**Вопросы для защиты**

## **1. Что изучают следующие разделы криптографии: криптология, криптография, криптоанализ?**

* **Криптология** — наука, которая занимается методами шифрования и дешифровки. Криптология состоит из двух частей — криптографии и криптоанализа.
* **Криптография** занимается разработкой методов шифрования и дешифрования данных.
* **Криптоанализ** занимается оценкой сильных и слабых сторон методов шифрования.
* Mật mã học là khoa học nghiên cứu các phương pháp mã hóa và giải mã. Mật mã học bao gồm hai phần: mật mã học và phân tích mật mã.
* Mật mã học là ngành nghiên cứu các phương pháp mã hóa và giải mã dữ liệu.
* Phân tích mật mã là nghiên cứu về điểm mạnh và điểm yếu của các phương pháp mã hóa.

## **2. Основные отличия, определения, примеры для следующих систем: асимметричные криптосистемы, симметричные криптосистемы, криптографические протоколы.**

2. Sự khác biệt chính, định nghĩa, ví dụ cho các hệ thống sau: hệ thống mật mã bất đối xứng, hệ thống mật mã đối xứng, giao thức mật mã.

### **1. Симметричные криптосистемы *Hệ thống mật mã đối xứng\*\****

**Определение:** Криптографические системы, в которых один и тот же ключ используется как для шифрования, так и для дешифрования данных.

*Hệ thống mật mã trong đó sử dụng cùng một khóa để mã hóa và giải mã dữ liệu.*

**Основные отличия:**

* Высокая скорость работы по сравнению с асимметричными системами.
* Требуется безопасный канал для передачи ключа между отправителем и получателем.
* Уязвимость к атаке посредника (MitM), если ключ скомпрометирован.

*- Tốc độ hoạt động cao so với hệ thống không đối xứng.*

*- Cần có một kênh an toàn để truyền khóa giữa người gửi và người nhận.*

*- Dễ bị tấn công theo kiểu trung gian (MitM) nếu khóa bị xâm phạm.*

**Примеры алгоритмов:**

* AES (Advanced Encryption Standard) — один из самых популярных алгоритмов симметричного шифрования.

*AES (Tiêu chuẩn mã hóa nâng cao) là một trong những thuật toán mã hóa đối xứng phổ biến nhất.*

* DES (Data Encryption Standard) — устаревший, но исторически значимый алгоритм.

*DES (Tiêu chuẩn mã hóa dữ liệu) là một thuật toán lỗi thời nhưng có ý nghĩa lịch sử quan trọng.*

**Пример использования:** VPN, Wi-Fi защита (WPA2), дисковое шифрование (BitLocker, VeraCrypt).

### **2. Асимметричные криптосистемы**

**Определение:** Криптографические системы, использующие пару ключей: открытый (public) для шифрования и закрытый (private) для дешифрования.

*Hệ thống mật mã sử dụng một cặp khóa: khóa công khai để mã hóa và khóa riêng tư để giải mã.*

**Основные отличия:**

* Не требует передачи секретного ключа по небезопасному каналу.
* Более медленные по сравнению с симметричными системами.
* Подходят для цифровых подписей и защиты соединений.

*- Không yêu cầu truyền khóa bí mật qua kênh không an toàn.*

*- Chậm hơn so với hệ thống đối xứng.*

*- Thích hợp cho chữ ký số và bảo mật kết nối.*

**Примеры алгоритмов:**

* **RSA (Rivest-Shamir-Adleman)** — широко используемый алгоритм для шифрования и цифровых подписей.

*RSA (Rivest-Shamir-Adleman) là thuật toán được sử dụng rộng rãi để mã hóa và chữ ký số.*

* **ECC (Elliptic Curve Cryptography)** — более современный и эффективный алгоритм, использующий эллиптические кривые.

*ECC (Elliptic Curve Cryptography) là thuật toán hiện đại và hiệu quả hơn sử dụng đường cong elip.*

* **Diffie-Hellman** — протокол обмена ключами, основанный на асимметричной криптографии.

*Diffie-Hellman là giao thức trao đổi khóa dựa trên mật mã bất đối xứng.*

**Пример использования:** TLS/SSL (HTTPS), цифровые подписи, системы шифрования электронной почты (PGP, S/MIME).

### **3. Криптографические протоколы**

**Определение:** Набор правил и алгоритмов, определяющих, как участники обмениваются зашифрованными данными и аутентифицируют друг друга.

*Một tập hợp các quy tắc và thuật toán xác định cách người tham gia trao đổi dữ liệu được mã hóa và xác thực lẫn nhau.*

**Основные отличия:**

* Используют симметричное и/или асимметричное шифрование.
* Включают механизмы защиты от атак (например, повторного воспроизведения).
* Применяются в различных сценариях (аутентификация, обмен ключами, безопасное соединение).

*- Sử dụng mã hóa đối xứng và/hoặc bất đối xứng.*

*- Cho phép sử dụng cơ chế bảo vệ chống lại các cuộc tấn công (ví dụ: phát lại).*

*- Được sử dụng trong nhiều tình huống khác nhau (xác thực, trao đổi khóa, kết nối an toàn).*

**Примеры протоколов:**

* TLS (Transport Layer Security) — защита интернет-соединений (HTTPS).
* SSH (Secure Shell) — защищенный доступ к удаленным серверам.
* IPsec — защита интернет-трафика на уровне сетевого протокола.

*- TLS (Bảo mật lớp truyền tải) — bảo vệ kết nối Internet (HTTPS).*

*- SSH (Secure Shell) - truy cập an toàn vào máy chủ từ xa.*

*- IPsec - bảo vệ lưu lượng truy cập Internet ở cấp độ giao thức mạng.*

**Пример использования:** Банковские платежи, защищенные соединения, VPN, цифровая аутентификация.

## **3. Выделите примеры шифров для каждого этапа развития криптографии: наивная криптография, формальная криптография, математическая криптография.**

*Cung cấp ví dụ về mật mã cho từng giai đoạn phát triển của mật mã: mật mã ngây thơ, mật mã chính thức, mật mã toán học.*

### **1. Наивная криптография (до XVI века)**

**Характеристика:**

* Основывается на простых заменах и перестановках.
* Не требует математического анализа.
* Уязвима к простому перебору или частотному анализу.

*- Dựa trên phép thay thế và hoán vị đơn giản.*

*- Không cần phân tích toán học.*

*- Dễ bị ảnh hưởng bởi phép liệt kê đơn giản hoặc phân tích tần suất.*

**Примеры шифров:**

* **Шифр Цезаря** – сдвиг букв алфавита на фиксированное число позиций.
* **Шифр Атбаш** – инверсия алфавита (А → Я, Б → Ю в русском языке).
* **Шифр Полибия** – использование квадратной таблицы для шифрования символов.
* **Скоттский шифр** – простая система шифрования из средневековых военных писем.

*- \*\*Mật mã Caesar\*\* – dịch chuyển các chữ cái trong bảng chữ cái theo một số vị trí cố định.*

*- \*\*Mã Atbash\*\* – đảo ngược chữ cái (A → Ya, B → Yu trong tiếng Nga).*

*- \*\*Mã hóa Polybius\*\* – sử dụng bảng vuông để mã hóa các ký hiệu.*

*- \*\*Mã hóa Scotland\*\* là một hệ thống mã hóa đơn giản lấy từ các lá thư quân sự thời trung cổ.*

### 

### 

### **2. Формальная криптография (XVI – XIX века)**

**Характеристика:**

* Использует сложные схемы замен и перестановок.
* Противостоит простому частотному анализу.
* Всё ещё уязвима перед аналитическими методами криптоанализа.

*- Sử dụng các phương án thay thế và hoán vị phức tạp.*

*- Mâu thuẫn với phân tích tần số đơn giản.*

*- Vẫn dễ bị tổn thương bởi các phương pháp phân tích mật mã.*

**Примеры шифров:**

* **Шифр Виженера** – полиалфавитный шифр, использующий ключевое слово.
* **Шифр Плейфера** – биграммная замена букв с использованием таблицы 5×5.
* **Шифровальная решетка Кардано** – метод стеганографии, где текст скрывается в матрице с вырезами.
* **Шифр Гронсфельда** – вариация шифра Виженера с числовыми ключами.

*- \*\*Mã hóa Vigenere\*\* là mã hóa đa chữ cái sử dụng từ khóa.*

*- \*\*Mã Playfair\*\* – thay thế các chữ cái bằng bigram sử dụng bảng 5x5.*

*- \*\*Mạng lưới Cardano\*\* là một phương pháp ẩn chữ trong đó văn bản được ẩn trong một ma trận có các khía.*

*- \*\*Mã hóa Gronsfeld\*\* – một biến thể của mã hóa Vigenere với các khóa số.*

### **3. Математическая криптография (XX век – настоящее время)**

**Характеристика:**

* Основывается на строгих математических моделях.
* Использует теорию чисел, алгебру, вероятностные методы.
* Обеспечивает стойкость даже перед вычислительными атаками.

*- Dựa trên các mô hình toán học chặt chẽ.*

*- Sử dụng lý thuyết số, đại số, phương pháp xác suất.*

*- Cung cấp khả năng chống lại ngay cả các cuộc tấn công bằng máy tính.*

**Примеры шифров:**

* **AES (Advanced Encryption Standard)** – современный симметричный блочный шифр.
* **RSA (Rivest-Shamir-Adleman)** – асимметричный алгоритм на основе факторизации чисел.
* **ECC (Elliptic Curve Cryptography)** – криптография на эллиптических кривых.
* **ChaCha20** – потоковый шифр, используемый в современных VPN и мессенджерах.
* **SHA-256** – криптографическая хеш-функция для цифровых подписей и блокчейна.

*- \*\*AES (Tiêu chuẩn mã hóa nâng cao)\*\* – một thuật toán mã hóa khối đối xứng hiện đại.*

*- \*\*RSA (Rivest-Shamir-Adleman)\*\* – một thuật toán bất đối xứng dựa trên phân tích số.*

*- \*\*ECC (Mã hóa đường cong Elliptic)\*\* – mã hóa trên đường cong Elliptic.*

*- \*\*ChaCha20\*\* – một mã hóa luồng được sử dụng trong các VPN và trình nhắn tin tức thời hiện đại.*

*- \*\*SHA-256\*\* – hàm băm mật mã cho chữ ký số và chuỗi khối.*

С развитием квантовых вычислений ожидается переход к **постквантовой криптографии**, включающей **шифры на решетках (NTRU, Kyber)** и **кодовую криптографию (McEliece)**.

## **4. Шифры замены, перестановки и сдвига**

*Mã hóa thay thế, hoán vị và dịch chuyển*

### **1. Шифры замены Mã thay thế\*\***

**Описание:** Каждая буква или символ заменяется другим символом по фиксированному правилу. Частотный анализ помогает взломать такие шифры.

*Mỗi chữ cái hoặc ký hiệu được thay thế bằng một ký hiệu khác theo một quy tắc cố định. Phân tích tần suất giúp giải mã những mã như vậy.*

**Примеры:**

* **Шифр Цезаря** – каждая буква заменяется на букву, сдвинутую на фиксированное количество позиций (например, A → D при сдвиге 3).
* **Шифр Атбаш** – алфавит меняется на обратный (A ↔ Z, B ↔ Y и т. д.).
* **Шифр Виженера** – каждый символ заменяется с использованием ключевого слова, что делает частотный анализ сложнее.

*- \*\*Mã Caesar\*\* – mỗi chữ cái được thay thế bằng một chữ cái khác dịch chuyển một số vị trí cố định (ví dụ: A → D với độ dịch chuyển là 3).*

*- \*\*Mã Atbash\*\* – bảng chữ cái bị đảo ngược (A ↔ Z, B ↔ Y, v.v.).*

*- \*\*Mã Vigenere\*\* – mỗi ký hiệu được thay thế bằng một từ khóa, khiến việc phân tích tần suất trở nên khó khăn hơn.*

### **2. Шифры перестановки Mã hóa hoán vị\*\***

**Описание:** Буквы или группы символов меняются местами по определённому алгоритму, но сами не изменяются.

*Các chữ cái hoặc nhóm ký tự thay đổi vị trí theo một thuật toán nhất định, nhưng bản thân chúng thì không thay đổi.*

**Примеры:**

* **Шифр железнодорожной изгороди (Rail Fence)** – текст записывается в виде "забора" и считывается построчно.
* **Шифр колонной перестановки** – текст записывается в таблицу построчно, а затем считывается в другом порядке.
* **Шифровальная решетка Кардано** – текст пишется в таблицу, часть символов скрыта решёткой.

*- \*\*Mã hàng rào đường sắt\*\* – văn bản được viết dưới dạng "hàng rào" và được đọc theo từng dòng.*

*- \*\*Mã hóa hoán vị cột\*\* – văn bản được viết vào bảng theo từng dòng, sau đó đọc theo thứ tự khác.*

*- \*\*Mạng lưới mã hóa Cardano\*\* – văn bản được viết vào bảng, một số ký hiệu được ẩn bởi mạng lưới.*

### **3. Шифры сдвига Mật mã dịch chuyển\*\***

**Описание:** Частный случай шифров замены, где буквы алфавита циклически сдвигаются на определённое число позиций.

*Một trường hợp đặc biệt của mật mã thay thế, trong đó các chữ cái trong bảng chữ cái được dịch chuyển tuần hoàn theo một số vị trí nhất định.*

**Примеры:**

* **Шифр Цезаря** – (описан выше, сдвиг букв на фиксированное число позиций).
* **Шифр ROT13** – частный случай Цезаря с сдвигом на 13 позиций (A ↔ N, B ↔ O и т. д.), используется в интернете для скрытия спойлеров.
* **Шифр Гронсфельда** – вариация Виженера, где ключ состоит из чисел, определяющих сдвиг букв.

*- \*\*Mật mã Caesar\*\* – (được mô tả ở trên, dịch chuyển các chữ cái theo một số vị trí cố định).*

*- \*\*Mã hóa ROT13\*\* – một trường hợp đặc biệt của Caesar với sự dịch chuyển 13 vị trí (A ↔ N, B ↔ O, v.v.), được sử dụng trên Internet để ẩn phần tiết lộ cốt truyện.*

*- \*\*Mã hóa Gronsfeld\*\* - một biến thể của mã hóa Vigenere, trong đó khóa mã bao gồm các con số xác định độ dịch chuyển của các chữ cái.*

## **5. Атака полного перебора ключа и частотный анализ символов**

*Tấn công Brute Force và Phân tích tần suất biểu tượng*

### **1. Aтака полного перебора ключа (Brute Force Attack)**

**Описание:** Метод криптоанализа, при котором перебираются все возможные ключи до нахождения верного.  
 *Phương pháp phân tích mật mã bằng cách thử tất cả các khóa có thể để tìm khóa đúng.*

**Особенности:**

* Эффективность зависит от длины ключа: чем длиннее ключ, тем сложнее взлом.  
   *Hiệu quả phụ thuộc vào độ dài khóa: khóa càng dài thì càng khó bị phá.*
* Современные системы используют ключи достаточной длины (например, 128-битный AES), что делает атаку невозможной за разумное время.  
   *Các hệ thống hiện đại sử dụng khóa có độ dài đủ lớn (ví dụ: AES 128-bit), khiến cuộc tấn công gần như không thể trong thời gian hợp lý.*
* Использование распределённых вычислений и квантовых алгоритмов (например, алгоритма Гровера) может ускорить перебор.  
   *Sử dụng tính toán phân tán và các thuật toán lượng tử (ví dụ: thuật toán Grover) có thể tăng tốc quá trình thử khóa.*

**Пример:**

* Взлом **шифра Цезаря** занимает максимум 25 попыток (если алфавит из 26 букв).  
   *Phá mã Caesar mất tối đa 25 lần thử (nếu bảng chữ cái có 26 ký tự).*
* Взлом **64-битного DES** возможен за считанные дни с мощными кластерами (что привело к переходу на AES).  
   *Phá mã DES 64-bit có thể thực hiện trong vài ngày với các cụm máy tính mạnh mẽ (dẫn đến sự chuyển đổi sang AES).*

**Защита:**

* Увеличение длины ключа (например, AES-256 вместо AES-128).  
   *Tăng độ dài khóa (ví dụ: AES-256 thay vì AES-128).*
* Ограничение количества попыток (капчи, блокировка после нескольких неудачных входов).  
   *Giới hạn số lần thử (CAPTCHA, khóa tài khoản sau một số lần đăng nhập thất bại).*
* Использование дополнительных методов шифрования (например, хеширование паролей с солью).  
   *Sử dụng các phương pháp mã hóa bổ sung (ví dụ: băm mật khẩu kèm với muối).*

### **2. Частотный анализ символов**

**Описание:** Метод криптоанализа, основанный на изучении частоты встречаемости символов или биграмм в зашифрованном тексте.  
 *Phương pháp phân tích mật mã dựa trên việc nghiên cứu tần suất xuất hiện của các ký tự hoặc cặp ký tự trong văn bản đã mã hóa.*

**Особенности:**

* Эффективен против простых шифров замены (например, шифра Цезаря, Атбаша).  
   *Hiệu quả đối với các mã thay thế đơn giản (ví dụ: mã Caesar, Atbash).*
* Использует статистику частоты букв в языке (например, в русском чаще всего встречаются «О», «Е», «А»).  
   *Dựa vào thống kê tần suất xuất hiện của chữ cái trong ngôn ngữ (ví dụ, trong tiếng Nga, các chữ cái phổ biến nhất là «О», «Е», «А»).*
* Можно усложнить, если шифр использует несколько алфавитов (полиалфавитные шифры, например, Виженера).  
   *Có thể làm phức tạp hơn nếu mã hóa sử dụng nhiều bảng chữ cái (ví dụ: mã Vigenère).*

**Пример атаки:**

1. Анализируем частоту букв в зашифрованном тексте.  
    *Phân tích tần suất xuất hiện của các chữ cái trong văn bản mã hóa.*
2. Сравниваем с известной частотой букв в языке.  
    *So sánh với tần suất chữ cái đã biết trong ngôn ngữ.*
3. Подбираем вероятные замены и восстанавливаем исходный текст.  
    *Dự đoán các ký tự thay thế và khôi phục văn bản gốc.*

**Защита:**

* Использование **полиалфавитного шифрования** (например, шифр Виженера).  
   *Sử dụng mã hóa đa bảng chữ cái (ví dụ: mã Vigenère).*
* Применение **перестановок** в дополнение к замене.  
   *Áp dụng phương pháp hoán vị kết hợp với thay thế.*
* Использование современных алгоритмов, исключающих прямую зависимость между открытым текстом и зашифрованным.  
   *Sử dụng các thuật toán hiện đại loại bỏ sự phụ thuộc trực tiếp giữa văn bản gốc và văn bản mã hóa.*

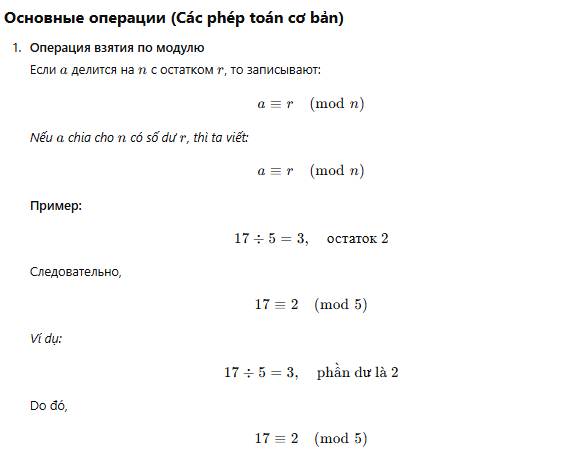
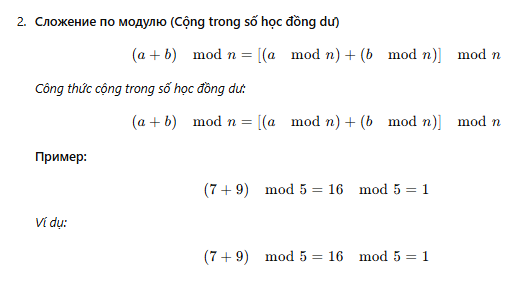
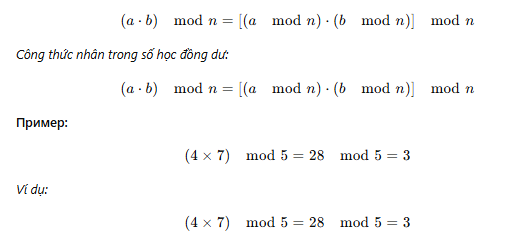
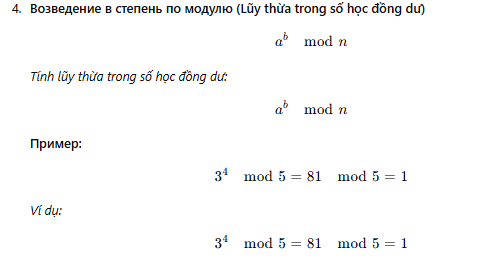
Частотный анализ был причиной отказа от простых шифров и перехода к математической криптографии.  
 *Phân tích tần suất là lý do khiến các mã hóa đơn giản bị loại bỏ và chuyển sang mật mã học toán học.*

## **6. Модульная арифметика. Простые примеры.**

### **Модульная арифметика (Số học đồng dư)**

**Определение:** Модульная арифметика – это раздел математики, в котором числа рассматриваются по остаткам при делении на некоторое фиксированное число (модуль).  
 *Toán học đồng dư là một nhánh của toán học, trong đó các số được xem xét theo phần dư khi chia cho một số cố định (mô-đun).*

### **Основные операции (Các phép toán cơ bản)**

1. **Операция взятия по модулю**
2. **Сложение по модулю (Cộng trong số học đồng dư)**
3. **Умножение по модулю (Nhân trong số học đồng dư)** 
4. **Возведение в степень по модулю (Lũy thừa trong số học đồng dư)**

### **Применения (Ứng dụng)**

* **Шифрование RSA** использует свойства модульной арифметики в вычислениях с большими числами.  
   *Mã hóa RSA sử dụng tính chất của số học đồng dư trong các phép tính với số lớn.*
* **Циклические часы** работают по модулю 12 или 24.  
   *Đồng hồ tuần hoàn hoạt động theo mô-đun 12 hoặc 24.*
* **Проверка контрольных сумм** в номерах банковских карт, штрих-кодах.  
   *Kiểm tra mã kiểm tra trong số thẻ ngân hàng, mã vạch.*

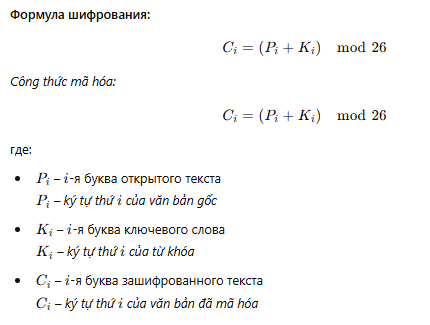
Модульная арифметика – основа многих криптографических алгоритмов и используется в программировании, компьютерных науках и теории чисел.  
 *Số học đồng dư là nền tảng của nhiều thuật toán mật mã và được sử dụng trong lập trình, khoa học máy tính và lý thuyết số.*

## **7. Шифр Виженера. Тест Казисского**

### **Шифр Виженера (Mã Vigenère)**

**Определение:** Шифр Виженера – это полиалфавитный шифр замены, в котором каждый символ открытого текста заменяется символом, определяемым ключевым словом.  
 *Mã Vigenère là một mã thay thế đa bảng chữ cái, trong đó mỗi ký tự của văn bản gốc được thay thế bằng một ký tự xác định bởi từ khóa.*

**Формула шифрования:**

* 

### **Пример шифрования (Ví dụ mã hóa)**



### **Тест Казисского (Phương pháp kiểm tra Kasiski)**

**Определение:** Тест Казисского – это метод криптоанализа шифра Виженера, который помогает определить длину ключа.  
 *Phương pháp Kasiski là một phương pháp phân tích mật mã của mã Vigenère, giúp xác định độ dài của từ khóa.*

**Шаги атаки (Các bước thực hiện):**

1. **Поиск повторяющихся фрагментов текста**
   * В зашифрованном тексте ищут повторяющиеся последовательности букв.  
      *Tìm các chuỗi ký tự lặp lại trong văn bản mã hóa.*
2. **Определение расстояний между повторами**
   * Записывают расстояния между этими повторами.  
      *Ghi lại khoảng cách giữa các lần lặp.*
3. **Поиск общих делителей**
   * Находят наибольший общий делитель (НОД) между расстояниями, который может указывать на длину ключа.  
      *Tìm ước số chung lớn nhất (ƯCLN) của các khoảng cách, có thể là độ dài của từ khóa.*

**Пример атаки (Ví dụ về tấn công):**

* Зашифрованный текст:  
   **"LXFOPV EF RNHR"** *Văn bản mã hóa:* ***"LXFOPV EF RNHR"***
* Повторяющаяся последовательность: **"EF"** *Chuỗi lặp lại:* ***"EF"***
* Расстояние между повторами: **9** *Khoảng cách giữa các lần lặp:* ***9***
* Возможная длина ключа: **9 или его делители (3, 9 и т. д.)** *Độ dài từ khóa có thể là* ***9 hoặc ước số của nó (3, 9, v.v.)***

После определения длины ключа можно разбирать текст на группы и применять частотный анализ для восстановления ключа.  
 *Sau khi xác định độ dài từ khóa, có thể chia văn bản thành các nhóm và áp dụng phân tích tần suất để khôi phục từ khóa.*

### **Защита от атаки Казисского (Cách bảo vệ khỏi phương pháp Kasiski)**

* Использование **случайного ключа**, длина которого больше текста.  
   *Sử dụng từ khóa ngẫu nhiên có độ dài lớn hơn văn bản.*
* Применение **шифра Вернама**, который делает анализ невозможным.  
   *Áp dụng mã Vernam, khiến phân tích trở nên không khả thi.*
* Использование **дополнительных перестановок** для усложнения анализа.  
   *Sử dụng hoán vị bổ sung để làm phức tạp quá trình phân tích.*

Шифр Виженера считается исторически важным, но устаревшим методом шифрования, поскольку его можно взломать с помощью анализа частоты и теста Казисского.  
 *Mã Vigenère được coi là một phương pháp mã hóa quan trọng về mặt lịch sử nhưng đã lỗi thời, vì có thể bị phá bằng phân tích tần suất và phương pháp Kasiski.*

## **8. Принцип Кергоффса**

### **Принцип Кергоффса (Nguyên tắc Kerckhoffs)**

**Определение:** Принцип Кергоффса утверждает, что безопасность криптосистемы не должна зависеть от сохранения в тайне алгоритма шифрования, а только от секретности ключа.  
 *Nguyên tắc Kerckhoffs khẳng định rằng tính bảo mật của một hệ thống mật mã không nên phụ thuộc vào việc giữ bí mật thuật toán mã hóa, mà chỉ dựa vào việc bảo vệ khóa bí mật.*

### **Формулировка принципа (Công thức nguyên tắc)**

В 1883 году Огюст Кергоффс сформулировал несколько требований к криптографическим системам, среди которых главное:

*«Система должна быть безопасной, даже если все её детали, кроме ключа, известны противнику.»* *"Hệ thống phải an toàn ngay cả khi mọi chi tiết của nó, ngoại trừ khóa, đều bị đối thủ biết."*

Это означает, что алгоритм шифрования может быть публичным, но его безопасность должна обеспечиваться исключительно за счет секретного ключа.  
 *Điều này có nghĩa là thuật toán mã hóa có thể công khai, nhưng tính bảo mật của nó phải được đảm bảo hoàn toàn bởi khóa bí mật.*

### **Примеры (Ví dụ)**

✅ **Соответствуют принципу Кергоффса:**

1. **AES (Advanced Encryption Standard)** – алгоритм известен, но без ключа его невозможно взломать.  
    *AES (Tiêu chuẩn mã hóa nâng cao) – thuật toán được công khai, nhưng không thể phá nếu không có khóa.*
2. **RSA** – широко используемый алгоритм асимметричного шифрования, основанный на сложности факторизации больших чисел.  
    *RSA – một thuật toán mã hóa bất đối xứng phổ biến dựa trên độ khó của việc phân tích số nguyên lớn.*

❌ **Нарушают принцип Кергоффса:**

1. **Собственные закрытые алгоритмы компаний** – если алгоритм будет раскрыт, безопасность системы рухнет.  
    *Các thuật toán mã hóa độc quyền của công ty – nếu thuật toán bị lộ, hệ thống sẽ mất an toàn.*
2. **Шифры с «секретным» методом защиты** – такие системы уязвимы к обратному проектированию.  
    *Các mã hóa với phương pháp bảo vệ "bí mật" – những hệ thống này dễ bị tấn công ngược.*

### **Значение принципа (Ý nghĩa của nguyên tắc)**

✅ **Простота проверки** – открытые алгоритмы можно анализировать на безопасность.  
 *Dễ kiểm tra – các thuật toán công khai có thể được phân tích về mức độ an toàn.* ✅ **Надежность** – даже если алгоритм станет известен, безопасность не будет нарушена.  
 *Đáng tin cậy – ngay cả khi thuật toán bị lộ, tính bảo mật vẫn không bị ảnh hưởng.* ✅ **Устойчивость к атакам** – криптоаналитики могут проверять и улучшать алгоритмы.  
 *Chống tấn công – các nhà phân tích mật mã có thể kiểm tra và cải thiện thuật toán.*

Принцип Кергоффса остается фундаментальным в современной криптографии и используется при разработке защищенных систем.  
 *Nguyên tắc Kerckhoffs vẫn là nền tảng trong mật mã hiện đại và được áp dụng khi thiết kế các hệ thống bảo mật.*

## **9. Роторные машины. Краткое описание принципа работы и внутренней структуры. Пространство ключей роторной машины.**

*Máy quay. Mô tả ngắn gọn về nguyên lý hoạt động và cấu trúc bên trong. Không gian phím máy quay*

### **Роторные машины (Máy mã hóa rotor)**

Роторные машины – это электромеханические устройства, использовавшиеся для шифрования и дешифрования сообщений в первой половине XX века.  
 *Máy mã hóa rotor là các thiết bị điện cơ được sử dụng để mã hóa và giải mã thông điệp trong nửa đầu thế kỷ XX.*

Они широко применялись в военной и дипломатической связи, наиболее известной является **немецкая машина "Энигма" (Enigma)**.  
 *Chúng được sử dụng rộng rãi trong thông tin liên lạc quân sự và ngoại giao, nổi tiếng nhất là* ***máy "Enigma" của Đức***.

### **Принцип работы (Nguyên lý hoạt động)**

1. **Ввод символа (Nhập ký tự)**
   * Оператор нажимает клавишу на клавиатуре.  
      *Người vận hành nhấn một phím trên bàn phím.*
2. **Прохождение через роторы (Truyền qua các rotor)**
   * Электрический сигнал проходит через серию вращающихся роторов, изменяя путь при каждом вводе.  
      *Tín hiệu điện đi qua một loạt rotor quay, thay đổi lộ trình mỗi lần nhập ký tự.*
3. **Отражатель (Bộ phản chiếu)**
   * Сигнал проходит через отражающий диск, который перенаправляет его обратно через роторы.  
      *Tín hiệu đi qua một bộ phản chiếu, sau đó được chuyển hướng quay lại qua các rotor.*
4. **Вывод символа (Xuất ký tự)**
   * Закодированная буква загорается на индикаторной панели.  
      *Chữ cái đã mã hóa sáng lên trên bảng hiển thị.*

Каждый нажатый символ приводит к вращению роторов, изменяя схему шифрования.  
 *Mỗi lần nhập ký tự sẽ làm các rotor xoay, thay đổi cách mã hóa.*

### **Внутренняя структура (Cấu trúc bên trong)**

1. **Клавиатура (Bàn phím)** – ввод исходного текста.  
    *Dùng để nhập văn bản gốc.*
2. **Роторы (Rotor)** – основные элементы шифрования, меняют сигнал по сложному пути.  
    *Các bộ phận chính của mã hóa, thay đổi tín hiệu theo đường dẫn phức tạp.*
3. **Отражатель (Bộ phản chiếu)** – перенаправляет сигнал обратно через роторы, создавая симметричное шифрование.  
    *Chuyển hướng tín hiệu quay lại qua các rotor, tạo ra mã hóa đối xứng.*
4. **Ламповая панель (Bảng đèn hiển thị)** – показывает зашифрованные символы.  
    *Hiển thị ký tự đã mã hóa.*
5. **Соединительные кабели (Dây cắm kết nối)** – в некоторых моделях (например, Enigma) использовались для дополнительного усложнения схемы.  
    *Trong một số phiên bản (ví dụ, Enigma), dây cắm giúp làm phức tạp hơn cách mã hóa.*

### **Пространство ключей роторной машины (Không gian khóa của máy rotor)**

Пространство ключей определяется следующими параметрами:  
 *Không gian khóa được xác định bởi các yếu tố sau:*

1. **Количество и типы роторов (Số lượng và loại rotor)**
   * Например, в Enigma использовались 3-5 роторов, каждый из которых можно было переставлять.  
      *Ví dụ, máy Enigma sử dụng 3-5 rotor, có thể sắp xếp theo nhiều cách khác nhau.*
2. **Начальные позиции роторов (Vị trí ban đầu của rotor)**
   * Каждому ротору можно было задать определенное начальное положение.  
      *Mỗi rotor có thể được đặt ở một vị trí ban đầu khác nhau.*
3. **Настройки коммутационной панели (Cấu hình bảng cắm dây)**
   * В некоторых моделях использовались сменные соединения между буквами.  
      *Một số phiên bản có bảng cắm dây thay đổi kết nối giữa các chữ cái.*
4. **Механизм вращения роторов (Cơ chế quay của rotor)**
   * Каждый раз при вводе символа роторы поворачивались в определенной последовательности.  
      *Mỗi lần nhập ký tự, các rotor quay theo một trình tự nhất định.*

## **10. Криптостойкость. Вычислительная(практическая) и математическая(теоретическая) криптостойкость.**

Khả năng chống lại mật mã. Khả năng chống lại mật mã tính toán (thực tế) và toán học (lý thuyết).

### **Криптостойкость (Độ bền mật mã)**

**Криптостойкость** – это способность криптографического алгоритма противостоять взлому, то есть расшифровке данных без знания ключа.  
 ***Độ bền mật mã*** là khả năng của một thuật toán mật mã chống lại việc bị bẻ khóa, tức là giải mã dữ liệu mà không cần biết khóa bí mật.

Она зависит от **математических свойств алгоритма**, сложности атак и возможностей вычислительных устройств.  
 *Nó phụ thuộc vào* ***tính chất toán học của thuật toán****, độ phức tạp của các cuộc tấn công và khả năng tính toán của thiết bị.*

### **1. Вычислительная (практическая) криптостойкость (Độ bền mật mã tính toán - thực tế)**

Это мера того, **насколько сложно взломать шифр с учетом современных вычислительных ресурсов**.  
 *Đây là thước đo* ***độ khó của việc bẻ khóa mật mã dựa trên tài nguyên tính toán hiện tại****.*

🔹 **Принципы (Nguyên tắc):** ✔️ Если на взлом уходит **неприемлемо долгое время**, алгоритм считается безопасным.  
 *Nếu việc bẻ khóa mất* ***một khoảng thời gian không thể chấp nhận được****, thuật toán được coi là an toàn.* ✔️ Криптостойкость зависит от **мощности компьютеров и методов атаки**.  
 *Độ bền mật mã phụ thuộc vào* ***sức mạnh tính toán của máy tính và phương pháp tấn công****.* ✔️ При появлении **квантовых компьютеров** некоторые алгоритмы могут стать уязвимыми.  
 *Với sự xuất hiện của* ***máy tính lượng tử****, một số thuật toán có thể trở nên dễ bị tấn công hơn.*

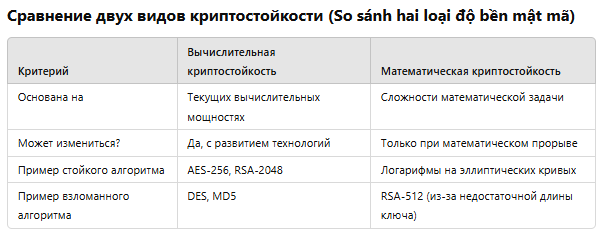
🔹 **Примеры (Ví dụ):** ✅ **AES-256** считается вычислительно стойким, так как даже суперкомпьютерам потребуется миллиарды лет на его взлом.  
 *AES-256 được coi là có độ bền mật mã cao vì ngay cả siêu máy tính cũng cần hàng tỷ năm để bẻ khóa nó.* ✅ **RSA-2048** – взлом требует огромных вычислительных мощностей.  
 *RSA-2048 – bẻ khóa nó đòi hỏi sức mạnh tính toán cực lớn.* ❌ **DES (56 бит)** – взломан с использованием мощных компьютеров в течение нескольких часов.  
 *DES (56 bit) đã bị bẻ khóa trong vài giờ bằng cách sử dụng các siêu máy tính mạnh mẽ.*

### **2. Математическая (теоретическая) криптостойкость (Độ bền mật mã toán học - lý thuyết)**

Это стойкость алгоритма, **основанная на сложных математических проблемах**, которые трудно решить даже при бесконечных ресурсах.  
 *Đây là độ bền mật mã* ***dựa trên các bài toán toán học phức tạp****, rất khó giải ngay cả khi có tài nguyên vô hạn.*

🔹 **Принципы (Nguyên tắc):** ✔️ Если алгоритм основан на **NP-трудной задаче**, его взлом считается невозможным без прорыва в математике.  
 *Nếu thuật toán dựa trên* ***bài toán thuộc lớp NP-khó****, thì việc bẻ khóa nó được coi là không khả thi trừ khi có đột phá toán học.* ✔️ Некоторые алгоритмы могут быть **теоретически взломаны**, но на практике атака занимает миллионы лет.  
 *Một số thuật toán* ***có thể bị phá lý thuyết****, nhưng trên thực tế, việc tấn công có thể mất hàng triệu năm.*

🔹 **Примеры (Ví dụ):** ✅ **RSA** основан на сложности разложения больших чисел на простые множители.  
 *RSA dựa trên độ khó của bài toán phân tích số nguyên lớn thành thừa số nguyên tố.* ✅ **ECC (эллиптические кривые)** – безопасность зависит от сложности логарифма на эллиптических кривых.  
 *ECC (mật mã đường cong elliptic) dựa trên độ khó của bài toán logarit trên đường cong elliptic.* ❌ Если найдется эффективный алгоритм решения **дискретного логарифма**, многие системы перестанут быть безопасными.  
 *Nếu có thuật toán hiệu quả để giải* ***bài toán logarit rời rạc****, nhiều hệ thống mật mã sẽ không còn an toàn nữa.*



## **11. Примеры криптосистемы этапа математической криптографии.**

*Ví dụ về hệ thống mật mã ở giai đoạn mật mã toán học.*

### **Примеры криптосистем этапа математической криптографии**

### ***(Các ví dụ về hệ thống mật mã thuộc giai đoạn mật mã toán học)***

**Математическая криптография** – это современный этап развития криптографии, основанный на сложных математических задачах.  
 ***Mật mã toán học*** là giai đoạn phát triển hiện đại của mật mã, dựa trên các bài toán toán học phức tạp.

Эти криптосистемы обладают **теоретической стойкостью**, то есть их безопасность зависит от сложности определенных математических проблем.  
 *Những hệ thống mật mã này có* ***độ bền lý thuyết****, nghĩa là tính bảo mật của chúng phụ thuộc vào độ khó của các bài toán toán học nhất định.*

### **1. RSA (Rivest–Shamir–Adleman)**

🔹 **Принцип работы (Nguyên lý hoạt động)** ✅ Основан на **сложности разложения больших чисел на простые множители**.  
 *Dựa trên* ***độ khó của việc phân tích một số nguyên lớn thành các thừa số nguyên tố****.* ✅ Открытый ключ содержит произведение двух больших простых чисел, а закрытый ключ связан с их факторизацией.  
 *Khóa công khai chứa tích của hai số nguyên tố lớn, trong khi khóa bí mật phụ thuộc vào việc phân tích chúng.*

🔹 **Применение (Ứng dụng)** ✔️ Используется в **шифровании, цифровых подписях, защищенной передаче данных**.  
 *Được sử dụng trong* ***mã hóa, chữ ký số, truyền dữ liệu an toàn****.* ✔️ Встречается в **SSL/TLS (защита интернета), PGP (шифрование электронной почты)**.  
 *Xuất hiện trong* ***SSL/TLS (bảo mật internet), PGP (mã hóa email)****.*

🔹 **Уязвимости (Lỗ hổng)** ❌ **Маленькие ключи (<1024 бит)** могут быть взломаны методом факторизации.  
 *Khóa* ***quá ngắn (<1024 bit)*** *có thể bị bẻ khóa bằng phương pháp phân tích số nguyên.* ❌ Квантовые компьютеры (алгоритм Шора) могут полностью взломать RSA.  
 *Máy tính lượng tử (thuật toán Shor) có thể bẻ khóa hoàn toàn RSA.*

### **2. ECC (Elliptic Curve Cryptography – криптография на эллиптических кривых)**

🔹 **Принцип работы (Nguyên lý hoạt động)** ✅ Основан на **сложности вычисления дискретного логарифма на эллиптических кривых**.  
 *Dựa trên* ***độ khó của bài toán logarit rời rạc trên đường cong elliptic****.* ✅ Дает **такую же безопасность, как RSA, но при меньшей длине ключа** (например, ECC-256 ≈ RSA-3072).  
 *Cung cấp* ***độ bảo mật tương đương RSA nhưng với độ dài khóa ngắn hơn*** *(ví dụ, ECC-256 ≈ RSA-3072).*

🔹 **Применение (Ứng dụng)** ✔️ Используется в **блокчейне (Bitcoin, Ethereum), мессенджерах (Signal, WhatsApp)**.  
 *Được sử dụng trong* ***blockchain (Bitcoin, Ethereum), ứng dụng nhắn tin (Signal, WhatsApp)****.* ✔️ Встречается в **TLS, SSH, цифровых подписях**.  
 *Xuất hiện trong* ***TLS, SSH, chữ ký số****.*

🔹 **Уязвимости (Lỗ hổng)** ❌ Квантовые атаки (алгоритм Шора) смогут взломать ECC.  
 *Tấn công lượng tử (thuật toán Shor) có thể phá ECC.* ❌ Некорректный выбор параметров кривых может привести к слабостям.  
 *Việc chọn sai tham số đường cong có thể tạo ra điểm yếu bảo mật.*

### **3. Алгоритм Диффи-Хеллмана (Diffie-Hellman Key Exchange – обмен ключами)**

🔹 **Принцип работы (Nguyên lý hoạt động)** ✅ Позволяет двум сторонам **создать общий секретный ключ через незащищенный канал**.  
 *Cho phép hai bên* ***tạo khóa bí mật chung thông qua kênh không an toàn****.* ✅ Основан на **сложности вычисления дискретного логарифма**.  
 *Dựa trên* ***độ khó của bài toán logarit rời rạc****.*

🔹 **Применение (Ứng dụng)** ✔️ Используется в **TLS (HTTPS), VPN, протоколах безопасности**.  
 *Được dùng trong* ***TLS (HTTPS), VPN, các giao thức bảo mật****.* ✔️ Встречается в **мессенджерах и PGP**.  
 *Xuất hiện trong* ***các ứng dụng nhắn tin và PGP****.*

🔹 **Уязвимости (Lỗ hổng)** ❌ **Маленькие простые числа** делают алгоритм уязвимым.  
 *Nếu chọn* ***số nguyên tố nhỏ****, thuật toán có thể bị tấn công.* ❌ **Квантовые компьютеры (алгоритм Шора)** смогут его взломать.  
 *Máy tính lượng tử (thuật toán Shor) có thể phá Diffie-Hellman.*

### **4. Постквантовые алгоритмы (Mật mã hậu lượng tử)**

🔹 **Принцип работы (Nguyên lý hoạt động)** ✅ Разрабатываются для защиты от **квантовых атак**.  
 *Được phát triển để bảo vệ khỏi* ***các cuộc tấn công lượng tử****.* ✅ Основаны на **сложных математических задачах, не решаемых квантовыми компьютерами**.  
 *Dựa trên* ***các bài toán toán học phức tạp mà máy tính lượng tử không thể giải quyết****.*

🔹 **Примеры (Ví dụ)** ✅ **Lattice-based криптография** (основана на сложных задачах решеток).  
 *Mật mã dựa trên* ***lưới số học*** *(dựa trên các bài toán lưới phức tạp).* ✅ **Hash-based подписи** (используют криптографические хеш-функции).  
 *Chữ ký số dựa trên* ***hàm băm mật mã****.*

🔹 **Применение (Ứng dụng)** ✔️ Активно тестируются для будущих стандартов (например, NIST PQC).  
 *Đang được thử nghiệm để trở thành tiêu chuẩn trong tương lai (ví dụ, NIST PQC).*

## **12. Криптоанализ. Классический криптоанализ. SCA.**

### **Криптоанализ (Phân tích mật mã)**

**Криптоанализ** – это наука о методах взлома криптографических систем без знания ключа.  
 ***Phân tích mật mã*** là khoa học nghiên cứu các phương pháp phá vỡ hệ thống mật mã mà không cần biết khóa bí mật.

Цель криптоанализа – **найти слабости в алгоритме шифрования** или способ его обхода.  
 *Mục tiêu của phân tích mật mã là* ***tìm ra điểm yếu trong thuật toán mã hóa*** *hoặc cách vượt qua nó.*

## **1. Классический криптоанализ (Phân tích mật mã cổ điển)**

**Классический криптоанализ** изучает методы взлома традиционных (доцифровых) шифров.  
 ***Phân tích mật mã cổ điển*** nghiên cứu các phương pháp phá vỡ các thuật toán mã hóa truyền thống (trước thời đại số hóa).

🔹 **Основные методы (Các phương pháp chính):** ✔️ **Частотный анализ** – изучение частоты встречаемости символов в шифртексте.  
 *Phân tích tần suất – nghiên cứu tần suất xuất hiện của các ký tự trong bản mã.* ✔️ **Анализ биграмм и триграмм** – поиск часто встречающихся комбинаций букв.  
 *Phân tích bigram và trigram – tìm kiếm các cặp hoặc bộ ba ký tự phổ biến.* ✔️ **Методы проб и ошибок** – подбор ключей вручную на основе знаний о языке.  
 *Phương pháp thử và sai – thử nghiệm các khóa dựa trên hiểu biết về ngôn ngữ.*

🔹 **Примеры атак (Các cuộc tấn công tiêu biểu):** ✅ **Взлом шифра Цезаря** – частотный анализ быстро выявляет смещение символов.  
 *Bẻ khóa mã Caesar – phân tích tần suất có thể nhanh chóng xác định độ dịch chuyển.* ✅ **Взлом шифра Виженера** – метод Казисского помогает определить длину ключа.  
 *Bẻ khóa mã Vigenère – phương pháp Kasiski giúp xác định độ dài khóa.*

🔹 **Ограничения (Hạn chế):** ❌ Современные алгоритмы не уязвимы к классическому криптоанализу.  
 *Các thuật toán hiện đại không dễ bị tấn công bằng phân tích mật mã cổ điển.*

## **2. Современный криптоанализ (Phân tích mật mã hiện đại)**

🔹 **Методы (Các phương pháp):** ✔️ **Атака полного перебора (Brute-force attack)** – проверка всех возможных ключей.  
 *Tấn công vét cạn – thử tất cả các khóa có thể.* ✔️ **Дифференциальный криптоанализ** – анализ изменений в шифрованном тексте при малых изменениях входных данных.  
 *Phân tích vi phân – nghiên cứu cách thay đổi nhỏ trong dữ liệu đầu vào ảnh hưởng đến bản mã.* ✔️ **Линейный криптоанализ** – поиск линейных зависимостей между открытым текстом и шифротекстом.  
 *Phân tích tuyến tính – tìm kiếm mối quan hệ tuyến tính giữa bản rõ và bản mã.*

🔹 **Примеры атак (Các cuộc tấn công tiêu biểu):** ✅ **Дифференциальный анализ DES** – позволил обнаружить уязвимости в ранних версиях алгоритма.  
 *Phân tích vi phân DES – giúp tìm ra điểm yếu trong các phiên bản đầu tiên của thuật toán.* ✅ **Линейный анализ AES** – помогает находить слабые ключи.  
 *Phân tích tuyến tính AES – giúp phát hiện các khóa yếu.*

🔹 **Ограничения (Hạn chế):** ❌ Современные алгоритмы (AES, RSA) защищены от большинства классических атак.  
 *Các thuật toán hiện đại (AES, RSA) được thiết kế để chống lại hầu hết các cuộc tấn công cổ điển.*

## **3. SCA – Атаки по сторонним каналам (Phân tích kênh bên – Side-Channel Attacks)**

**SCA (Side-Channel Attacks)** – это атаки, использующие физические характеристики работы криптосистемы.  
 ***Tấn công kênh bên (SCA)*** là các cuộc tấn công khai thác các đặc điểm vật lý của hệ thống mật mã thay vì phân tích thuật toán.

🔹 **Основные методы (Các phương pháp chính):** ✔️ **Анализ времени выполнения (Timing Attack)** – измерение времени обработки операций.  
 *Phân tích thời gian thực thi – đo thời gian xử lý của hệ thống để suy luận về dữ liệu bên trong.* ✔️ **Электромагнитный анализ (Electromagnetic Analysis)** – исследование электромагнитных излучений устройства.  
 *Phân tích điện từ – nghiên cứu tín hiệu điện từ do thiết bị phát ra trong quá trình xử lý dữ liệu.* ✔️ **Атака по потреблению энергии (Power Analysis)** – измерение изменений потребления энергии при шифровании.  
 *Phân tích tiêu thụ điện – đo mức tiêu thụ năng lượng trong quá trình mã hóa để suy luận về khóa.*

🔹 **Примеры атак (Các cuộc tấn công tiêu biểu):** ✅ **Атака по времени на RSA** – позволяет угадать частные ключи на основе анализа задержек вычислений.  
 *Tấn công thời gian RSA – giúp đoán khóa bí mật bằng cách phân tích độ trễ tính toán.* ✅ **Атака по потреблению энергии на AES** – позволяет восстановить ключ шифрования.  
 *Tấn công tiêu thụ điện năng AES – có thể khôi phục khóa mã hóa.*

🔹 **Ограничения (Hạn chế):** ❌ Требует **физического доступа** к устройству.  
 *Cần có* ***quyền truy cập vật lý*** *vào thiết bị.* ❌ Можно защититься с помощью **защиты аппаратного уровня**.  
 *Có thể được bảo vệ bằng* ***các biện pháp phòng thủ phần cứng****.*

## **13. Свойство диффузии и конфузии. Их связь с элементарными операциями в шифрах (перестановка, замена, сдвиг)**

Tính chất khuếch tán và lẫn lộn. Mối liên hệ của chúng với các phép toán cơ bản trong mật mã (hoán vị, thay thế, dịch chuyển)

### **Свойство диффузии и конфузии (Tính khuếch tán và tính rối loạn)**

Диффузия и конфузия – два фундаментальных свойства безопасных шифров, предложенных Клодом Шенноном.  
 ***Khuếch tán và rối loạn*** là hai tính chất cơ bản của các thuật toán mã hóa an toàn, được đề xuất bởi Claude Shannon.

Они обеспечивают защиту шифра от криптоанализа, усложняя восстановление ключа или открытого текста.  
 *Chúng giúp bảo vệ mã hóa khỏi các cuộc tấn công mật mã bằng cách làm cho việc khôi phục khóa hoặc bản rõ trở nên khó khăn hơn.*

## **1. Диффузия (Diffusion – Tính khuếch tán)**

🔹 **Определение (Định nghĩa):** Диффузия означает, что **изменение одного бита входных данных должно приводить к изменению множества бит в выходных данных**.  
 *Tính khuếch tán có nghĩa là* ***một thay đổi nhỏ trong dữ liệu đầu vào sẽ gây ra sự thay đổi lớn trong dữ liệu đầu ra****.*

🔹 **Цель (Mục tiêu):**

* Размыть статистические зависимости между открытым текстом и шифротекстом.  
   *Làm mờ mối quan hệ thống kê giữa bản rõ và bản mã.*
* Усложнить частотный анализ.  
   *Làm cho phân tích tần suất trở nên khó khăn hơn.*

🔹 **Пример (Ví dụ):** В **AES** небольшое изменение в открытом тексте приводит к радикальным изменениям в шифртексте.  
 *Trong* ***AES****, một thay đổi nhỏ trong bản rõ sẽ tạo ra sự thay đổi lớn trong bản mã.*

🔹 **Как достигается? (Đạt được bằng cách nào?)** ✔️ **Перестановка (Permutation – Hoán vị)** – перемешивание бит или блоков данных.  
 *Hoán vị – trộn lẫn các bit hoặc khối dữ liệu để làm mất cấu trúc ban đầu.* ✔️ **Распространение изменений по всем битам данных** в нескольких раундах шифрования.  
 *Sự lan truyền thay đổi trên toàn bộ dữ liệu qua nhiều vòng mã hóa.*

## **2. Конфузия (Confusion – Tính rối loạn)**

🔹 **Определение (Định nghĩa):** Конфузия означает, что **связь между ключом шифрования и шифртекстом должна быть максимально сложной**.  
 *Tính rối loạn có nghĩa là* ***mối quan hệ giữa khóa mã hóa và bản mã phải thật phức tạp****.*

🔹 **Цель (Mục tiêu):**

* Усложнить криптоанализ ключа.  
   *Làm cho việc tấn công để tìm khóa trở nên khó khăn hơn.*
* Сделать влияние изменения ключа на шифртекст непредсказуемым.  
   *Làm cho sự ảnh hưởng của khóa đến bản mã không thể đoán trước.*

🔹 **Пример (Ví dụ):** В **RSA** сложно определить закрытый ключ по открытому ключу.  
 *Trong* ***RSA****, rất khó để xác định khóa riêng từ khóa công khai.*

🔹 **Как достигается? (Đạt được bằng cách nào?)** ✔️ **Замена (Substitution – Thay thế)** – использование нелинейных функций, таких как S-блоки в AES.  
 *Thay thế – sử dụng các hàm phi tuyến, chẳng hạn như hộp S trong AES.* ✔️ **Смешивание бит ключа с данными** (например, сдвиг и сложение по модулю).  
 *Trộn lẫn các bit của khóa với dữ liệu (chẳng hạn như dịch bit hoặc cộng theo modulo).*

## **3. Связь диффузии и конфузии с операциями в шифрах (Mối liên hệ giữa khuếch tán, rối loạn và các phép toán trong mã hóa)**

## 

## 🔹 В **AES** используются **S-блоки** (замена) для конфузии и **MixColumns** (перестановка) для диффузии. *Trong* ***AES****, hộp S được sử dụng để tạo rối loạn, còn MixColumns giúp khuếch tán dữ liệu.*

🔹 В **DES** чередуются **S-блоки** (замена) и **P-блоки** (перестановка) для достижения обоих свойств.  
 *Trong* ***DES****, các hộp S (thay thế) và hộp P (hoán vị) được kết hợp để đảm bảo cả hai tính chất.*

## **Заключение (Kết luận)**

✔️ **Диффузия** защищает от анализа структуры открытого текста.  
 *Khuếch tán giúp bảo vệ chống lại phân tích cấu trúc của bản rõ.*

✔️ **Конфузия** затрудняет восстановление ключа.  
 *Rối loạn làm phức tạp quá trình tìm khóa bí mật.*

✔️ В современных шифрах (AES, DES) **оба свойства используются вместе** для максимальной безопасности.  
 *Trong các thuật toán mã hóa hiện đại (AES, DES),* ***cả hai tính chất đều được kết hợp*** *để đảm bảo độ an toàn tối đa.*