**PHÂN BIỆT CÁC KHÁI NIỆM**

***1. Privacy vs Secret vs Confidecential***

|  |  |  |  |
| --- | --- | --- | --- |
| Thuộc tính | Privacy | Confidential | Secret |
| Bản chất | Quyền của cá nhân | Nghĩa vụ/Trách nhiệm | Trạng thái của thông tin |
| Ngữ cảnh | Cá nhân, xã hội | Chuyên nghiệp, pháp lý | Cá nhân, tổ chức, chung chung |
| Hàm ý | Thường tích cực, liên quan đến quyền | Thường tích cực, liên quan đến sự tin cậy | Có thể tích cực hoặc tiêu cực, liên quan đến sự che giấu |
| Ví dụ | Quyền kiểm soát dữ liệu cá nhân trên mạng xã hội | Thông tin khách hàng của ngân hàng | Vị trí một kho báu bị giấu kín |

***2.*** ***Cryptosystem vs Cryptoscheme vs Cryptoprotocol vs Cryptoprimitive vs Cryptobuildingblocks***

**a) Cryptoprimitive & Cryptobuildingblocks**

**Cryptoprimitive** (Nguyên tố mật mã) và **Cryptobuildingblocks** (Khối xây dựng mật mã) thường được sử dụng thay thế cho nhau để chỉ các thuật toán mật mã cơ bản nhất. Chúng là những "nguyên tử" của một hệ thống mật mã, mỗi loại được thiết kế để thực hiện một chức năng cụ thể duy nhất với tính bảo mật đã được chứng minh.

* **Ví dụ:** Thuật toán **AES** (dùng cho mã hóa), **SHA-256** (dùng cho hàm băm), hoặc **RSA** (dùng cho mã hóa khóa công khai và chữ ký số).

**b) Cryptoscheme**

Một **Cryptoscheme** (Sơ đồ mật mã) là một mô tả trừu tượng và toán học về một quá trình mật mã. Nó định nghĩa các thuật toán, khóa và các tham số bảo mật nhưng không đi sâu vào chi tiết triển khai cụ thể. Nó thường được sử dụng trong các bối cảnh học thuật và lý thuyết.

* **Ví dụ:** Khái niệm chung về "mã hóa khóa công khai" là một cryptoscheme. **RSA** và **Diffie-Hellman** là các hệ thống mật mã cụ thể triển khai sơ đồ này.

**c) Cryptosystem**

Một **Cryptosystem** (Hệ thống mật mã) là một hệ thống hoàn chỉnh và thực tiễn để triển khai một sơ đồ mật mã. Nó là một tập hợp cụ thể của các thuật toán và quy trình dùng để đảm bảo an toàn cho việc truyền thông hoặc lưu trữ dữ liệu. Một cryptosystem bao gồm không chỉ các thuật toán mã hóa cốt lõi mà còn cả các quy tắc và quy trình sử dụng chúng, như việc quản lý khóa.

* **Ví dụ:** **Tiêu chuẩn mã hóa nâng cao (AES)** là một cryptosystem. Nó bao gồm thuật toán AES cùng với các kích thước khóa được xác định (128, 192, 256 bit) và cách thức thực hiện các quy trình mã hóa và giải mã. .

**d) Cryptoprotocol**

Một **Cryptoprotocol** (Giao thức mật mã) là một tập hợp các quy tắc và quy trình xác định cách sử dụng các nguyên tố mật mã và các hệ thống mật mã để đạt được một mục tiêu bảo mật rộng lớn hơn trong một hệ thống giao tiếp. Các giao thức này điều phối nhiều bước, thường liên quan đến nhiều bên, để đảm bảo một thuộc tính bảo mật mong muốn (ví dụ: xác thực, toàn vẹn hoặc bảo mật).

* **Ví dụ:** **TLS (Transport Layer Security)** là một cryptoprotocol. Nó sử dụng kết hợp các nguyên tố mật mã (như AES để mã hóa, SHA-256 để đảm bảo toàn vẹn và RSA để trao đổi khóa) và xác định một chuỗi các bước để hai bên thiết lập một kết nối an toàn, được xác thực và riêng tư qua mạng.

***3. Cryptology vs Cryptography vs Cryptoanalysis***

**a) Cryptology (Mật mã học)**

**Cryptology** là môn khoa học nghiên cứu tổng thể về mật mã. Nó bao gồm cả việc thiết kế các thuật toán bảo mật (Cryptography) và phân tích các điểm yếu của chúng (Cryptoanalysis). Một nhà mật mã học (**cryptologist**) không chỉ biết cách tạo ra các hệ thống an toàn mà còn phải hiểu cách thức chúng có thể bị tấn công để từ đó xây dựng các biện pháp phòng thủ tốt hơn.

**b) Cryptography (Mật mã)**

**Cryptography** là nghệ thuật và khoa học về việc tạo ra các phương pháp bảo mật thông tin. Mục tiêu chính của cryptography là đảm bảo tính bí mật, toàn vẹn, xác thực và không thể từ chối của dữ liệu. Lĩnh vực này tập trung vào việc phát triển các thuật toán và giao thức để mã hóa thông tin, biến nó thành dạng không thể đọc được đối với những người không được ủy quyền.

* **Ví dụ:** Các thuật toán mã hóa như **AES** và **RSA** là sản phẩm của cryptography.

**c) Cryptoanalysis (Phân tích mật mã)**

**Cryptoanalysis** là khoa học về việc phá vỡ các hệ thống mật mã. Mục tiêu của cryptoanalysis là tìm ra các điểm yếu trong một thuật toán hoặc hệ thống để giải mã thông tin mà không cần có khóa. Quá trình này rất quan trọng vì nó giúp kiểm tra và đánh giá độ an toàn của các thuật toán mật mã. Một hệ thống mật mã được coi là an toàn nếu nó có khả năng chống lại các cuộc tấn công cryptoanalysis.

* **Ví dụ:** Một cuộc tấn công bằng phương pháp Brute Force để tìm khóa giải mã là một hình thức của cryptoanalysis.

***4. Encoding vs Encrypting***

|  |  |  |
| --- | --- | --- |
| Đặc điểm | Encoding (Mã hóa) | Encrypting (Mã hóa) |
| Mục đích | Đảm bảo tính tương thích và toàn vẹn dữ liệu. | Đảm bảo tính bảo mật và riêng tư của dữ liệu. |
| Cơ chế | Chuyển đổi dữ liệu theo một quy tắc công khai. | Chuyển đổi dữ liệu bằng một thuật toán và khóa bí mật. |
| Khóa | Không yêu cầu khóa. | Yêu cầu một hoặc nhiều khóa để giải mã. |
| Bảo mật | Không có mục tiêu bảo mật. | Là một biện pháp bảo mật mạnh mẽ. |
| Khả năng đảo ngược | Luôn có thể đảo ngược với thuật toán công khai. | Chỉ có thể đảo ngược với khóa bí mật chính xác. |
| Ví dụ | Base64, mã hóa URL, mã hóa ASCII. | AES, RSA, DES. |