, chữ thường, số và ký tự đặc biệt.
   * **Lợi ích:** Tăng độ khó cho các cuộc tấn công brute force và dictionary.
2. **Sử dụng xác thực hai yếu tố (2FA):**
   * **Mô tả:** Yêu cầu một yếu tố xác thực bổ sung ngoài mật khẩu, chẳng hạn như mã OTP (One-Time Password) hoặc xác thực qua ứng dụng.
   * **Lợi ích:** Tăng cường bảo mật và giảm thiểu rủi ro từ các cuộc tấn công vào mật khẩu.
3. **Thường xuyên thay đổi mật khẩu:**
   * **Mô tả:** Thay đổi mật khẩu định kỳ để giảm thiểu nguy cơ mật khẩu bị lộ hoặc bị đánh cắp.
   * **Lợi ích:** Giảm khả năng kẻ tấn công sử dụng mật khẩu bị lộ.
4. **Không sử dụng cùng một mật khẩu cho nhiều tài khoản:**
   * **Mô tả:** Sử dụng mật khẩu riêng biệt cho mỗi tài khoản để ngăn chặn việc một mật khẩu bị lộ gây ảnh hưởng đến nhiều tài khoản.
   * **Lợi ích:** Giảm thiểu rủi ro từ các cuộc tấn công credential stuffing.
5. **Sử dụng phần mềm quản lý mật khẩu:**
   * **Mô tả:** Sử dụng các công cụ quản lý mật khẩu để tạo, lưu trữ và quản lý mật khẩu phức tạp.
   * **Lợi ích:** Giúp người dùng dễ dàng sử dụng mật khẩu mạnh và không phải nhớ nhiều mật khẩu.
6. **Đào tạo nhận thức bảo mật:**
   * **Mô tả:** Đào tạo người dùng về các mối đe dọa bảo mật, cách nhận biết các cuộc tấn công phishing và cách bảo vệ mật khẩu.
   * **Lợi ích:** Tăng cường khả năng phát hiện và phản ứng kịp thời trước các cuộc tấn công.
7. **Sử dụng các biện pháp bảo vệ bổ sung:**
   * **Mô tả:** Sử dụng các công cụ và kỹ thuật bảo vệ như salting và hashing mật khẩu trong cơ sở dữ liệu.
   * **Lợi ích:** Tăng cường bảo mật và giảm thiểu rủi ro từ các cuộc tấn công rainbow table.

Bằng cách áp dụng những biện pháp này, các tổ chức và cá nhân có thể giảm thiểu rủi ro từ các cuộc tấn công vào mật khẩu và bảo vệ thông tin cá nhân cũng như tài sản số của mình.

1. **Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên bất thường của hệ thống IDS/IPS?**

Hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) dựa trên bất thường sử dụng cơ chế phát hiện xâm nhập không dựa trên các mẫu tấn công đã biết trước mà dựa trên việc nhận diện các hành vi, hoạt động bất thường trong hệ thống mạng hoặc hệ thống máy tính. Dưới đây là các bước cơ bản trong cơ chế này:

1. **Thu thập dữ liệu**: IDS/IPS thu thập dữ liệu từ các nguồn khác nhau như lưu lượng mạng, nhật ký hệ thống, hoạt động của ứng dụng, và các sự kiện khác trong hệ thống.
2. **Xây dựng mô hình bình thường**: Hệ thống sẽ học và xây dựng một mô hình về hành vi bình thường của hệ thống dựa trên dữ liệu thu thập. Điều này có thể bao gồm lưu lượng mạng bình thường, mức sử dụng CPU, bộ nhớ, và các thông số khác của hệ thống.
3. **Giám sát và so sánh**: Sau khi mô hình bình thường được xây dựng, hệ thống sẽ giám sát liên tục các hoạt động hiện tại và so sánh chúng với mô hình bình thường.
4. **Phát hiện bất thường**: Nếu phát hiện các hành vi, hoạt động hoặc các thông số nào đó khác biệt so với mô hình bình thường vượt qua ngưỡng nhất định, hệ thống sẽ coi đó là bất thường và có thể là dấu hiệu của một cuộc tấn công hoặc xâm nhập.
5. **Cảnh báo và phản ứng**: Khi phát hiện bất thường, IDS sẽ tạo ra cảnh báo để quản trị viên hệ thống biết và có biện pháp xử lý. Với IPS, hệ thống có thể tự động thực hiện các hành động để ngăn chặn các hoạt động bất thường này, chẳng hạn như chặn gói tin, ngắt kết nối hoặc cô lập hệ thống bị nghi ngờ.

**Ưu điểm và Nhược điểm**

**Ưu điểm**:

* **Phát hiện các mối đe dọa mới**: Vì không dựa trên các mẫu tấn công đã biết, hệ thống có thể phát hiện các cuộc tấn công mới chưa được nhận diện.
* **Phát hiện các hành vi nội gián**: Có thể phát hiện các hoạt động bất thường từ bên trong hệ thống mà các phương pháp dựa trên mẫu có thể bỏ qua.

**Nhược điểm**:

* **Tỷ lệ cảnh báo sai cao**: Các thay đổi hợp pháp trong hoạt động của hệ thống cũng có thể được coi là bất thường, dẫn đến nhiều cảnh báo sai.
* **Yêu cầu thời gian học**: Cần thời gian để xây dựng mô hình bình thường, và trong thời gian này, hệ thống có thể không hoạt động hiệu quả.
* **Phức tạp và tốn tài nguyên**: Yêu cầu tài nguyên tính toán và lưu trữ lớn để phân tích và so sánh dữ liệu liên tục.

**Kết luận**

Hệ thống phát hiện xâm nhập và ngăn chặn xâm nhập dựa trên bất thường là một công cụ mạnh mẽ trong việc bảo vệ hệ thống khỏi các cuộc tấn công mới và chưa biết. Tuy nhiên, để đạt được hiệu quả tối đa, cần kết hợp với các phương pháp bảo mật khác và cần quản trị viên có kinh nghiệm để xử lý các cảnh báo đúng cách.

**9. Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên chữ ký của hệ thống IDS/IPS?**

**Cơ chế phát hiện xâm nhập dựa trên chữ ký của hệ thống IDS/IPS**

**Hệ thống phát hiện xâm nhập (IDS - Intrusion Detection System) và hệ thống ngăn chặn xâm nhập (IPS - Intrusion Prevention System) dựa trên chữ ký:**

**1. Khái niệm:**

* **Phát hiện dựa trên chữ ký (Signature-Based Detection):** Là phương pháp phát hiện xâm nhập bằng cách so sánh lưu lượng mạng hoặc hành vi hệ thống với một tập hợp các mẫu chữ ký đã được xác định trước. Các chữ ký này là các mẫu nhận diện các mối đe dọa đã biết, chẳng hạn như mẫu của các cuộc tấn công, phần mềm độc hại, hoặc các hoạt động không hợp lệ.

**2. Cách hoạt động:**

1. **Cơ sở dữ liệu chữ ký:**
   * **Chữ ký:** Mỗi chữ ký đại diện cho một mẫu nhận diện cụ thể của một mối đe dọa hoặc hành vi xâm nhập. Chữ ký có thể là các mẫu gói tin, chuỗi ký tự, hoặc hành vi mạng đặc thù.
   * **Cập nhật:** Cơ sở dữ liệu chữ ký được cập nhật thường xuyên để bao gồm các mối đe dọa mới và các biến thể của mối đe dọa cũ.
2. **Giám sát và phân tích:**
   * **Giám sát:** Hệ thống IDS/IPS giám sát liên tục lưu lượng mạng hoặc hành vi hệ thống để thu thập dữ liệu.
   * **Phân tích:** Khi dữ liệu được thu thập, hệ thống sẽ so sánh dữ liệu này với các mẫu chữ ký trong cơ sở dữ liệu. Nếu một mẫu trong dữ liệu khớp với một chữ ký, hệ thống sẽ xác định đây là một hành vi xâm nhập hoặc mối đe dọa.
3. **Phát hiện và phản ứng:**
   * **Phát hiện:** Khi phát hiện một mẫu khớp với chữ ký, hệ thống sẽ tạo ra một cảnh báo.
   * **Phản ứng:** Tùy thuộc vào cấu hình, hệ thống có thể thực hiện các hành động như ghi lại nhật ký, gửi cảnh báo cho quản trị viên, chặn lưu lượng, hoặc ngắt kết nối (đối với IPS).

**3. Lợi ích và hạn chế:**

**Lợi ích:**

* **Chính xác cao với mối đe dọa đã biết:** Phương pháp này có độ chính xác cao trong việc phát hiện các mối đe dọa đã biết, giúp giảm thiểu tỷ lệ cảnh báo sai.
* **Hiệu suất tốt:** Thường có hiệu suất tốt vì chỉ cần so sánh dữ liệu với một tập hợp mẫu chữ ký, không cần phân tích phức tạp.

**Hạn chế:**

* **Không phát hiện được mối đe dọa mới:** Không hiệu quả trong việc phát hiện các mối đe dọa mới hoặc chưa có chữ ký.
* **Cần cập nhật thường xuyên:** Yêu cầu cập nhật cơ sở dữ liệu chữ ký thường xuyên để đảm bảo khả năng phát hiện các mối đe dọa mới.
* **Bỏ sót các biến thể:** Có thể bỏ sót các biến thể của mối đe dọa nếu các chữ ký không được thiết kế để nhận diện các biến thể này.

**4. Ứng dụng:**

**IDS/IPS dựa trên chữ ký** thường được sử dụng trong các môi trường mà việc phát hiện các mối đe dọa đã biết là ưu tiên hàng đầu. Chúng thích hợp cho các hệ thống mà mẫu lưu lượng mạng và hành vi hệ thống ít thay đổi, cho phép nhận diện các mối đe dọa một cách hiệu quả và nhanh chóng.

**Tóm tắt**

**Phương pháp phát hiện dựa trên chữ ký** là một công cụ quan trọng trong bảo mật mạng, cung cấp khả năng phát hiện nhanh chóng và chính xác các mối đe dọa đã biết. Tuy nhiên, để đạt hiệu quả cao nhất, phương pháp này thường được kết hợp với các phương pháp phát hiện khác, như phát hiện dựa trên bất thường, để cung cấp một lớp bảo mật toàn diện và sâu rộng hơn.

**10. Anh/chị hãy giải thích tấn công kiểu Social Engineering và nêu các cách phòng chống?**

**Tấn công kiểu Social Engineering và cách phòng chống**

**Tấn công kiểu Social Engineering:**

**1. Khái niệm:**

* **Social Engineering (Kỹ thuật xã hội):** Là hình thức tấn công mà kẻ tấn công sử dụng các kỹ thuật tâm lý để lừa đảo, thao túng người dùng tiết lộ thông tin nhạy cảm, thực hiện các hành động không an toàn, hoặc cho phép truy cập vào hệ thống mà họ không nên truy cập.

**2. Các hình thức tấn công Social Engineering:**

1. **Phishing:**
   * **Mô tả:** Kẻ tấn công gửi email, tin nhắn, hoặc liên kết giả mạo, giả danh các tổ chức hoặc cá nhân tin cậy để lừa người dùng cung cấp thông tin cá nhân, thông tin đăng nhập, hoặc tải xuống phần mềm độc hại.
   * **Ví dụ:** Email giả mạo từ ngân hàng yêu cầu xác nhận thông tin tài khoản.
2. **Spear Phishing:**
   * **Mô tả:** Là một hình thức phishing nhưng được tùy chỉnh và nhắm mục tiêu cụ thể vào một cá nhân hoặc tổ chức.
   * **Ví dụ:** Email giả mạo từ giám đốc điều hành gửi đến nhân viên yêu cầu chuyển khoản tiền.
3. **Pretexting:**
   * **Mô tả:** Kẻ tấn công tạo ra một kịch bản hoặc bối cảnh giả để lừa người dùng cung cấp thông tin hoặc thực hiện các hành động không an toàn.
   * **Ví dụ:** Giả vờ là nhân viên IT yêu cầu người dùng cung cấp mật khẩu để "sửa lỗi hệ thống".
4. **Baiting:**
   * **Mô tả:** Kẻ tấn công sử dụng một mồi nhử, như một ổ đĩa USB chứa phần mềm độc hại, để thu hút nạn nhân.
   * **Ví dụ:** Đặt ổ đĩa USB có nhãn hấp dẫn như "Danh sách tiền thưởng" tại nơi công cộng để nạn nhân nhặt và cắm vào máy tính.
5. **Quid Pro Quo:**
   * **Mô tả:** Kẻ tấn công hứa hẹn cung cấp một lợi ích nào đó để đổi lấy thông tin hoặc truy cập vào hệ thống.
   * **Ví dụ:** Giả vờ là nhân viên hỗ trợ kỹ thuật cung cấp dịch vụ miễn phí để lấy thông tin đăng nhập.
6. **Tailgating:**
   * **Mô tả:** Kẻ tấn công cố gắng theo sau một người được phép vào một khu vực bảo mật mà không cần phải tự xác thực.
   * **Ví dụ:** Kẻ tấn công theo sau một nhân viên vào tòa nhà văn phòng bằng cách giữ cửa cho họ.

**Cách phòng chống tấn công Social Engineering:**

1. **Đào tạo và nâng cao nhận thức:**
   * **Mô tả:** Đào tạo nhân viên về các hình thức tấn công Social Engineering, cách nhận diện chúng và cách phản ứng khi gặp phải.
   * **Lợi ích:** Giúp nhân viên nhận biết các dấu hiệu của tấn công và giảm thiểu rủi ro bị lừa đảo.
2. **Xác thực hai yếu tố (2FA):**
   * **Mô tả:** Sử dụng xác thực hai yếu tố để bảo vệ tài khoản, yêu cầu xác thực bổ sung ngoài mật khẩu.
   * **Lợi ích:** Tăng cường bảo mật và giảm thiểu rủi ro từ việc lộ mật khẩu.
3. **Kiểm tra kỹ trước khi cung cấp thông tin:**
   * **Mô tả:** Luôn xác minh danh tính của người yêu cầu thông tin và lý do yêu cầu trước khi cung cấp thông tin nhạy cảm.
   * **Lợi ích:** Ngăn chặn việc vô tình cung cấp thông tin cho kẻ tấn công.
4. **Sử dụng các biện pháp kỹ thuật:**
   * **Mô tả:** Sử dụng phần mềm chống phishing, lọc email và các công cụ bảo mật khác để phát hiện và chặn các cuộc tấn công.
   * **Lợi ích:** Tăng cường bảo vệ hệ thống khỏi các cuộc tấn công.
5. **Xây dựng và thực hiện chính sách bảo mật:**
   * **Mô tả:** Xây dựng các chính sách bảo mật rõ ràng và thực hiện chúng, bao gồm các quy trình về việc xử lý thông tin và truy cập hệ thống.
   * **Lợi ích:** Tạo ra một môi trường bảo mật và giảm thiểu rủi ro bị tấn công.
6. **Kiểm tra định kỳ:**
   * **Mô tả:** Thực hiện các cuộc kiểm tra bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật.
   * **Lợi ích:** Giảm thiểu rủi ro từ các lỗ hổng bảo mật và nâng cao khả năng phát hiện các mối đe dọa.

**Tóm tắt**

**Tấn công Social Engineering** là một mối đe dọa nghiêm trọng đối với an ninh thông tin vì nó khai thác yếu tố con người, yếu tố mà thường dễ bị tổn thương nhất trong hệ thống bảo mật. Tuy nhiên, bằng cách kết hợp các biện pháp kỹ thuật và đào tạo nhận thức, các tổ chức có thể giảm thiểu rủi ro và bảo vệ hệ thống của mình khỏi các cuộc tấn công này.

**Câu 11:** Anh/chị hãy phân tích các kỹ thuật kiểm soát truy nhập trên tường lửa? Liệt kê các hạn chế tường lửa

**Các kỹ thuật kiểm soát truy nhập trên tường lửa**

1. **Kiểm soát dựa trên địa chỉ IP**:
   * Cho phép hoặc chặn truy cập dựa trên địa chỉ IP nguồn hoặc đích.
2. **Kiểm soát dựa trên giao thức**:
   * Quản lý truy cập theo các giao thức mạng như TCP, UDP, ICMP.
3. **Kiểm soát dựa trên cổng**:
   * Giới hạn truy cập theo các cổng mạng (port) cụ thể.
4. **Kiểm soát dựa trên ứng dụng**:
   * Lọc lưu lượng dựa trên các ứng dụng hoặc dịch vụ cụ thể.
5. **Kiểm soát dựa trên trạng thái**:
   * Theo dõi và kiểm soát các trạng thái của kết nối mạng (stateful inspection).

**Các hạn chế của tường lửa**

1. **Không bảo vệ khỏi các mối đe dọa nội bộ**:
   * Tường lửa không thể ngăn chặn các cuộc tấn công từ bên trong mạng.
2. **Không thể phát hiện các mối đe dọa mới**:
   * Tường lửa truyền thống có thể không nhận diện được các mối đe dọa chưa biết.
3. **Giới hạn trong việc kiểm soát lưu lượng mã hóa**:
   * Khó kiểm soát hoặc giám sát lưu lượng mạng được mã hóa.
4. **Phụ thuộc vào cấu hình chính xác**:
   * Hiệu quả của tường lửa phụ thuộc vào việc cấu hình đúng và đầy đủ.
5. **Không thay thế các biện pháp bảo mật khác**:

**Câu 12**. Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?

**Quan hệ giữa mối đe dọa và lỗ hổng**

* **Lỗ hổng (Vulnerability)**: Là điểm yếu hoặc thiếu sót trong hệ thống thông tin mà có thể bị khai thác.
* **Mối đe dọa (Threat)**: Là bất kỳ sự kiện hoặc hành động nào có thể gây hại đến hệ thống thông tin.

**Quan hệ**:

* Mối đe dọa lợi dụng lỗ hổng để tấn công và gây hại cho hệ thống. Nếu không có lỗ hổng, mối đe dọa không thể khai thác được.

**Các mối đe dọa thường gặp**

1. **Phần mềm độc hại (Malware)**:
   * Virus, Trojan, Ransomware.
2. **Tấn công từ chối dịch vụ (DDoS)**:
   * Làm tê liệt hệ thống bằng cách quá tải lưu lượng truy cập.
3. **Tấn công mạng (Network Attacks)**:
   * Sniffing, Spoofing, Man-in-the-Middle.
4. **Tấn công vào ứng dụng web (Web Application Attacks)**:
   * SQL Injection, Cross-Site Scripting (XSS).
5. **Tấn công bằng kỹ nghệ xã hội (Social Engineering)**:
   * Phishing, Baiting.
6. **Truy cập trái phép (Unauthorized Access)**:
   * Tấn công brute force, tấn công mật khẩu.

**Câu 13.** Anh/chị hãy trình bày về biện pháp điều khiển truy nhập MAC và cho ví dụ?

**Biện pháp điều khiển truy nhập MAC**

* **Mandatory Access Control (MAC)**: Là cơ chế kiểm soát truy nhập dựa trên các chính sách bảo mật trung tâm do quản trị hệ thống định rõ. Người dùng và tài nguyên đều được gán các mức độ bảo mật cụ thể và quyền truy cập được kiểm soát dựa trên những mức độ này.

**Ví dụ**

* **Hệ thống quân sự**:
  + Các tài liệu được phân loại thành "Mật", "Tối Mật", "Tuyệt Mật".
  + Người dùng có các quyền truy cập tương ứng như "Bí mật", "Tối mật".
  + Người dùng chỉ có thể truy cập tài liệu nếu mức độ bảo mật của họ tương ứng hoặc cao hơn tài liệu.
* **SELinux (Security-Enhanced Linux)**:
  + Một ví dụ về hệ điều hành sử dụng MAC để kiểm soát truy cập các file, quá trình và tài nguyên khác dựa trên các chính sách bảo mật được xác định trước.

**Câu 14**. Anh/chị hãy trình bày về biện pháp điều khiển truy nhập DAC và cho ví dụ?

**Biện pháp điều khiển truy nhập DAC**

* **Discretionary Access Control (DAC)**: Là cơ chế kiểm soát truy nhập mà chủ sở hữu của tài nguyên có quyền xác định ai có thể truy cập và sử dụng tài nguyên đó. Quyền truy cập có thể được gán và thay đổi bởi chủ sở hữu tài nguyên.

**Ví dụ**

* **Hệ điều hành Windows**:
  + Người dùng tạo một file và có quyền quyết định ai có thể đọc, viết hoặc thực thi file đó.
  + Chủ sở hữu có thể thay đổi quyền truy cập của các người dùng khác bất cứ lúc nào.
* **UNIX/Linux**:
  + Một người dùng tạo một thư mục và thiết lập quyền truy cập cho nhóm hoặc người dùng cụ thể bằng các lệnh như chmod, chown.
  + Chủ sở hữu có thể gán quyền đọc, viết hoặc thực thi cho các file hoặc thư mục.

**Câu 15**. Anh/chị hãy so sánh đặc điểm của hệ mật mã khóa đối xứng với hệ mật mã khóa

**So sánh hệ mật mã khóa đối xứng và khóa bất đối xứng**

**Hệ mật mã khóa đối xứng (Symmetric Encryption)**

* **Khóa sử dụng**: Một khóa duy nhất cho cả mã hóa và giải mã.
* **Tốc độ**: Nhanh hơn, thích hợp cho mã hóa dữ liệu lớn.
* **Quản lý khóa**: Khó khăn trong việc phân phối và quản lý khóa an toàn.
* **Ví dụ**: AES, DES, 3DES.

**Hệ mật mã khóa bất đối xứng (Asymmetric Encryption)**

* **Khóa sử dụng**: Sử dụng một cặp khóa - khóa công khai (public key) và khóa riêng (private key).
* **Tốc độ**: Chậm hơn, thường được sử dụng để mã hóa dữ liệu nhỏ hoặc trao đổi khóa.
* **Quản lý khóa**: Dễ dàng hơn trong việc phân phối khóa công khai, khóa riêng được giữ bí mật.
* **Ví dụ**: RSA, ECC, DSA.

**Tóm tắt**

* **Khóa đối xứng**: Nhanh, khó quản lý khóa, dùng cho dữ liệu lớn.
* **Khóa bất đối xứng**: Chậm, dễ quản lý khóa, dùng cho dữ liệu nhỏ hoặc trao đổi khóa.

16. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã, giải thích sơ đồ?

Plaintext

|

V

Initial Permutation (IP)

|

V

16 Rounds of Feistel Structure

|

V

Inverse Initial Permutation (IP^-1)

|

V

Ciphertext

Sơ đồ mô tả các bước chính trong quá trình mã hóa DES:

1. **Hoán vị ban đầu (IP)** : Đây là một vị trí bắt đầu được phép, được áp dụng rõ ràng để tạo ra các khối đầu vào cho 16 vòng lặp sau đó.
2. **16 Vòng của Cấu trúc Feistel** : Quá trình mã hóa diễn đàn qua 16 vòng, trong đó mỗi vòng lặp bao gồm các thao tác được phép như được phép thay thế và được phép cộng modulo 2.
3. **Hoán vị ban đầu nghịch đảo (IP^-1)** : Sau khi hoàn thành 16 vòng, một vị trí đảo ngược được phép áp dụng để tạo ra bản mật cuối cùng.

Mỗi vòng lặp trong Feistel Structure đều có cấu hình tương thích, bao gồm việc chia khối dữ liệu hiện tại thành hai nửa, thực hiện cho phép vị trí và thay thế trên một nửa, sau đó kết hợp lại. Điều này giúp tạo ra sự phức tạp và không xứng đáng cần thiết cho quá trình mã hóa.

17. Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước sinh khóa phụ của hệ mã, giải thích sơ đồ?

Master Key

|

V

PC-1 Permutation

|

V

Left Shift Operations

|

V

PC-2 Permutation

|

V

Round Keys

Sơ đồ mô tả các bước chính trong quá trình phụ khóa sinh học của hệ mã DES:

1. **PC-1 Permutation** : Đầu tiên, khóa master được áp dụng cho phép PC-1 để tạo ra hai khối con, gọi là C0 và D0.
2. **Thao tác dịch trái** : Khi đó, C0 tiến về D0 và nó tiến 1 hoặc 2 bit, sau đó C1, C2, ..., C16 tiến về D1, D2, ..., D16.
3. **PC-2 Permutation** : Các khối C và D được kết hợp lại và được phép sử dụng vị trí PC-2 để tạo ra các khóa phụ K1, K2, ..., K16 được sử dụng trong 16 vòng lặp Feistel.

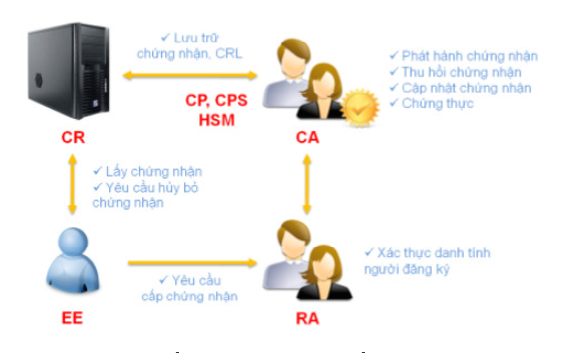
Quá trình sinh khóa phụ này được thực hiện bài hát với quá trình mã hóa, cung cấp các phụ khóa cần thiết cho mỗi vòng lặp Feistel. Việc dịch trái C và D giúp tạo ra các khóa phụ khác nhau, đảm bảo tính bảo mật của hệ thống mã DES.

18. Anh/chị hãy cho biết các thành phần và chức năng của hạ tầng quản lý khóa công khai PKI?

Public Key Infrastructure – PKI (Cơ sở hạ tầng khóa công khai).

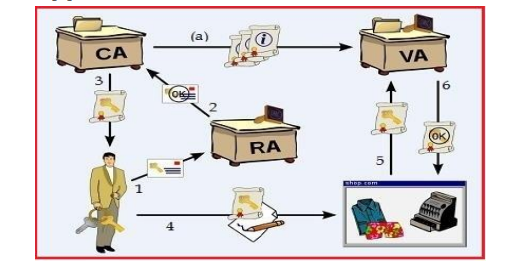
A) Các thành phần của một hạ tầng cơ sở khóa công khai

PKI là cơ cấu tổ chức gồm con người, tiến trình, chính sách, thủ tục, phần cứng và phần mềm dùng để phát sinh, quản lý, lưu trữ, triển khai và thu hồi các chứng nhận khóa công khai.



PKI gồm các thành phần chính sau:

* ***Thực thể cuối (End Entity – EE):***
  + Đối tượng sử dụng chứng nhận (chứng thư số): có thể là một tổ chức, một người cụ thể hay một dịch vụ trên máy chủ, …
* ***Tổ chức chứng nhận(Certificate Authority – CA):***
  + Có nhiệm vụ phát hành, quản lý và hủy bỏ các chứng thư số
  + Là thực thể quan trọng trong một PKI mà được thực thể cuối tín nhiệm
  + Gồm tập hợp các con người và các hệ thống máy tính có độ an toàn cao
* ***Chứng nhận khoá công khai (Public Key Certificate):***
  + Một chứng nhận khóa công khai thể hiện hay chứng nhận sự ràng buộc của danh tính và khóa công khai của thực thể cuối
  + Chứng nhận khóa công khai chứa đủ thông tin cho những thực thể khác có thể xác nhận hoặc kiể m tra danh tính của chủ nhận chứng nhận đó
  + Định dạng được sử dụng rộng rãi nhất của chứng nhận số dựa trên chuẩn IETF X.509.
* ***Tổ chức đăng kí chứng nhận (Registration Authority – RA):*** Mục đích chính của RA là để giảm tải công việc của CA
  + Xác thực cá nhân, chủ thể đăng ký chứng thư số.
  + Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
  + Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số được yêu cầu.
  + Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không (chứng minh sở hữu).
  + Tạo cặp khóa bí mật, công khai. (nếu chủ thể yêu cầu)
  + Phân phối bí mật được chia sẻ đến thực thể cuối (ví dụ khóa công khai của CA).
  + Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
  + Lưu trữ khóa riêng.
  + Khởi sinh quá trình khôi phục khóa
  + Phân phối thẻ bài vật lý (thẻ thông minh)
* ***Kho lưu trữ chứng nhận (Certificate Repository – CR):***
  + Hệ thống (có thể tập trung hoặc phân tán) lưu trữ chứng thư và danh sách các chứng thư bị thu hồi
  + Cung cấp cơ chế phân phối chứng thư và danh sách thu hồi chứng thư (CRLs - Certificate Revocatio Lists).



* (1) : Người dùng gửi yêu cầu phát hành thẻ chứng thư số và khóa công khai của nó đến RA;
* (2) : Sau khi xác nhận tính hợp lệ định danh của người dùng thì RA sẽ chuyển yêu cầu này đến CA;
* (3) : CA phát hành thẻ chứng thư số cho người dùng;
* (4) : Sau đó người dùng “ký” thông điệp trao đổi với thẻ chứng thư số mới vừa nhận được từ CA và sử dụng chúng (thẻ chứng thực số + chữ ký số) trong giao dịch;
* (5) : Định danh của người dùng được kiểm tra bởi đối tác thông qua sự hỗ trợ của VA;

VA (validation authority) : Cơ quan xác thực của bên thứ ba có thể cung cấp thông tin thực thể này thay mặt cho CA.)

* (6) : Nếu chứng thư số của người dùng được xác nhận tính hợp lệ thì đối tác mới tin cậy người dùng và có thể bắt đầu quá trình trao đổi thông tin với nó (VA nhận thông tin về thẻ chứng thư số đã được phát hành từ CA (a))

B) Chức năng

PKI cho phép những người tham gia xác thực lẫn nhau. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định danh người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

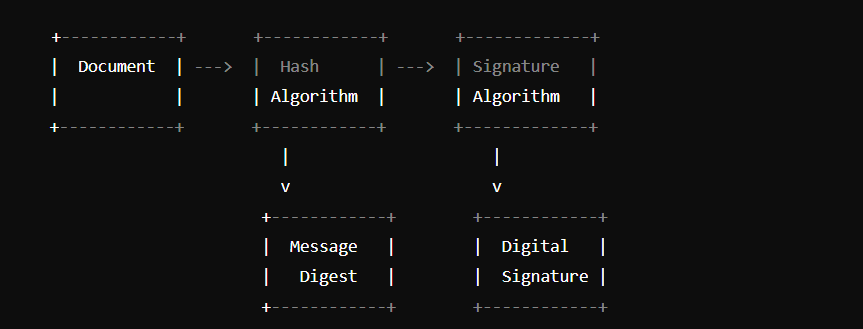
* Mã hóa, giải mã văn bản;
* Xác thực người dùng ứng dụng;
* Mã hóa email hoặc xác thực người gửi email;
* Tạo chữ ký số trên văn bản điện tử.

   Một PKI phải đảm bảo được các tính chất sau trong một hệ thống trao đổi thông tin:

* ***Tính bí mật (Confidentiality):*** PKI phải đảm bảo tính bí mật của dữ liệu.
* ***Tính toàn vẹn (Integrity):*** PKI phải đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa và các giao tác không thể bị thay đổi.
* ***Tính xác thực (Authentication):*** PKI phải đảm bảo danh tính của thực thể được xác minh.
* ***Tính không thể chối từ (Non-Repudiation):*** PKI phải đảm bảo dữ liệu không thể bị không thừa nhận hoặc giao tác bị từ chối.

19. Anh/chị hãy vẽ sơ đồ quá trình tạo và kiểm tra chữ ký số, giải thích sơ đồ?

A) Quá trình tạo chữ ký số



-) Giải thích sơ đồ

1 Document: Tài liệu cần ký số.

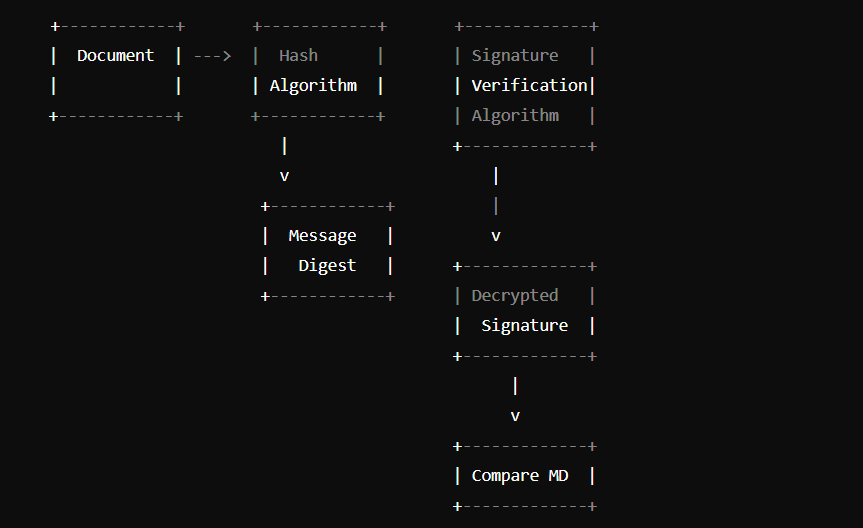
2 Hash Algorithm: Tài liệu được đưa qua một hàm băm (hash function) để tạo ra một thông điệp băm (message digest).

3 Message Digest: Kết quả của hàm băm, thường có kích thước cố định.

4 Signature Algorithm: Thông điệp băm được mã hóa bằng khóa riêng (private key) của người ký để tạo ra chữ ký số (digital signature).

5 Digital Signature: Kết quả cuối cùng là chữ ký số, được gắn kèm với tài liệu.

B) Quá trình kiểm tra chữ ký số



-) Giải thích sơ đồ

1 Document: Tài liệu đã ký số.

2 Hash Algorithm: Tài liệu được đưa qua cùng một hàm băm để tạo ra một thông điệp băm mới.

3 Message Digest: Kết quả của hàm băm, dùng để so sánh với thông điệp băm đã giải mã từ chữ ký số.

4 Signature Verification Algorithm: Chữ ký số được giải mã bằng khóa công khai (public key) của người ký để lấy lại thông điệp băm ban đầu (decrypted message digest).

5 Decrypted Signature: Thông điệp băm đã được giải mã từ chữ ký số.

6 Compare Message Digest: Thông điệp băm mới được tạo từ tài liệu và thông điệp băm giải mã từ chữ ký số được so sánh với nhau. Nếu hai thông điệp băm trùng khớp, chữ ký số hợp lệ.

Tóm Tắt:

Tạo Chữ Ký Số: Tài liệu → Hàm băm → Thông điệp băm → Mã hóa bằng khóa riêng → Chữ ký số.

Kiểm Tra Chữ Ký Số: Tài liệu → Hàm băm → Thông điệp băm mới → Giải mã chữ ký số bằng khóa công khai → So sánh hai thông điệp băm.

Quá trình này đảm bảo rằng tài liệu không bị thay đổi và xác nhận nguồn gốc của tài liệu thông qua chữ ký số.

20. Anh/chị hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số, giải thích sơ đồ?

Chứng chỉ số (Digital certificate), còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một chữ ký số để liên kết một khóa công khai và thông tin nhận dạng của một thực thể.

A) Sơ đồ cấp chứng chỉ số



Giải thích sơ đồ:

1 Applicant (User): Người dùng yêu cầu chứng thư số từ CA (Certificate Authority).

2 Certificate Authority (CA): Thực hiện xác minh danh tính của người dùng.

3 Verify Identity: CA xác minh thông tin của người dùng.

4 Generate Digital Certificate: CA tạo ra chứng thư số cho người dùng.

5 Issue Certificate: CA cấp chứng thư số và lưu trữ trong kho chứng thư.

6 User's Key Pair: Người dùng nhận cặp khóa (khóa công khai và khóa bí mật) cùng với chứng thư số.

B) Quy trình sử dụng chứng chỉ số



1 Sender (User): Người gửi tạo chữ ký số bằng cách băm (hash) tài liệu và mã hóa bằng khóa bí mật của họ.

2 Digital Signature: Chữ ký số được gắn kèm tài liệu.

3 Receiver (User): Người nhận kiểm tra chữ ký số.

4 Verify Signature: Người nhận giải mã chữ ký số bằng khóa công khai của người gửi và so sánh với giá trị băm của tài liệu.

5 Retrieve Sender's Certificate from CA: Người nhận truy xuất chứng thư số của người gửi từ CA để xác minh.

6 Compare Hash Values: So sánh giá trị băm. Nếu trùng khớp, chữ ký số hợp lệ và tài liệu không bị thay đổi.