ĐỀ CƯƠNG ÔN THI MÔN BẢN QUYỀN SỐ

1. Tổng quan về bản quyền số, khái niệm và lịch sử phát triển.

- Bản quyền số là những quyền con người và quyền hợp pháp cho phép các cá nhân truy cập, sử dụng, sao chép, chia sẻ, tạo và xuất bản sản phẩm kỹ thuật số. Khái niệm này đặc biệt liên quan đến việc bảo vệ và thực hiện các hình thức chứng thực bảo mật, trong bối cảnh của công nghệ kỹ thuật số, đặc biệt là Internet.
- Sản phẩm nội dung số: sản phẩm nội dung, thông tin bao gồm văn bản, dữ liệu, hình ảnh, âm thanh được thể hiện dưới dạng số, được lưu giữ, truyền đưa trên môi trường mạng."
- Về phân loại sản phẩm nội dung số bao gồm các sản phẩm sau:
  - Giáo trình, bài giảng, tài liệu học tập dưới dạng điện tự.
  - Sách, báo, tài liệu dưới dạng số.
  - Các loại trò chơi điện tử bao gồm trò chơi trên máy tính đơn, trò chơi trực tuyến, trò chơi trên điện thoại di động, trò chơi tương tác qua truyền hình, sản phẩm giải trí trên mạng viễn thông di động và cố định.
  - Thư viện số, kho dữ liệu số, từ điển điện tử.
  - Phim số, ảnh số, nhạc số, quảng cáo số.
  - Các sản phẩm nội dung số khác.
- Lịch sử phát triển :
  - Năm 1983: Hệ thống dịch vụ phần mềm (SSS) được phát minh bởi kỹ sư người Nhật Ryuichi Moriya, sau đó được phát triển thành superdistribution.
  - Mã hóa: SSS sử dụng mã hóa và phần cứng chuyên dụng để kiểm soát việc giải mã.
  - Thanh toán: SSS cho phép gửi thanh toán đến chủ sở hữu bản quyền.
  - Phân phối không hạn chế: Nguyên tắc của SSS và superdistribution là sản phẩm kỹ thuật số được mã hóa phải được phân phối mà không bị hạn chế.
  - Phân phối lại: Người dùng được phép và khuyến khích phân phối lại sản phẩm.
- DRM (Digital Rights Management) hay Quản lý bản quyền nội dung số là một tập hợp các công nghệ và quy định nhằm kiểm soát quyền truy cập và sử dụng nội dung số có bản quyền. Mục đích chính của DRM là ngăn chặn việc sao chép và phân phối trái phép nội dung số, bảo vệ quyền lợi của chủ sở hữu bản quyền.
- Cách thức hoạt động của DRM:
  - Mã hóa: Nội dung số được mã hóa để chỉ những người có quyền truy cập hợp lệ mới có thể giải mã và xem/sử dụng.

  - Quản lý khóa: Các khóa mã hóa được phân phối cho người dùng hợp lệ và được quản lý chặt chẽ để ngăn chặn truy cập trái phép.
  - Xác thực: Người dùng cần xác thực danh tính trước khi truy cập nội dung số.
  - Hạn chế sử dụng: DRM có thể hạn chế số lần truy cập, thời gian sử dụng, thiết bị sử dụng,... nội dung số.
- Ứng dụng DRM:
  - Đĩa DVD phim: DRM được sử dụng để ngăn chặn việc sao chép đĩa DVD trái phép.
  - Sách điện tử: DRM được sử dụng để hạn chế số lần người dùng có thể tải xuống và đọc sách điện tử.
  - Âm nhạc trực tuyến: DRM được sử dụng để ngăn chặn việc tải xuống và chia sẻ nhạc trái phép.
- Thách thức trong việc quản lý bản quyền nội dung số:
  - Sự phát triển của công nghệ số khiến việc sao chép và phân phối nội dung số trở nên dễ dàng hơn.
  - Khó khăn trong việc xác định và truy tố hành vi vi phạm bản quyền.
  - Sự khác biệt về luật bản quyền giữa các quốc gia.Z

2. Các biện pháp công nghệ kỹ thuật áp dụng, nguyên tắc, cách thức thực hiện bảo vệ bản quyền số sản phẩm đa phương tiện.

- Xác minh:
  - Product Key:
    + Một trong những phương pháp bảo vệ DRM lâu đời nhất và ít phức tạp nhất dành cho các trò chơi điện tử trên máy tính . Là một dãy số hoặc chữ số đại diện cho giấy phép sử dụng phần mềm.
    + Sử dụng để xác minh quyền sở hữu hợp pháp của người dùng đối với sản phẩm.

    Ví dụ: Khóa CD, khóa kích hoạt.

  - Kích hoạt cài đặt giới hạn:
    + Hạn chế số lần cài đặt hoặc sử dụng phần mềm trên nhiều thiết bị.
    + Yêu cầu xác thực trực tuyến với máy chủ để kích hoạt.
  - Xác thực trực tuyến liên tục:
    + Không cung cấp trọn vẹn sản phẩm mà cung cấp dần dần theo nhu cầu của người dùng, cách này thường áp dụng với các nền tảng trò chơi trực tuyến.

- Mã hóa:
    - Mã hóa nội dung sản phẩm trước khi phân phối.
    - Chỉ giải mã khi người dùng có giấy phép hợp lệ.
    - Hình thức DRM mã hóa có thể đảm bảo rằng các biện pháp hạn chế khác không thể bị bỏ qua bằng cách sửa đổi phần mềm, vì vậy các hệ thống DRM tinh vi dựa vào mã hóa để có hiệu quả hoàn toàn.
    - Các ví dụ hiện đại hơn bao gồm ADEPT, FairPlay, Hệ thống nội dung truy cập nâng cao.
- Hạn chế sao chép:
    - Áp dụng cho sách và tài liệu điện tử.
    - Ngăn chặn việc sao chép, in ấn, chuyển tiếp và lưu bản sao lưu trái phép.
    - Có thể sử dụng kết hợp với các biện pháp bảo vệ khác như mã hóa và xác minh.

3. Các nội dung liên quan lập trình Python để bảo vệ bản quyền số

- Mã hóa:
    - Sử dụng các thư viện như hashlib, cryptography để mã hóa nội dung kỹ thuật số (phim, nhạc, phần mềm,...).
    - Mã hóa đối xứng: Sử dụng cùng một khóa để mã hóa và giải mã dữ liệu. Ưu điểm: Tốc độ nhanh, đơn giản. Nhược điểm: Khóa cần được chia sẻ an toàn.
    - Mã hóa bất đối xứng: Sử dụng hai khóa riêng biệt: khóa công khai để mã hóa và khóa bí mật để giải mã. Ưu điểm: Bảo mật cao, không cần chia sẻ khóa bí mật. Nhược điểm: Tốc độ chậm hơn mã hóa đối xứng.
    - Mã hóa hàm băm: Biến đổi dữ liệu thành chuỗi ký tự có độ dài cố định, không thể đảo ngược. Ứng dụng: Xác minh tính toàn vẹn dữ liệu, phát hiện thay đổi trái phép.
- Ẩn tin số (Steganography):
    - Sử dụng Pillow để ẩn thông tin bản quyền trong nội dung kỹ thuật số khác (như hình ảnh, âm thanh).
    - Ẩn thông tin vào các pixel của hình ảnh hoặc các bit của âm thanh.
    - Ưu điểm: Khó phát hiện bằng mắt thường. Nhược điểm: Dung lượng thông tin ẩn có giới hạn, có thể ảnh hưởng đến chất lượng nội dung gốc.
- Quản lý khóa:
    - Sử dụng thư viện cryptography để tạo, lưu trữ, quản lý và hủy khóa an toàn.
    - Mã hóa khóa bằng mật mã để bảo mật.
    - Cập nhật khóa định kỳ để giảm thiểu nguy cơ bị bẻ khóa.

- Xác thực điện tử:
    - Sử dụng thư viện cryptography để tạo chữ ký số cho dữ liệu, đảm bảo tính toàn vẹn và nguồn gốc dữ liệu.
    - Sử dụng khóa bất đối xứng để tạo và xác minh chữ ký số.
    - Ứng dụng: Xác minh danh tính người dùng, bảo vệ giao dịch điện tử.

4. Bảo vệ bản quyền bằng khóa sản phẩm (Product Key)

- Khái niệm
    - Product Key là một mã chuyên dụng cho một phần mềm được cấp phép. Bằng cách sử dụng Product Key, các công ty phần mềm có thể đảm bảo rằng người dùng không "bẻ khóa" sản phẩm hoặc truy cập bất hợp pháp
- Phân loại
    - **OEM License**: Là khóa sản phẩm được tích hợp sẵn trên máy tính bởi nhà sản xuất và chỉ có thể sử dụng cho máy đó. Không cho phép nâng cấp lên phiên bản Windows mới hơn.
    - **OEM License key**: Cho phép xóa cài đặt hoặc cài đặt tùy chỉnh, có thể đưa máy về trạng thái như mới thông qua việc cài lại Windows hoặc sử dụng tính năng Recovery.
    - **Full License key**: Còn gọi là phiên bản đóng gói đầy đủ, cho phép cài đặt và sau đó nâng cấp lên phiên bản Windows mới hơn. Thường có giá cao và không đi kèm với máy tính.
    - **Upgrade License**: Dùng để nâng cấp Windows, có giá rẻ hơn và thường mua cho máy tính đã có OEM License.
    - **Volume License**: Dành cho doanh nghiệp hoặc tổ chức với số lượng lớn, có thể kích hoạt cho nhiều máy tính.
    - **Retail License**: Mua từ cửa hàng bán lẻ, có thể sử dụng lại nhiều lần nhưng phải xoá khóa trước khi cài mới Windows.
    - **License Key**: Tương tự như Product Key, có thể sử dụng để kích hoạt Windows.
- Các thuật toán mã hóa
    - **DES (Data Encryption Standard)**: Là thuật toán mã hóa đối xứng cũ, sử dụng một khóa độc nhất để mã hóa và giải mã dữ liệu, bảo mật Product Key.
    - **AES (Advanced Encryption Standard)**: Một thuật toán mã hóa đối xứng mạnh mẽ hơn DES, sử dụng khóa có độ dài 128, 192 hoặc 256 bit, được coi là an toàn nhất hiện nay.

- **SHA-1 (Secure Hash Algorithm 1)**: Thuật toán băm tạo ra chuỗi băm 160 bit từ dữ liệu đầu vào, dùng để kiểm tra tính toàn vẹn của Product Key.
- **MD5 (Message Digest 5)**: Thuật toán băm tạo ra chuỗi băm 128 bit, cũng dùng để kiểm tra tính toàn vẹn của Product Key.

- Quy trình mã hóa
  - **Tạo khóa ngẫu nhiên**: Tùy thuộc vào thuật toán, tạo một số ngẫu nhiên với độ dài phù hợp (ví dụ: 128 bit hoặc 256 bit cho AES).
  - **Mã hóa bằng khóa**: Sử dụng số ngẫu nhiên này làm khóa để mã hóa Product Key, thường dùng các thuật toán đối xứng như DES hoặc AES.
  - **Tạo mã băm**: Nếu cần, áp dụng thuật toán băm như SHA-1 hoặc MD5 để tạo mã băm cho Product Key mã hóa, giúp kiểm tra tính toàn vẹn và ngăn chặn sự giả mạo.
  - **Thêm thông tin**: Trong quá trình tạo, có thể thêm các tham số như số lần sử dụng, thời gian sử dụng, hoặc số phiên bản sản phẩm vào Product Key và mã hóa chúng cùng với khóa.
- Các phương pháp xác thực
  - Xác thực bằng hàm băm:
  + Ưu điểm: Đơn giản, hiệu quả, không cần phần mềm/thiết bị đặc biệt.
  + Nhược điểm: Bảo mật không cao, có thể bị tấn công bằng kỹ thuật tấn công băm.
  - Xác thực bằng mã hóa đối xứng:
  + Ưu điểm: Bảo mật cao hơn hàm băm, sử dụng thuật toán như DES, AES.
  + Nhược điểm: Chi phí phát triển cao do yêu cầu phần mềm/thiết bị mã hóa và giải mã.
  - Xác thực bằng chữ ký số:
  + Ưu điểm: Bảo mật rất cao, xác thực chính xác, kiểm tra tính toàn vẹn của Product Key.
  + Nhược điểm: Cần công nghệ phức tạp, kỹ năng kỹ thuật cao, chi phí phát triển tăng.

5. Bảo vệ bản quyền bằng kỹ thuật khóa khu vực (Regional Lockout)

- **Khái niệm:**
  - Khóa khu vực (Regional Lockout) là một kỹ thuật bảo vệ bản quyền được sử dụng để hạn chế việc sử dụng phần mềm, nội dung kỹ thuật số hoặc sản phẩm vật lý cho một khu vực địa lý cụ thể. Kỹ thuật này hoạt động

bằng cách xác định vị trí của người dùng và chỉ cho phép họ sử dụng sản phẩm nếu họ ở trong khu vực được phép.

- **Ưu điểm:**
  - Giúp kiểm soát việc phân phối sản phẩm và ngăn chặn việc bán hàng giả hoặc hàng lậu.
  - Giúp định giá sản phẩm phù hợp với từng khu vực, dựa trên điều kiện kinh tế và thị hiếu của người tiêu dùng.
  - Giúp bảo vệ quyền sở hữu trí tuệ bằng cách ngăn chặn việc sao chép và phân phối trái phép sản phẩm.
- **Nhược điểm:**
  - Có thể gây bất tiện cho người dùng ở những khu vực không được phép sử dụng sản phẩm.
  - Có thể bị bẻ khóa bởi những kẻ tấn công có trình độ cao.
  - Có thể làm tăng chi phí sản xuất và phân phối sản phẩm.
- **Các phương pháp khóa khu vực:**
  - **Khóa IP:** Sử dụng địa chỉ IP của người dùng để xác định vị trí của họ.
  - **Khóa GPS:** Sử dụng GPS để xác định vị trí của người dùng.
  - **Khóa phần cứng:** Sử dụng chip đặc biệt trong thiết bị để xác định vị trí của thiết bị.
  - **Khóa phần mềm:** Sử dụng phần mềm để xác định vị trí của thiết bị.

6. Các kỹ thuật bảo vệ bản quyền Games

- Mã hóa:
  - Mã hóa đối xứng: Sử dụng cùng một khóa để mã hóa và giải mã dữ liệu.
  - Mã hóa bất đối xứng: Sử dụng hai khóa riêng biệt: khóa công khai để mã hóa và khóa bí mật để giải mã.
  - Mã hóa hàm băm: Biến đổi dữ liệu thành chuỗi ký tự có độ dài cố định, không thể đảo ngược.
- Ẩn tin số (Steganography):
  - Ẩn thông tin bản quyền trong nội dung game, khiến cho người chơi bình thường không thể phát hiện được.
  - Một số phương pháp ẩn tin số phổ biến bao gồm:
  + Ẩn thông tin vào các pixel của hình ảnh hoặc các bit của âm thanh.
  + Sử dụng các thuật toán đặc biệt để ẩn thông tin trong các tệp tin.
- Quản lý khóa:
  - Sử dụng các hệ thống quản lý khóa để bảo mật các khóa mã hóa và các khóa khác được sử dụng để bảo vệ game.
  - Một số hệ thống quản lý khóa phổ biến bao gồm:

    + Hệ thống quản lý khóa dựa trên phần mềm: Lưu trữ khóa trên máy chủ và sử dụng phần mềm để quản lý truy cập và sử dụng khóa.
    + Hệ thống quản lý khóa dựa trên phần cứng: Lưu trữ khóa trên các thiết bị phần cứng chuyên dụng và sử dụng phần mềm để quản lý truy cập và sử dụng khóa.
- Xác thực điện tử:
    - Xác thực bằng mật khẩu: Người chơi sử dụng mật khẩu để đăng nhập vào game.
    - Xác thực hai yếu tố: Người chơi sử dụng hai yếu tố xác thực, chẳng hạn như mật khẩu và mã OTP, để đăng nhập vào game.
    - Xác thực sinh trắc học: Người chơi sử dụng dấu vân tay hoặc khuôn mặt để xác minh danh tính của họ.
- Phát triển các hệ thống quản lý bản quyền số:
    - Hệ thống quản lý bản quyền dựa trên DRM (Digital Rights Management): Sử dụng các kỹ thuật mã hóa, ẩn tin số, quản lý khóa và xác thực điện tử để bảo vệ game.
    - Hệ thống quản lý bản quyền dựa trên blockchain: Sử dụng blockchain để lưu trữ thông tin bản quyền và quản lý truy cập vào game.

7. Blockchain

- **Khái niệm**
    - Blockchain, hay còn gọi là chuỗi khối, là một công nghệ sổ cái phân tán (DLT) ghi lại các giao dịch và thông tin một cách an toàn, minh bạch và không thể thay đổi. Nó được tạo thành từ các khối được liên kết với nhau bằng mã hóa mật mã, mỗi khối chứa thông tin về khối trước đó. \
- **Ứng dụng trong bản quyền số**
    - Lưu trữ thông tin bản quyền: Blockchain có thể được sử dụng để lưu trữ thông tin về tác phẩm, tác giả, ngày tạo, quyền sở hữu, v.v. một cách an toàn và minh bạch.
    - Xác minh danh tính: Blockchain có thể được sử dụng để xác minh danh tính của tác giả và nguồn gốc của tác phẩm.
    - Quản lý quyền sử dụng: Blockchain có thể được sử dụng để quản lý quyền sử dụng tác phẩm, cho phép tác giả cấp phép sử dụng tác phẩm của họ cho người khác một cách dễ dàng và minh bạch.
    - Thu phí bản quyền: Blockchain có thể được sử dụng để thu phí bản quyền cho tác phẩm một cách tự động và hiệu quả.
- **Một số giải pháp**

- Maidsafe: Nền tảng phi tập trung lưu trữ dữ liệu và chia sẻ tệp tin, cho phép người dùng kiểm soát hoàn toàn dữ liệu của họ và nhận phí bản quyền khi người khác sử dụng dữ liệu đó.
- Creative Commons: Cung cấp các giấy phép bản quyền mở cho phép người dùng chia sẻ, sử dụng và sửa đổi tác phẩm kỹ thuật số một cách hợp pháp.
- Open Music Initiative: Nền tảng phi tập trung để phân phối nhạc và thu phí bản quyền cho nhạc sĩ.

- **Một số lợi ích**
  - Tăng cường an ninh: Blockchain là một hệ thống an toàn và minh bạch, giúp bảo vệ thông tin bản quyền khỏi bị giả mạo hoặc thay đổi.
  - Tăng hiệu quả: Blockchain có thể giúp tự động hóa các quy trình quản lý bản quyền, giúp tiết kiệm thời gian và chi phí cho tác giả và nhà xuất bản.
  - Tăng tính minh bạch: Blockchain cung cấp một sổ cái minh bạch về quyền sở hữu và lịch sử sử dụng tác phẩm, giúp tăng cường sự tin tưởng giữa tác giả, nhà xuất bản và người dùng.

8. Hợp đồng thông minh (Smart Contract)

- Khái niệm
- **Hợp đồng thông minh** Smart Contract) là một chương trình máy tính hoặc giao thức giao dịch được thiết kế để tự động thực hiện các điều khoản của hợp đồng theo cách an toàn, minh bạch và không thể thay đổi. Nó được thực thi trên nền tảng Blockchain, sử dụng mật mã để xác minh và bảo mật các điều khoản hợp đồng.
- Đặc điểm chính của hợp đồng thông minh:
- **Tự động hóa:** Hợp đồng thông minh tự động thực hiện các điều khoản khi các điều kiện được đáp ứng, loại bỏ nhu cầu trung gian và thủ tục thủ công.
- **Minh bạch:** Tất cả các bên tham gia có thể truy cập và kiểm tra các điều khoản của hợp đồng, đảm bảo tính minh bạch và tin cậy.
- **An toàn:** Hợp đồng thông minh được bảo mật bằng mật mã, giúp bảo vệ dữ liệu và ngăn chặn gian lận hoặc sửa đổi trái phép.
- **Không thể thay đổi:** Một khi hợp đồng thông minh được triển khai trên Blockchain, nó không thể bị thay đổi bởi bất kỳ bên nào, đảm bảo tính chính xác và tính pháp lý.
- Lợi ích của hợp đồng thông minh:
- **Tiết kiệm thời gian và chi phí:** Loại bỏ nhu cầu trung gian và thủ tục thủ công, giúp tiết kiệm thời gian và chi phí giao dịch.

- **Tăng cường hiệu quả:** Tự động hóa các quy trình và giảm thiểu lỗi do con người, giúp tăng cường hiệu quả hoạt động.
- **Tăng cường tính minh bạch:** Mọi giao dịch đều được ghi lại trên Blockchain, đảm bảo tính minh bạch và truy xuất nguồn gốc.
- **Giảm thiểu rủi ro gian lận:** Mật mã giúp bảo vệ dữ liệu và ngăn chặn gian lận hoặc sửa đổi trái phép.

- Ứng dụng của hợp đồng thông minh:

- **Tài chính:** Thanh toán, cho vay, bảo hiểm, quản lý tài sản,...
- **Chuỗi cung ứng:** Theo dõi hàng hóa, quản lý hợp đồng, thanh toán,...
- **Bất động sản:** Mua bán nhà đất, cho thuê, quản lý tài sản,...
- **Chính phủ:** Cấp phép, thu thuế, quản lý dịch vụ công,...
- **Giải trí:** Bản quyền, thanh toán cho tác giả, quản lý quyền sở hữu trí tuệ,...

9. NFT

- Khái niệm

- **NFT (Non-Fungible Token)** là một loại token (mã thông báo) kỹ thuật số đại diện cho một tài sản số duy nhất và không thể thay thế. Nó được lưu trữ trên Blockchain, đảm bảo tính an toàn, minh bạch và không thể thay đổi. NFT có tiềm năng to lớn trong việc định danh tài sản số và bảo vệ bản quyền số.

- NFT định danh tài sản số như thế nào?

- **Mỗi NFT là duy nhất:** Mỗi NFT có một mã định danh riêng biệt, không thể sao chép hoặc làm giả. Điều này giúp xác minh quyền sở hữu và nguồn gốc của tài sản số một cách chính xác.
- **Lưu trữ trên Blockchain:** NFT được lưu trữ trên Blockchain, một sổ cái phân tán an toàn và minh bạch. Điều này giúp bảo vệ NFT khỏi bị hack hoặc thay đổi trái phép.
- **Thông tin chi tiết về tài sản:** NFT có thể chứa thông tin chi tiết về tài sản số, bao gồm mô tả, tác giả, ngày tạo, lịch sử sở hữu, v.v. Thông tin này được lưu trữ vĩnh viễn trên Blockchain và có thể truy cập được bởi bất kỳ ai.

- Lợi ích của việc sử dụng NFT cho bản quyền số:

- **Chống vi phạm bản quyền:** NFT giúp xác minh quyền sở hữu của tài sản số và ngăn chặn việc sao chép trái phép. Điều này giúp bảo vệ quyền lợi của tác giả và khuyến khích sáng tạo nội dung chất lượng cao.

- **Theo dõi lịch sử sử dụng:** NFT có thể ghi lại lịch sử sử dụng của tài sản số, giúp theo dõi việc cấp phép và thanh toán bản quyền một cách minh bạch.
- **Tăng cường khả năng tiếp cận:** NFT giúp người dùng dễ dàng truy cập và sở hữu tài sản số một cách hợp pháp.
- **Mở ra các mô hình kinh doanh mới:** NFT có thể được sử dụng để tạo ra các mô hình kinh doanh mới cho bản quyền số, chẳng hạn như bán tác phẩm nghệ thuật kỹ thuật số, nhạc, video, v.v.

• Ví dụ về ứng dụng:

- **OpenSea:** Nền tảng giao dịch NFT lớn nhất thế giới, nơi người dùng có thể mua, bán và tạo NFT cho nhiều loại tài sản số khác nhau.
- **Rarible:** Nền tảng giao dịch NFT tập trung vào nghệ thuật kỹ thuật số, cho phép người sáng tạo bán tác phẩm của họ trực tiếp cho người hâm mộ.
- **SuperRare:** Nền tảng giao dịch NFT dành cho các tác phẩm nghệ thuật kỹ thuật số độc đáo và quý hiếm.

10. Mã hóa cổ điển

• Khái niệm:

- Mã hóa cổ điển là một phương pháp mã hóa sử dụng các kỹ thuật đơn giản để thay đổi văn bản gốc thành dạng không thể đọc được.
- Mục đích: Giữ bí mật thông tin và bảo vệ nó khỏi những người không được phép truy cập.

• Kỹ thuật:

- Thay thế: Thay thế các ký tự trong văn bản gốc bằng các ký tự khác theo một quy tắc nhất định.
- Đơn bảng chữ cái (Monoalphabetic): Mỗi ký tự trong bảng chữ cái được thay thế bằng một ký tự khác cố định.
- Đa bảng chữ cái (Polyalphabetic): Sử dụng nhiều bảng chữ cái thay thế khác nhau để mã hóa văn bản.
- Hoán vị: Thay đổi vị trí các ký tự trong văn bản gốc theo một quy tắc nhất định.

• Ưu điểm:

- Dễ dàng triển khai và sử dụng.
- Không yêu cầu thiết bị hay phần mềm phức tạp.

• Nhược điểm:

- Mức độ bảo mật thấp, dễ bị bẻ khóa bằng các phương pháp phân tích mật mã.

- Không an toàn cho việc bảo mật thông tin quan trọng.

- Ví dụ:

- Mã Caesar: Mã hóa mỗi ký tự bằng cách dịch chuyển nó một số vị trí nhất định trong bảng chữ cái.
- Mã Vigenère: Sử dụng một từ khóa để mã hóa văn bản, mỗi ký tự trong văn bản gốc được thay thế bằng ký tự tương ứng trong từ khóa.
- Mã Playfair: Chia văn bản thành các cặp ký tự và mã hóa mỗi cặp bằng cách sử dụng bảng 5x5.
- Mã hàng rào sắt: Viết văn bản theo hàng ngang, sau đó sắp xếp lại các ký tự theo thứ tự nhất định.

- Lưu ý:

- Mã hóa cổ điển không còn được sử dụng rộng rãi trong bảo mật thông tin hiện đại do tính an toàn thấp.
- Các phương pháp mã hóa hiện đại như mã hóa đối xứng và mã hóa bất đối xứng có mức độ bảo mật cao hơn nhiều.

11. Mã hóa đối xứng :

- Khái niệm:

- Mã hóa đối xứng là một loại mật mã sử dụng chung một khóa cho cả quá trình mã hóa và giải mã dữ liệu.
- Khóa này được giữ bí mật và không được chia sẻ với bất kỳ ai khác.

- Cách thức hoạt động:

- Một khóa duy nhất được sử dụng cho cả hai quá trình:
- Mã hóa: Chuyển đổi văn bản gốc thành bản mã.
- Giải mã: Chuyển đổi bản mã thành văn bản gốc.

- Mức độ bảo mật:

- Mức độ bảo mật phụ thuộc vào độ dài khóa và thuật toán mã hóa được sử dụng.
- Khóa càng dài, càng khó bị bẻ khóa bằng cách tấn công brute force.
- Các thuật toán mã hóa hiện đại như AES có khả năng chống lại các cuộc tấn công tiên tiến.

- Ưu điểm:

- Dễ dàng triển khai và sử dụng.
- Hiệu quả tính toán cao.

- Nhược điểm:

- Cần chia sẻ khóa bí mật một cách an toàn.
- Nếu kẻ tấn công lấy được khóa, họ có thể mã hóa và giải mã bất kỳ dữ liệu nào.

- Ví dụ:
- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- Blowfish
- Ứng dụng:
- Bảo vệ dữ liệu nhạy cảm khi truyền tải hoặc lưu trữ.
- Bảo mật giao tiếp trực tuyến.
- Xác thực danh tính người dùng.

12. Mã hóa bất đối xứng

- Khái niệm:
- Mã hóa bất đối xứng, còn gọi là mã hóa công khai, sử dụng cặp khóa gồm:
- Khóa công khai (Public Key): Được chia sẻ cho mọi người.
- Khóa riêng (Private Key): Giữ bí mật và không được chia sẻ với bất kỳ ai.
- Cách thức hoạt động:
- Mã hóa: Sử dụng khóa công khai của người nhận để mã hóa thông tin.
- Giải mã: Sử dụng khóa riêng của người nhận để giải mã thông tin.
- Ưu điểm:
- Dễ dàng chia sẻ khóa công khai: Không cần thiết lập kênh truyền tin bí mật để chia sẻ khóa.
- An toàn hơn: Khóa riêng được giữ bí mật, chỉ người nhận mới có thể giải mã thông tin.
- Xác thực nguồn gốc thông tin: Có thể sử dụng chữ ký số để xác thực nguồn gốc của thông tin.
- Hiệu quả cho giao tiếp nhóm: Chỉ cần n cặp khóa cho n người tham gia.
- Nhược điểm:
- Khả năng bị tấn công "người đứng giữa": Kẻ tấn công có thể giả mạo người nhận và đánh lừa người gửi để tiết lộ thông tin.
- Tính toán phức tạp: Tính toán bằng khóa bất đối xứng phức tạp hơn so với mã hóa đối xứng.
- Ứng dụng:
- Trao đổi khóa an toàn.
- Chữ ký số.
- Xác thực danh tính.
- Bảo mật email.
- Thương mại điện tử.

- Ví dụ:
- RSA (Rivest-Shamir-Adleman)
- ElGamal
- Diffie-Hellman
- Elliptic Curve Cryptography (ECC)
- Lưu ý:
- Cần bảo quản khóa riêng an toàn.
- Sử dụng các thuật toán mã hóa hiện đại và có độ dài khóa đủ lớn.
- Cập nhật phần mềm và hệ điều hành thường xuyên để vá các lỗ hổng bảo mật.

13. Hàm băm

- Khái niệm:
- Hàm băm (Hash function) là một thuật toán biến đổi một chuỗi dữ liệu (có thể là văn bản, hình ảnh, tệp tin, v.v.) thành một giá trị có độ dài cố định gọi là giá trị băm (hash value) hoặc mã băm (hash digest).
- Quá trình này được gọi là băm (hashing).
- Đặc điểm:
- Hàm một chiều: Dễ dàng tính toán giá trị băm từ dữ liệu đầu vào, nhưng rất khó (hoặc không thể) tính toán dữ liệu đầu vào từ giá trị băm.
- Chống va chạm: Hai dữ liệu đầu vào khác nhau sẽ tạo ra giá trị băm khác nhau.
- Chống thay đổi: Bất kỳ thay đổi nào đối với dữ liệu đầu vào sẽ dẫn đến thay đổi giá trị băm.
- Ứng dụng:
- Xác minh tính toàn vẹn dữ liệu: Phát hiện lỗi hoặc thay đổi trái phép trong dữ liệu.
- Bảo mật mật khẩu: Lưu trữ mật khẩu dưới dạng giá trị băm để bảo mật.
- Xác thực danh tính: Xác minh tính xác thực của tệp tin hoặc thông tin kỹ thuật số.
- Tạo chữ ký số: Tạo chữ ký điện tử để đảm bảo tính toàn vẹn và xác thực của tài liệu.
- Lọc spam: Xác định và loại bỏ thư rác.
- Ví dụ:
- MD5 (Message Digest 5)
- SHA-1 (Secure Hash Algorithm 1)
- SHA-256 (Secure Hash Algorithm 256)
- SHA-3 (Secure Hash Algorithm 3)

- Lưu ý:
- Cần sử dụng hàm băm mạnh mẽ và có độ dài giá trị băm đủ lớn để đảm bảo an ninh.
- Cập nhật thuật toán băm thường xuyên để vá các lỗ hổng bảo mật.

14. Chữ ký số (Digital Signature)

- **Khái niệm:**
  - Chữ ký số là một kỹ thuật bảo mật sử dụng mật mã bất đối xứng để xác thực danh tính của người gửi và đảm bảo tính toàn vẹn của thông điệp. Nó tương tự như chữ ký tay trên tài liệu giấy, nhưng được thực hiện trên các văn bản số.
- **Đặc điểm:**
  - Độ an toàn cao: Khó bị giả mạo hoặc thay đổi.
  - Được sử dụng rộng rãi: Trong nhiều lĩnh vực như thương mại điện tử, ngân hàng, thuế, ...
  - Dựa trên mật mã bất đối xứng: Sử dụng cặp khóa bí mật (Private Key) và công khai (Public Key).
  - Cần sử dụng nhà cung cấp dịch vụ Chữ ký số (CA): Để cấp và quản lý Chữ ký số.
- **Lợi ích:**
  - Xác thực danh tính: Đảm bảo người gửi thực sự là ai.
  - Bảo đảm tính toàn vẹn: Đảm bảo thông điệp không bị thay đổi trong quá trình truyền tải.
  - Tăng cường tính pháp lý: Giúp các giao dịch điện tử có giá trị pháp lý như giao dịch giấy tờ.
  - Tiết kiệm thời gian và chi phí: Giảm thiểu thủ tục giấy tờ và chi phí giao dịch.
- **Cách thức hoạt động:**
  - Tạo cặp khóa: Người dùng tạo cặp khóa Private Key và Public Key. Private Key phải được giữ bí mật, còn Public Key có thể được chia sẻ.
  - Ký thông điệp: Người dùng sử dụng Private Key để ký thông điệp, tạo ra chữ ký số.
  - Gửi thông điệp: Thông điệp cùng với chữ ký số được gửi cho người nhận.
  - Xác minh chữ ký: Người nhận sử dụng Public Key của người gửi để xác minh chữ ký số.
    + Nếu chữ ký hợp lệ, thông điệp được xác nhận là từ người gửi và chưa bị thay đổi.

+ Nếu chữ ký không hợp lệ, thông điệp có thể bị giả mạo hoặc thay đổi.

15. Xác thực điện tử

- **Khái niệm**

  Xác thực điện tử là một tập hợp các kỹ thuật và phương pháp được sử dụng để đảm bảo tính an toàn, tin cậy cho các giao dịch điện tử.

- **Nguyên tắc hoạt động:**
  - Dựa trên việc sử dụng các phương pháp mật mã, bao gồm mã hóa, giải mã, chữ ký số, hàm băm.
  - Sử dụng các cơ sở dữ liệu để lưu trữ thông tin về người dùng, khóa xác thực và các chứng thư điện tử.
  - Áp dụng các quy trình và thủ tục để xác minh danh tính, kiểm tra tính toàn vẹn của thông tin và ghi chép nhật ký giao dịch.
- **Phương pháp xác thực điện tử phổ biến:**
  - Xác thực dựa trên mật khẩu: Sử dụng mật khẩu để xác minh danh tính người dùng.
  - Xác thực sinh trắc học: Sử dụng các đặc điểm sinh học của cơ thể người như dấu vân tay, khuôn mặt, mống mắt để xác minh danh tính.
  - Xác thực hai yếu tố (2FA): Sử dụng kết hợp hai phương pháp xác thực khác nhau, ví dụ như mật khẩu và mã OTP gửi qua tin nhắn SMS hoặc email.
  - Xác thực bằng chứng thư điện tử: Sử dụng chứng thư điện tử để xác minh danh tính người dùng.
  - Xác thực bằng mã OTP: Sử dụng mã OTP (One Time Password) được tạo ngẫu nhiên và chỉ có giá trị sử dụng trong một khoảng thời gian ngắn để xác minh danh tính người dùng.

16. Thủy vân số

- Khái niệm:
  - Thủy vân số (watermarking) là kỹ thuật nhúng thông tin ẩn vào một đối tượng kỹ thuật số như ảnh, âm thanh, video hoặc tài liệu. Thông tin ẩn này được gọi là "thủy vân" (watermark) và có thể chứa nhiều loại dữ liệu khác nhau như logo, bản quyền, thông tin xác thực, v.v.
- Mục đích:
  - Bảo vệ bản quyền: Ngăn chặn việc sao chép trái phép nội dung kỹ thuật số.
  - Xác thực nguồn gốc: Xác minh nguồn gốc của nội dung kỹ thuật số.

- Theo dõi phân phối: Theo dõi cách thức nội dung kỹ thuật số được phân phối và sử dụng.
- Kiểm soát truy cập: Hạn chế quyền truy cập vào nội dung kỹ thuật số.

- Loại hình:
- Thủy vân số có thể nhìn thấy: Có thể nhìn thấy bằng mắt thường.
- Thủy vân số không thể nhìn thấy: Không thể nhìn thấy bằng mắt thường, chỉ có thể phát hiện bằng các thuật toán đặc biệt.

- Phương pháp:
- Kỹ thuật nhúng thay thế: Thay đổi một phần nhỏ dữ liệu gốc để nhúng thông tin ẩn.
- Kỹ thuật nhúng bổ sung: Thêm thông tin ẩn vào dữ liệu gốc mà không thay đổi dữ liệu gốc.

- Ứng dụng:
- Hình ảnh: Bảo vệ bản quyền ảnh, theo dõi việc sử dụng ảnh, xác thực ảnh.
- Âm thanh: Bảo vệ bản quyền nhạc, theo dõi việc sử dụng nhạc, xác thực nguồn gốc nhạc.
- Video: Bảo vệ bản quyền phim, theo dõi việc phân phối phim, xác minh nguồn gốc phim.
- Tài liệu: Bảo vệ bản quyền tài liệu, theo dõi việc sử dụng tài liệu, xác minh nguồn gốc tài liệu.

- Ưu điểm:
- Dễ dàng nhúng thông tin ẩn vào nội dung kỹ thuật số.
- Khó phát hiện và loại bỏ thủy vân số.
- Có thể áp dụng cho nhiều loại nội dung kỹ thuật số khác nhau.

- Nhược điểm:
- Có thể ảnh hưởng đến chất lượng nội dung kỹ thuật số nếu không được nhúng cẩn thận.
- Có thể bị bẻ khóa bởi những kẻ tấn công có trình độ cao.

17. Giấu tin số (Steganography):

- Khái niệm:
- Giấu tin số (Steganography) là kỹ thuật ẩn thông tin bí mật vào trong một đối tượng kỹ thuật số khác như ảnh, âm thanh, video, hoặc tài liệu. Thông tin bí mật này được gọi là "thông điệp ẩn" (hidden message) và có thể chứa nhiều loại dữ liệu khác nhau như văn bản, hình ảnh, âm thanh, v.v.

- Mục đích:

- Bảo mật thông tin: Giữ bí mật thông tin quan trọng bằng cách che giấu nó trong một đối tượng khác.
- Truyền thông bí mật: Giao tiếp bí mật giữa hai hoặc nhiều người bằng cách sử dụng phương tiện truyền tải công khai.
- Xác thực danh tính: Xác minh danh tính của người gửi hoặc người nhận thông tin.

• Loại hình:

- Giấu tin dựa trên hình ảnh: Ẩn thông điệp vào trong ảnh bằng cách thay đổi các pixel, độ sáng, hoặc màu sắc của ảnh.
- Giấu tin dựa trên âm thanh: Ẩn thông điệp vào trong âm thanh bằng cách thay đổi tần số, biên độ, hoặc pha của âm thanh.
- Giấu tin dựa trên video: Ẩn thông điệp vào trong video bằng cách thay đổi các khung hình, màu sắc, hoặc âm thanh của video.
- Giấu tin dựa trên văn bản: Ẩn thông điệp vào trong văn bản bằng cách thay đổi các ký tự, khoảng trắng, hoặc định dạng của văn bản.

• Phương pháp:

- Kỹ thuật nhúng thay thế: Thay đổi một phần nhỏ dữ liệu gốc để nhúng thông điệp ẩn.
- Kỹ thuật nhúng bổ sung: Thêm thông điệp ẩn vào dữ liệu gốc mà không thay đổi dữ liệu gốc.

• Ưu điểm:

- Dễ dàng ẩn thông điệp bí mật vào trong đối tượng kỹ thuật số.
- Khó phát hiện và loại bỏ thông điệp ẩn.
- Có thể áp dụng cho nhiều loại đối tượng kỹ thuật số khác nhau.

• Nhược điểm:

- Có thể ảnh hưởng đến chất lượng đối tượng kỹ thuật số nếu không được nhúng cẩn thận.
- Có thể bị bẻ khóa bởi những kẻ tấn công có trình độ cao.

• Ứng dụng:

- Bảo mật thông tin: Bảo vệ thông tin nhạy cảm như dữ liệu tài chính, thông tin cá nhân, v.v.
- Truyền thông bí mật: Giao tiếp bí mật giữa các cá nhân hoặc tổ chức.
- Xác thực danh tính: Xác minh danh tính của người gửi hoặc người nhận thông tin.
- Bảo vệ bản quyền: Bảo vệ bản quyền nội dung kỹ thuật số như ảnh, âm thanh, video, v.v.

18. Các nguyên lý tạo lập và bảo vệ bản quyền số, kiểm soát bản quyền, chống sao chép trái phép, các chuẩn mực xã hội liên quan.

- Hiểu cơ bản thì DRM hoạt động dựa trên việc mã hóa nội dung file bằng 1 **secret key**. Khi có nhu cầu sử dụng file, ứng dụng riêng biệt để đọc file sẽ tiến hành giải mã file. Lúc này chúng ta mới có thể sử dụng được file.

- **Mã hóa**

- Đầu tiên, người tiến hành đóng gói file sẽ gửi yêu cầu tới DRM System để nhận eKey.
- Sau đó sử dụng eKey để mã hóa file.
- Encrypted file sẽ được chia sẻ ra ngoài khi có người cần sử dụng.
- Đôi khi Encryption key được tạo bởi chính người tiến hành đóng gói file. Sau đó key này mới được lưu trữ trên DRM System.

- **Giải mã**

- Khi có nhu cầu sử dụng file. Người dùng sẽ mở **file X** bằng ứng dụng chuyên biệt. (File X là một file chứa thông tin về nội dung người dùng muốn truy cập)
- Ứng dụng sẽ tải nội dung đã được mã hóa về.
- Sau khi có Encrypted file rồi, ứng dụng sẽ yêu cầu nhận Decryption key từ DRM System.
- Nếu thông tin xác thực được chấp nhận, DRM System sẽ gửi lại dKey. Ứng dụng sẽ giải mã file DRM bằng dKey này để người dùng sử dụng.

19. Giấy phép tài liệu tự do GNU, giấy phép GPL, giấy phép Common Creative…

- Giới thiệu:

- Ba loại giấy phép phổ biến được sử dụng để bảo vệ và chia sẻ sáng tạo là Giấy phép Tài liệu Tự do GNU (GNU FDL), Giấy phép Công cộng GNU (GNU GPL) và Giấy phép Creative Commons (CC). Mỗi loại giấy phép có những đặc điểm và ứng dụng riêng, phù hợp với nhu cầu khác nhau của tác giả và người sử dụng.

- Giấy phép Tài liệu Tự do GNU (GNU FDL):

- Mục đích: Dành cho tài liệu hướng dẫn phần mềm miễn phí.
- Điều khoản chính:
  + Tự do sao chép, sửa đổi và phân phối miễn phí.
  + Yêu cầu ghi chú bản quyền và danh sách sửa đổi.
  + Yêu cầu cấp phép bản phái sinh theo FDL.
  + Yêu cầu cung cấp mã nguồn phần mềm liên quan (nếu có).
  + Gây khó khăn cho việc xuất bản thương mại.
- Ứng dụng: Tài liệu hướng dẫn phần mềm miễn phí (GNU/Linux, GCC, Firefox...).

- Giấy phép Công cộng GNU (GNU GPL):

- Mục đích: Dành cho phần mềm miễn phí.
- Điều khoản chính:
  + Tự do sử dụng, nghiên cứu, chia sẻ và sửa đổi miễn phí.

+ Yêu cầu ghi chú bản quyền và danh sách sửa đổi.
+ Yêu cầu cấp phép bản phái sinh theo GPL.
+ Yêu cầu cung cấp mã nguồn cho mọi bản phân phối.

- Ứng dụng: Phần mềm miễn phí phổ biến (GNU/Linux, GCC, Firefox...).

• Giấy phép Creative Commons (CC):

- Mục đích: Dành cho nhiều loại tác phẩm sáng tạo (văn học, nghệ thuật, âm nhạc...).
- Điểm đặc biệt: Cung cấp nhiều lựa chọn cấp phép linh hoạt hơn FDL và GPL.
- Các loại giấy phép CC phổ biến:
  + CC BY: Ghi chú nguồn gốc (bắt buộc).
  + CC BY-SA: Ghi chú nguồn gốc - Chia sẻ tương tự (bắt buộc).
  + CC BY-ND: Ghi chú nguồn gốc - Không được phép sửa đổi (bắt buộc).
  + CC BY-NC: Ghi chú nguồn gốc - phi thương mại (bắt buộc).
  + CC Zero (CC0): Miễn phí sử dụng - Miễn phí chia sẻ - Miễn phí sửa đổi (không cần ghi chú nguồn gốc).
- Ứng dụng: Sách điện tử, bài báo khoa học, âm nhạc, ảnh, video...

20. Các nội dung liên quan phương pháp bảo vệ bản quyền Windows, mã hóa phần cứng,…

• Khái niệm

- Product Key là một chuỗi bao gồm 25 ký tự, cả chữ và số, được sử dụng để kích hoạt bản quyền trên Windows, giúp người dùng có thể sử dụng đầy đủ tính năng của hệ điều hành mà không bị giới hạn. Có rất nhiều loại Product Key khác nhau như Retail, OEM, MAK (Multiple Activation Key), mỗi loại có đặc điểm và mục đích sử dụng riêng.

• Các loại Product Key:

- Retail License Key:

+ Được mua riêng lẻ từ các cửa hàng hoặc trang web của Microsoft.
+ Có thể chuyển từ máy này sang máy khác miễn là chỉ được sử dụng trên một máy tính tại một thời điểm.

- OEM License Key (Original Equipment Manufacturer):

+ Được cài đặt sẵn trên các máy tính mới bởi các nhà sản xuất.
+ Liên kết với phần cứng cụ thể và không thể chuyển sang máy tính khác.

- Volume License Key (VLK):

+ Dành cho doanh nghiệp, tổ chức mua số lượng lớn.
+ Có thể sử dụng để kích hoạt nhiều máy tính.

- MAK (Multiple Activation Key):
+ Một loại Volume License Key.
+ Cho phép kích hoạt một số lượng nhất định các lần trên các máy tính khác nhau.
- Kiểm tra tính hợp lệ của Product Key trên Windows 95:
+ 3 ký tự đầu tiên: Không được là 333, 444, 555, 666, 777, 888, hoặc 999.
+ 7 ký tự cuối cùng:Phải là các số từ 0-8.
+ Tổng của 7 số cuối phải chia hết cho 7 và không có số dư.
+ Ký tự thứ tư: Không được chọn.
+ Nếu tất cả các kiểm tra vượt qua, khóa sản phẩm là hợp lệ

21. Các quy định pháp luật về bản quyền nói chung và bản quyền số ở các nước và các hiệp ước, hiệp định quốc tế liên quan bản quyền số

- Các văn bản pháp lý:

- Hoa Kỳ: Digital Millennium Copyright Act (DMCA)
- Liên minh Châu Âu: Information Society Directive và Directive 2001/29/EC
- Canada: Fact Sheet: Digital Rights Management (DRM)
- Hiệp định TRIPS (WTO): Agreement on Trade-Related Aspects of Intellectual Property Rights
- WIPO (Tổ chức Sở hữu Trí Tuệ Thế giới): Các hiệp ước quốc tế về sở hữu trí tuệ

- Quan niệm pháp lý:

- Quyền tác giả: Quyền của tác giả đối với tác phẩm của mình, bao gồm quyền về tinh thần và quyền lợi kinh tế.
- Bản quyền: Quyền lợi kinh tế của chủ sở hữu quyền tác giả đối với tác phẩm.
- Copyright: Khái niệm bản quyền theo hệ thống pháp luật common law (Anh - Mỹ).

22. Các nội dung pháp luật quy định trong các Luật, Bộ Luật có liên quan đến bản quyền số, sở hữu trí tuệ ở Việt Nam.

- Luật Sở hữu trí tuệ:

- Được Quốc hội Việt Nam thông qua ngày 29 tháng 11 năm 2005 và có hiệu lực từ ngày 1 tháng 7 năm 2006.

- Quy định về quyền tác giả, quyền liên quan đến quyền tác giả, quyền sở hữu công nghiệp, quyền đối với giống cây trồng và việc bảo hộ các quyền đó.
- Quyền sở hữu trí tuệ: Quyền của tổ chức, cá nhân đối với tài sản trí tuệ, bao gồm:
- Quyền tác giả: Quyền của tổ chức, cá nhân đối với tác phẩm do mình sáng tạo ra hoặc sở hữu.
- Quyền liên quan đến quyền tác giả: Quyền của tổ chức, cá nhân đối với cuộc biểu diễn, bản ghi âm, ghi hình, chương trình phát sóng, tín hiệu vệ tinh mang chương trình được mã hóa.
- Quyền sở hữu công nghiệp: Quyền của tổ chức, cá nhân đối với sáng chế, kiểu dáng công nghiệp, thiết kế bố trí mạch tích hợp bán dẫn, nhãn hiệu, tên thương mại, chỉ dẫn địa lý, bí mật kinh doanh do mình sáng tạo ra hoặc sở hữu và quyền chống cạnh tranh không lành mạnh.
- Quyền đối với giống cây trồng: Quyền của tổ chức, cá nhân đối với giống cây trồng mới do mình chọn tạo hoặc phát hiện và phát triển hoặc được hưởng quyền sở hữu.
- Tên thương mại: Tên gọi của tổ chức, cá nhân dùng trong hoạt động kinh doanh để phân biệt chủ thể kinh doanh mang tên gọi đó với chủ thể kinh doanh khác trong cùng lĩnh vực và khu vực.
    - Luật an ninh mạng
    - Luật an toàn thông tin mạng
    - Luật CNTT