**2. Các yếu tố cấu trúc cơ bản của thuật toán mã khối đối xứng DES**

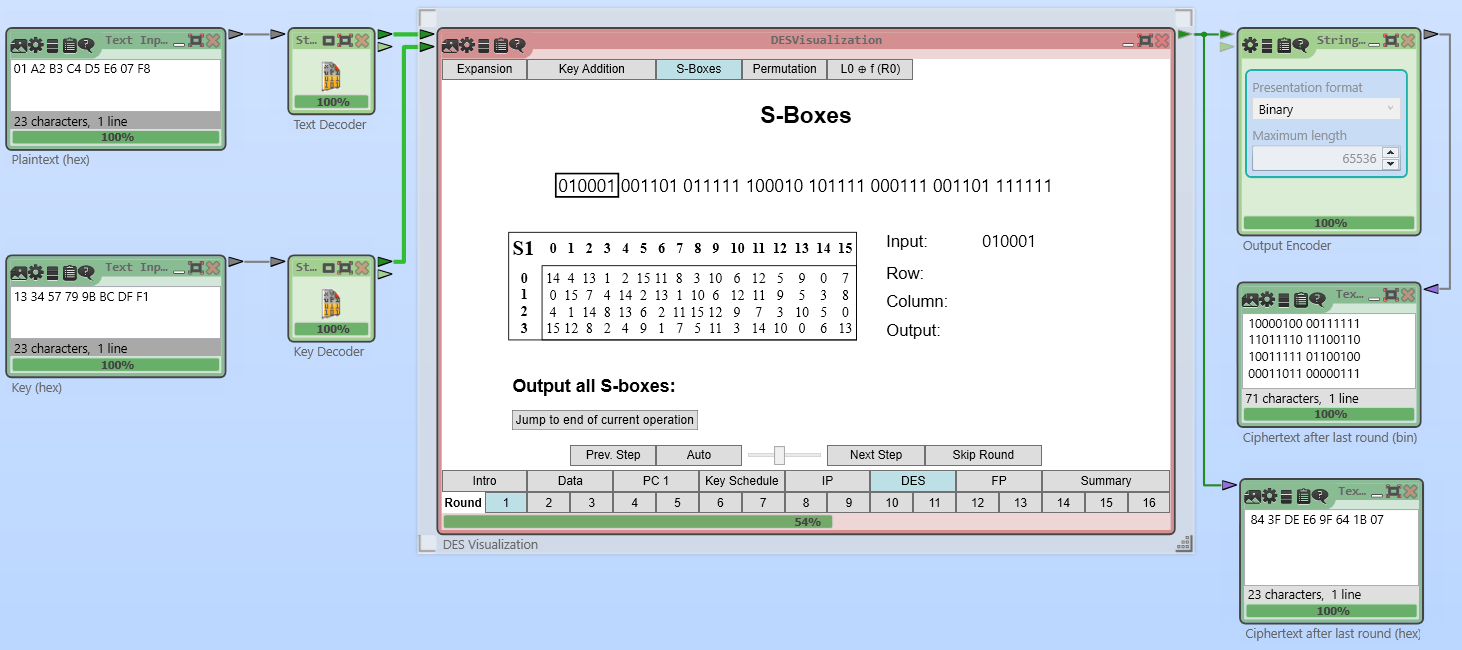
**Mục tiêu:** nghiên cứu các nguyên lý cơ bản của hoạt động của thuật toán DES.

**Nhiệm vụ của bài thực hành:**

1. Phân tích mô phỏng thuật toán DES và các cuộc tấn công sơ khai vào mã, sử dụng Cryptool 2. Xác định các thiết lập cần thiết chính của mã và những giới hạn yêu cầu đối với các tham số.
2. Thực hiện 1 chu kỳ của hàm vòng (round) của thuật toán DES thủ công, tức là thực hiện tất cả các hàm nằm trong hàm vòng của DES đối với một vector nhị phân đầu vào cố định, đồng thời hiển thị các giá trị trung gian của quá trình mã hóa. Ngoài ra, để nghiên cứu chi tiết hơn, có thể sử dụng một chương trình thực hiện 1 vòng (hoặc toàn bộ hệ thống) của DES trong chế độ gỡ lỗi, với việc hiển thị các giá trị trung gian của mã hóa.
3. Phân tích nguyên lý của tính không tuyến tính trong mật mã hiện đại trên ví dụ về thuật toán DES.

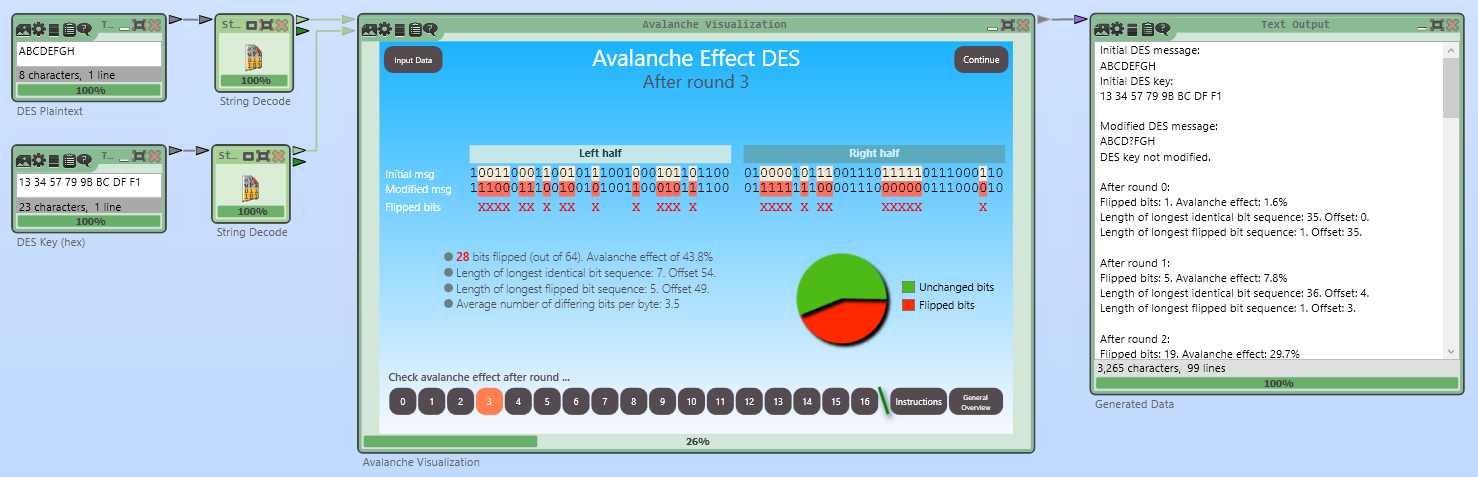
### **Trình tự thực hiện công việc:**

1. Để trực quan hóa thuật toán DES, đề xuất sử dụng mẫu trong chương trình Cryptool 2 (Templates -> cryptography -> modern -> symmetric -> DES Visualization). Hãy nhập dữ liệu đầu vào và khóa mã hóa của bạn vào mẫu này.



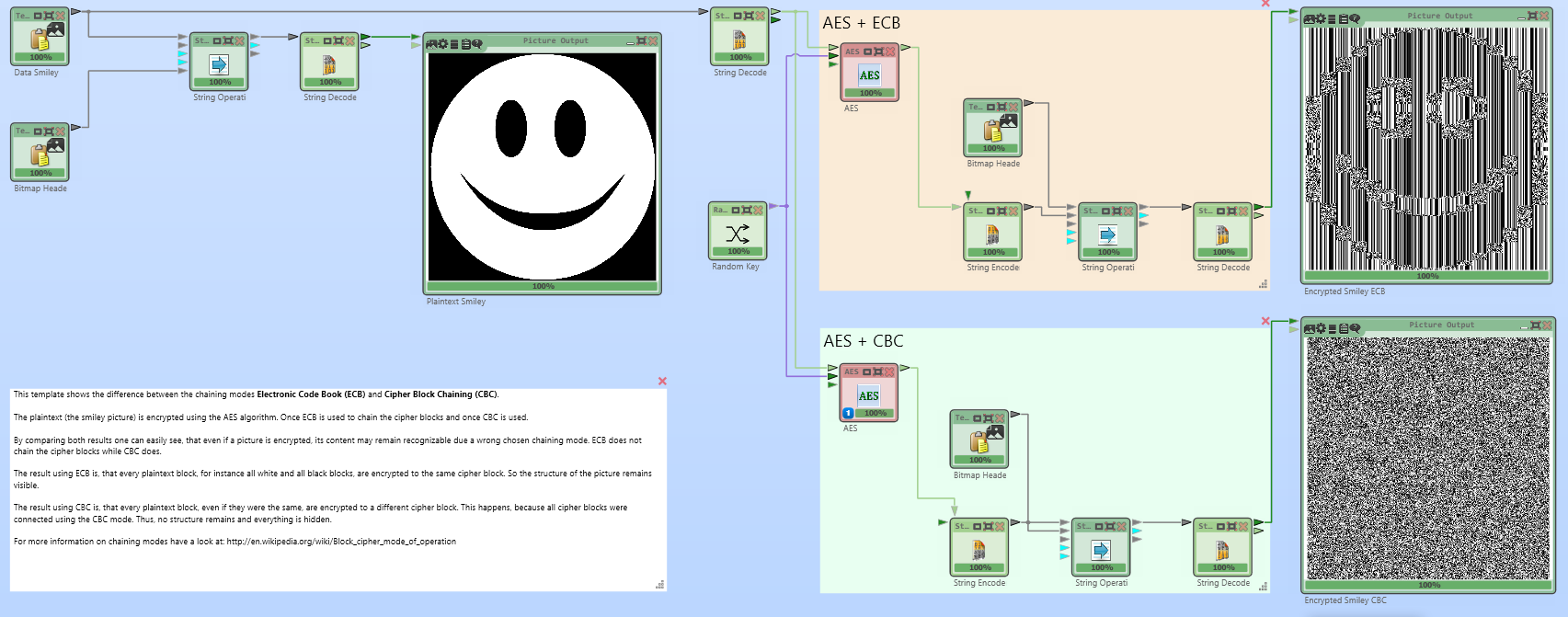
Hãy theo dõi quá trình mã hóa của thuật toán DES theo từng bước. Đặc biệt chú ý đến chức năng mở rộng khóa, cấu trúc mạng Feistel trong thuật toán DES, các bước của hàm vòng (hoán vị với mở rộng E, cộng với khóa, thay thế phi tuyến tính, hoán vị trực tiếp P). Ghi lại cách độ dài các khối con thay đổi sau mỗi vòng lặp.

1. **Trực quan hóa “hiệu ứng lở tuyết” (avalanche effect) của DES** (templates -> cryptoanalysis -> modern -> avalanche (DES)).  
    Theo dõi hiệu ứng lở tuyết trong quá trình mã hóa DES đối với giá trị văn bản gốc và khóa của bạn.



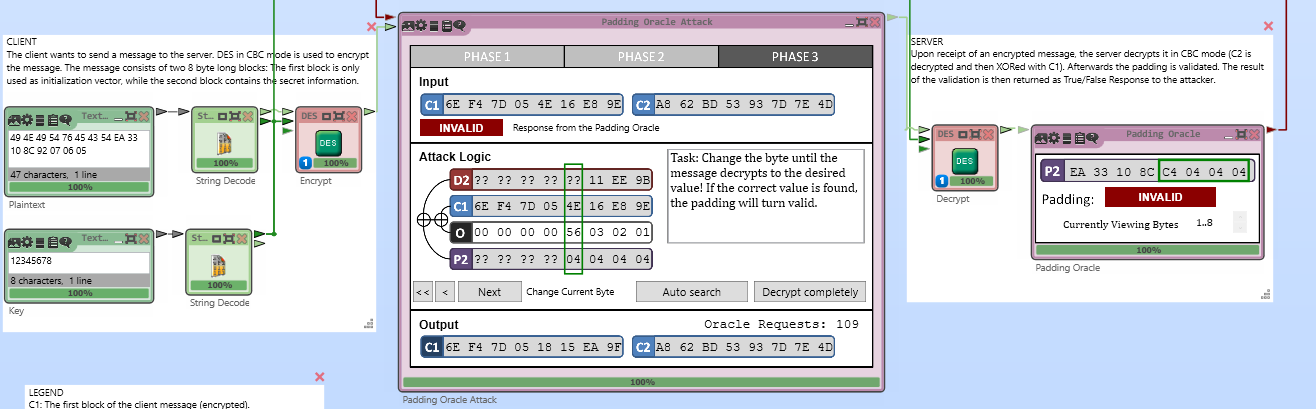
Ghi lại tỷ lệ phần trăm các bit bị thay đổi do quá trình mã hóa, tốc độ xảy ra hiệu ứng lở tuyết, đặc điểm của việc nhóm các giá trị bị biến đổi.  
 Gây ra biến đổi ở một vài bit và phân tích đặc điểm của hiệu ứng lở tuyết.  
 Gây ra biến đổi ở các giá trị trung gian của quá trình mã hóa tại vòng thứ 10, 12, và 14; theo dõi xem hiệu ứng lở tuyết đạt tới những giá trị nào.

1. **Nghiên cứu nguyên lý hoạt động của các chế độ mã hóa khác nhau của các mã khối đối xứng**, sử dụng mẫu trong **Cryptool 2**:  
    **Templates -> cryptography -> modern -> Block Modes of Symmetric Ciphers**.



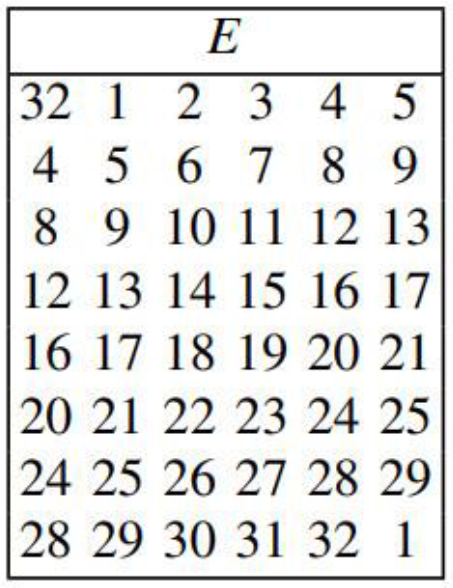
Ghi chú **mối nguy hiểm của việc sử dụng chế độ mã hóa ECB** xét từ góc độ **an toàn thông tin**.  
 Nghiên cứu các chế độ mã hóa khác và cách liên kết các khối (các chế độ: **CBC, CFB, OFB, RD, CTR, GCM**).

1. **Tiến hành tấn công padding oracle đối với thuật toán DES với các giá trị của bạn.** Xác định các bước thực hiện cuộc tấn công. **Đưa ra ví dụ về việc áp dụng cuộc tấn công này trong thực tế.**

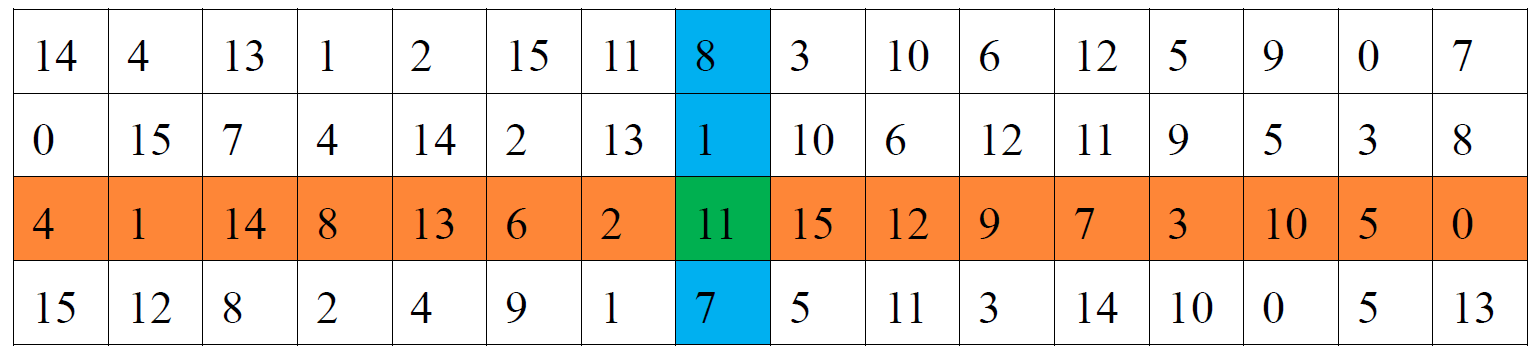


**5. Thực hiện thủ công 1 vòng của hàm vòng trong thuật toán DES.** Hãy tạo ngẫu nhiên một giá trị đầu vào dài 32 bit và một khóa vòng dài 48 bit. Trình bày cách thực hiện các thao tác sau trong thuật toán DES:

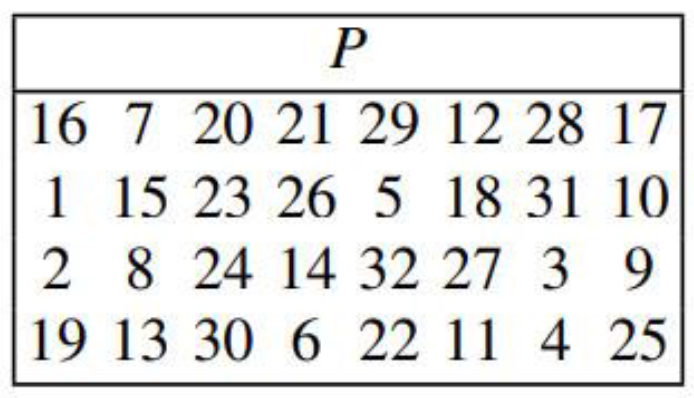
* Phép hoán vị mở rộng E (permutation with expansion E);



* Phép cộng bit với khóa (bitwise XOR with the key);
* Phép thay thế (S-box substitution);



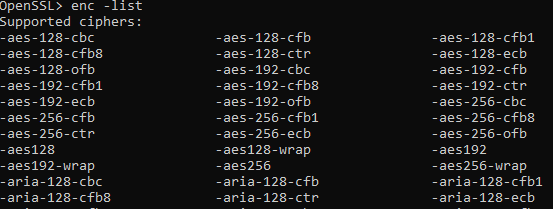
* Phép hoán vị trực tiếp P (permutation P).



Mô tả cách sử dụng các bảng thay thế và hoán vị được trình bày ở trên.  
 Kết quả thực hiện các thao tác với các giá trị đầu vào của bạn có thể được trình bày dưới các hình thức sau:

* Các trang báo cáo được quét lại, trên đó thể hiện quá trình mã hóa được thực hiện bằng tay;
* Các trang báo cáo với các bước mã hóa được soạn trên máy tính bằng bất kỳ trình soạn thảo văn bản nào;
* Các trang báo cáo chứa mã nguồn hoặc giả mã thực hiện các bước đã nêu của thuật toán.

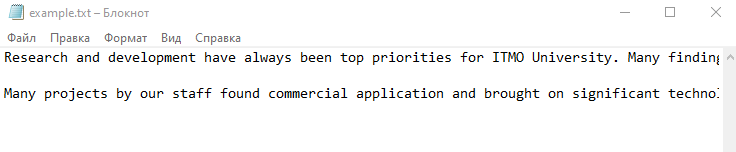
**6. Thực hiện mã hóa tệp bằng thư viện mật mã OpenSSL.** Để thực hiện việc này, sử dụng lệnh openssl enc -list để hiển thị danh sách các chuẩn mật mã khả dụng cho việc mã hóa.



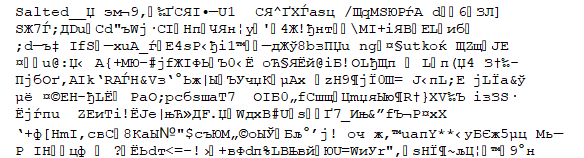
Chọn ít nhất **ba phương pháp mã hóa** có sử dụng thuật toán **DES**, ví dụ như sử dụng DES ở các chế độ mã hóa khác nhau hoặc một số biến thể của **3DES**.

Thiết lập giá trị đầu vào của bạn dưới dạng một **tệp tin** hoặc **chuỗi thông điệp trên dòng lệnh**, sau đó **mã hóa** chúng bằng **3 phương pháp mã hóa DES đã chọn**.





**Tệp example.txt.enc**, thu được sau khi mã hóa:



**Thực hiện giải mã tệp từ bước trước. Kiểm tra văn bản thu được sau khi giải mã để phát hiện lỗi. Phân tích các tùy chọn và tham số bổ sung cho mã hóa DES trong OpenSSL: -salt, -a, -k, -iter.**

**Các tùy chọn này ảnh hưởng như thế nào đến độ bền mật mã của thuật toán?**

**Phương án thay thế** của bài thực hành cho phép triển khai bằng lập trình một hệ mật mã khối đối xứng, dựa trên **mạng Feistel** (không nên nhầm lẫn giữa khái niệm mạng SP và mạng Feistel – mạng Feistel là một trường hợp riêng của mạng SP).  
 Đối với bài thực hành, chỉ cần **triển khai đầy đủ một thuật toán mã hóa** sử dụng mạng Feistel. Các quy trình chính cần phải thực hiện gồm:

* quá trình mã hóa;
* quá trình giải mã;
* quá trình mở rộng khóa (tức là tạo các khóa con từ khóa chính).

**Ví dụ về các thuật toán mã hóa dựa trên mạng Feistel** mà bạn có thể lựa chọn để triển khai:

* **DES**
* **ГОСТ 34.12** (phần 1, mã hóa với độ dài khối 64 bit) – thuật toán "Магма" (tên cũ là ГОСТ 28147)
* **RC6**
* **Blowfish**
* **FEAL**
* **KASUMI** (trong chuẩn GSM)

Một lựa chọn khác là **triển khai mã hóa dòng**, ví dụ như **bất kỳ thuật toán nào tham gia vào cuộc thi eStream**, có thể xem tại đây:  
<https://ru.wikipedia.org/wiki/ESTREAM>

**Câu hỏi bảo vệ**

1. Các mã khối đối xứng và mã dòng.
2. Mã dòng đồng bộ và không đồng bộ.
3. Các lĩnh vực ứng dụng của mã dòng.
4. Mã một lần dạng khối.
5. Thanh ghi dịch có phản hồi tuyến tính (LFSR).
6. Giao thức GSM A5/2.
7. Sự cần thiết của vector khởi tạo (IV) trong mã dòng.
8. Mã Trivium.
9. Mã Rabbit.
10. Các thuộc tính khuếch tán và nhiễu (confusion & diffusion) trong mã khối.
11. Mạng Feistel.
12. Thuật toán DES. Quy trình mã hóa/giải mã. Mở rộng khóa.
13. Kỹ thuật làm trắng khóa (key whitening).
14. 3DES.
15. Tiêu chuẩn GOST 28147 hoặc mã khối với độ dài khối 64 bit theo GOST 34.12.
16. Các chế độ mã hóa ECB, CBC, CFB, OFB, CTR, GCM. Khả năng chống lại các cuộc tấn công chèn và xóa khối. Hiệu ứng thác lũ (avalanche effect). Khả năng xử lý song song các khối.
17. Mã xác thực thông điệp (MAC).
18. Các sơ đồ băm dựa trên mã khối đối xứng.