### **Phân tích các mật mã lịch sử bằng công cụ phần mềm CrypTool 2.**

**Mục tiêu thực tiễn của nghiên cứu:** sử dụng công cụ phần mềm CrypTool 2 để nghiên cứu các nguyên tắc hoạt động của các mật mã lịch sử, cũng như thực hiện phân tích mật mã của chúng.

### **1. Nhiệm vụ nghiên cứu thực tiễn**

Sử dụng các chức năng của chương trình CrypTool 2, phân tích các nguyên lý mật mã sau:

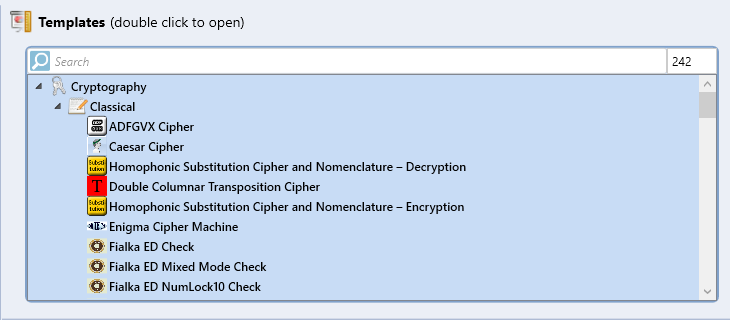
1. Mật mã Caesar, mật mã hoán vị và thay thế (ví dụ về mật mã đơn bảng);
2. Mật mã Vigenère (ví dụ về mật mã đa bảng);
3. Cấu trúc và quá trình mã hóa trong máy Enigma.

Việc nghiên cứu từng thuật toán mật mã được đề xuất theo kế hoạch nghiên cứu sau:

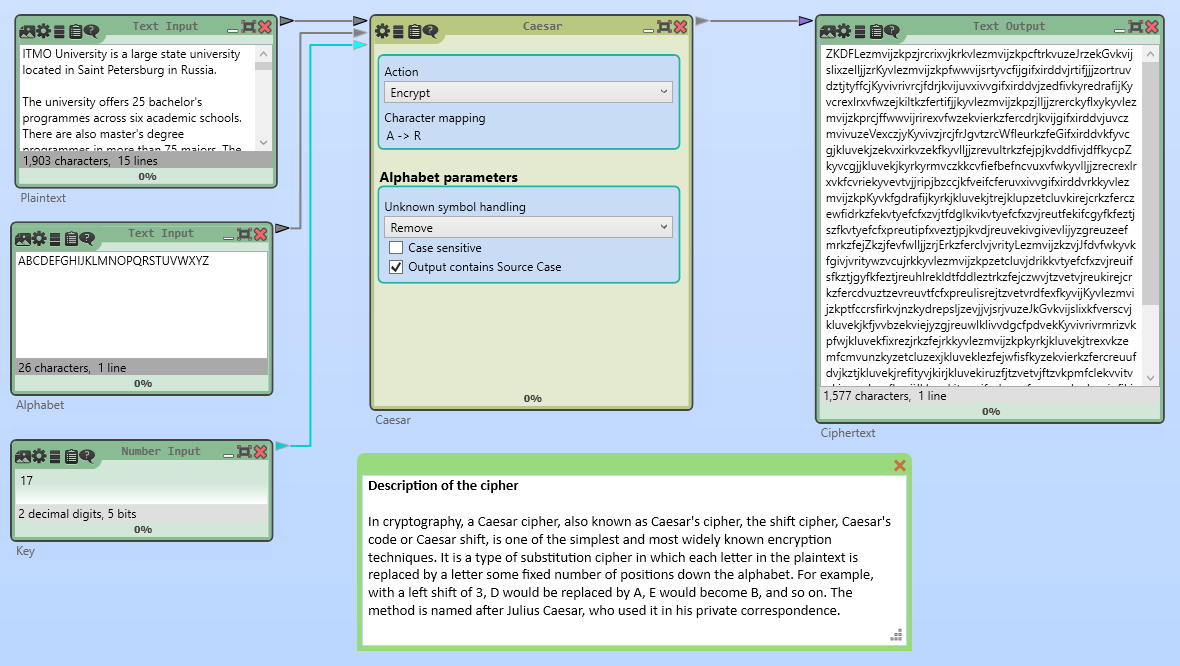
1. Thực hiện mã hóa một ví dụ về văn bản gốc với các cài đặt mật mã cá nhân. Nhận bản mã tương ứng với giá trị khóa được chỉ định. Nghiên cứu các thông số của hệ mật mã, cụ thể là: khả năng mở rộng không gian khóa, cơ chế bổ sung cho mã hóa và bảo vệ hệ thống mật mã, hạn chế và yêu cầu đối với các thông số mật mã (chẳng hạn như độ dài khóa mật mã, độ dài văn bản gốc và bản mã, các tham số, yêu cầu bắt buộc và khuyến nghị đối với cấu hình hệ mật mã).
2. Thực hiện giải mã văn bản mã hóa bằng khóa mật mã từ bước đầu tiên. Đánh giá mức độ khó của một cuộc tấn công vào hệ thống mật mã bằng phương pháp phân tích. Đánh giá độ phức tạp của quy trình mã hóa và cấu hình hệ thống mật mã để sử dụng (mã hóa/giải mã).
3. Thực hiện phân tích mật mã đơn giản bằng cách sử dụng các mẫu có sẵn trong CrypTool 2. Trong phân tích mật mã, có thể sử dụng một hoặc nhiều bản mã từ bước đầu tiên của kế hoạch nghiên cứu. Khi phân tích mật mã, giả định rằng khóa mật mã là không xác định và không có bất kỳ thông tin nào liên quan đến khóa. Các bản mã không có khóa mật mã có thể được thu thập ở giai đoạn mã hóa trong CrypTool 2 bằng cách ẩn trường nhập khóa.

### **2. Trình tự thực hiện công việc**

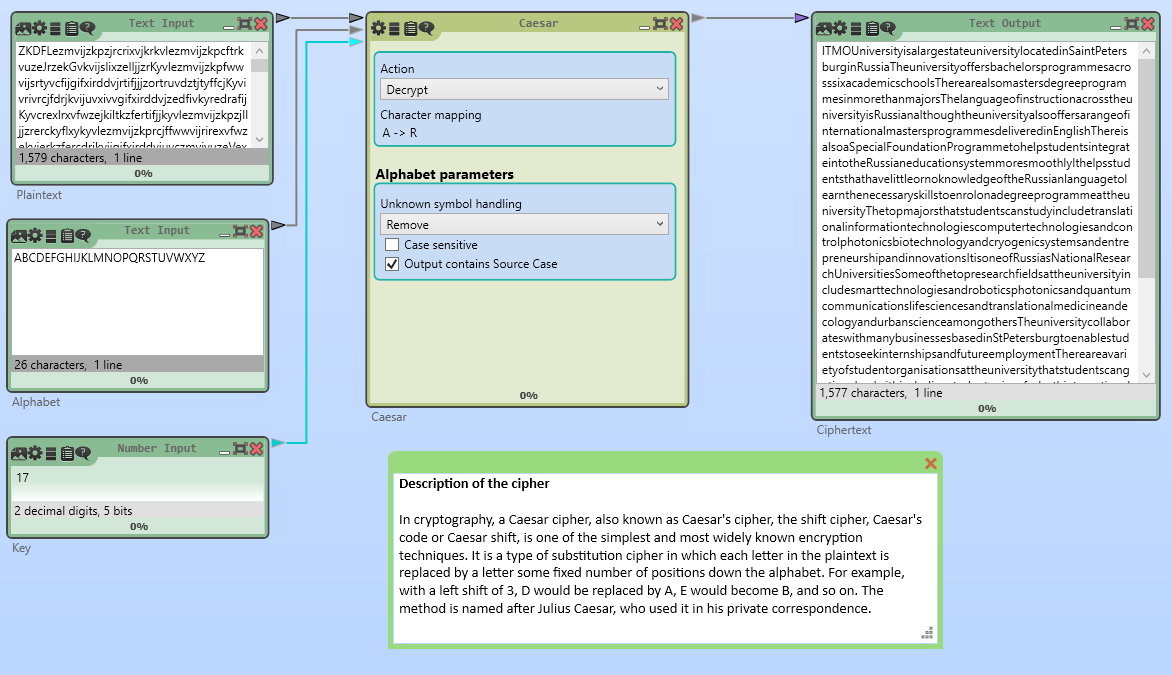
1. Thực hiện mã hóa văn bản gốc dựa trên ví dụ về hệ thống mật mã được triển khai trong phần mềm **CrypTool 2**.  
    Để mở mẫu tương ứng trong phần mềm, hãy chuyển đến mục **Templates**, sau đó vào thư mục con **Cryptography -> Classical -> Caesar Cipher**.



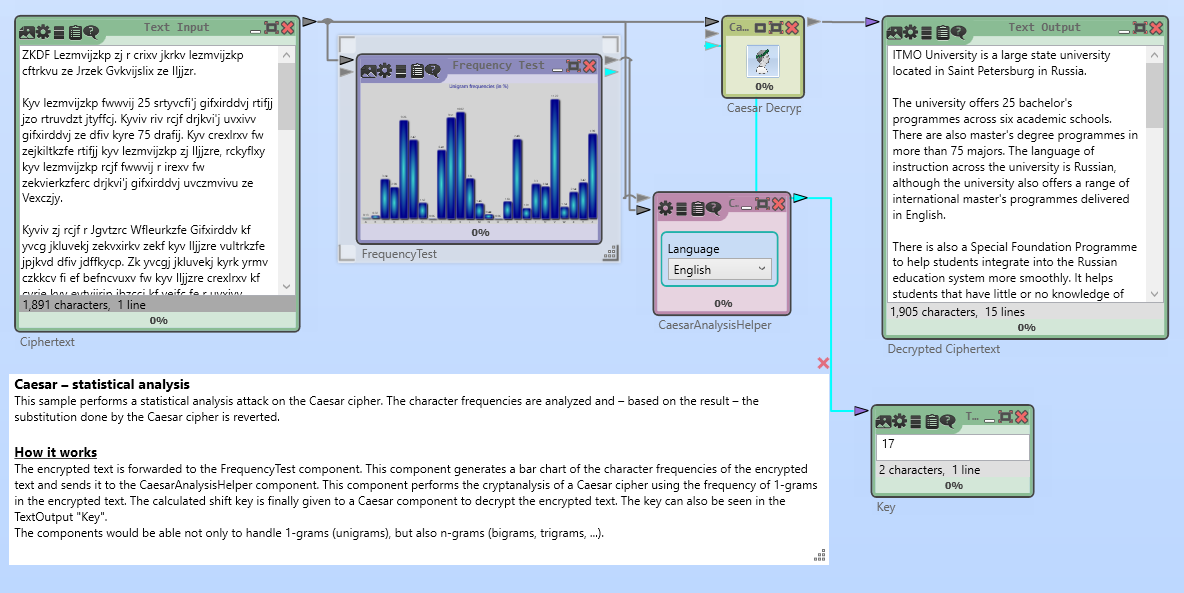
1. Mở mẫu mã hóa bằng **mật mã Caesar**. Nhập văn bản gốc của bạn vào trường **Plaintext**, nhập bảng chữ cái hợp lệ vào trường **Alphabet**, và đặt giá trị của **khóa mật mã**. Văn bản gốc và khóa sẽ do bạn tự chọn.  
    Để đảm bảo quá trình phân tích mật mã sau này diễn ra nhanh chóng và thành công, cần đảm bảo văn bản gốc có độ dài càng lớn càng tốt và không chứa các ký tự không hợp lệ (chẳng hạn như dấu câu, dấu ngoặc, hoặc ký tự từ bảng chữ cái khác).  
    **Lưu bản mã (Ciphertext) và giá trị khóa** để sử dụng ở bước tiếp theo.



1. Thực hiện **giải mã** bằng cách sử dụng cùng mẫu mã hóa, chọn chế độ **giải mã (decryption mode)** trong khối **Caesar**.  
    Phân tích kết quả đầu ra. Kiểm tra xem văn bản giải mã có hoàn toàn khớp với văn bản gốc từ bước 2 hay không.



1. Thực hiện **phân tích mật mã đơn giản** bằng cách sử dụng các mẫu có sẵn trong **CrypTool 2**.  
    (Mẫu cho tấn công dựa trên **phân tích tần suất** có thể tìm thấy theo đường dẫn: **Templates -> Cryptoanalysis -> Classical -> Caesar Analysis using character frequencies**).  
     
    **Mục tiêu của phân tích mật mã** là khôi phục khóa bí mật dựa trên văn bản mã hóa.  
   * Dữ liệu đầu vào: sử dụng văn bản mã hóa từ bước 2 và thử khôi phục lại văn bản gốc cùng khóa bí mật.
   * Phân tích bằng cách mã hóa các văn bản khác và sử dụng các đặc điểm tần suất để xác định các yếu tố ảnh hưởng đến mức độ thành công của việc phân tích mật mã, bao gồm:
     + **Độ dài văn bản gốc**
     + **Loại bỏ các ký hiệu và chèn đặc biệt không thuộc bảng chữ cái mật mã** (công thức, ký tự đặc biệt, ký hiệu biến, v.v.)
     + **Loại bỏ khoảng trắng giữa các từ**



1. Thực hiện **phân tích mật mã** của **mật mã Caesar** bằng cách sử dụng mẫu **tấn công vét cạn (brute-force attack)**.  
    Đường dẫn đến mẫu này trong **CrypTool 2**:  
    **Templates -> Cryptoanalysis -> Classical -> Caesar Brute Force Analysis**.
2. Tương tự như các bước **1-5**, tiến hành **phân tích các mật mã đơn bảng và đa bảng khác** từ phần thực hành, cũng như thực hiện các cuộc tấn công tương ứng đối với từng thuật toán mật mã.  
    Các mẫu cần thiết trong **CrypTool 2** (đường dẫn: **Templates -> Cryptoanalysis/Cryptography -> Classical**):  
     
    **Cho các mật mã:**
   * **Substitution Cipher (Mật mã thay thế)**
   * **Transposition Cipher (Mật mã hoán vị)**
   * **Vigenère Cipher (Mật mã Vigenère)**

**Cho các phương pháp tấn công:**

* + **Transposition Brute-Force Analysis (Tấn công vét cạn mật mã hoán vị)**
  + **Transposition Crib Analysis (Phân tích mẫu mật mã hoán vị)**
  + **Transposition Genetic Analysis (Phân tích di truyền mật mã hoán vị)**
  + **Transposition Hill Climbing Analysis (Phân tích tối ưu hóa mật mã hoán vị)**
  + **Monoalphabetic Substitution Analyzer (Phân tích thay thế đơn bảng)**
  + **Frequency Analysis (Phân tích tần suất)**
  + **Vigenère Analysis (Phân tích mật mã Vigenère)**

1. **Thực hiện các bước 1-5** đối với trình giả lập **máy mã hóa quay Enigma**.  
    Các mẫu cần thiết trong **CrypTool 2** (đường dẫn: **Templates -> Cryptoanalysis/Cryptography -> Classical**):  
     
    **Cho máy Enigma:**
   * **Enigma Cipher Machine**

**Cho các phương pháp tấn công vào máy Enigma:**

* + **Enigma Gillogly Attack**
  + **Enigma Hillclimbing Attack**
  + **Enigma Simulated Annealing Attack**
  + **Enigma Turing Bombe Attack**

### **3. Phương án thay thế**

Phương án thay thế trong bài thực hành này yêu cầu thực hiện phần mềm mô phỏng các hệ mật mã được nghiên cứu, bao gồm:

* **Các mật mã dịch chuyển, thay thế và hoán vị đơn giản**
* **Mật mã Vigenère**
* **Mô phỏng phần mềm của máy quay Enigma**

Cần phải triển khai tất cả các mật mã được liệt kê trong danh sách. Tuy nhiên, mỗi mật mã có thể được thay thế bằng một mật mã khác thuộc cùng loại, ví dụ:

* **Mật mã thay thế đơn giản có thể thay thế bằng mật mã đơn bảng affine**
* **Máy quay Enigma có thể thay bằng máy quay M209**
* **Mật mã Vigenère đa bảng có thể thay bằng mật mã Bofor đa bảng**

Nói cách khác:

* **Một mật mã đơn bảng có thể thay bằng một mật mã đơn bảng khác**
* **Một mật mã đa bảng có thể thay bằng một mật mã đa bảng khác**
* **Một máy quay có thể thay bằng một máy quay khác**

### **4. Câu hỏi bảo vệ (hỏi-đáp)**

1. **Các lĩnh vực sau đây của mật mã học nghiên cứu những gì:** mật mã học (cryptology), mật mã (cryptography), phân tích mật mã (cryptanalysis)?
2. **Sự khác biệt chính, định nghĩa và ví dụ** cho các hệ thống sau:
   * Hệ mật mã bất đối xứng
   * Hệ mật mã đối xứng
   * Giao thức mật mã
3. **Ví dụ về các loại mật mã tương ứng với từng giai đoạn phát triển của mật mã học:**
   * Mật mã học nguyên thủy
   * Mật mã học hình thức
   * Mật mã học toán học
4. **Các loại mật mã thay thế, hoán vị và dịch chuyển**
5. **Tấn công vét cạn khóa và phân tích tần suất ký tự**
6. **Số học mô-đun. Các ví dụ cơ bản.**
7. **Mật mã Vigenère. Kiểm tra Kazisker.**
8. **Nguyên lý Kerckhoffs.**
9. **Máy quay mật mã:**
   * Mô tả ngắn gọn về nguyên lý hoạt động và cấu trúc bên trong
   * Không gian khóa của máy quay
10. **Độ an toàn của hệ mật mã:**
    * Độ an toàn tính toán và độ an toàn thực tế
11. **Ví dụ về các hệ mật mã thuộc giai đoạn mật mã toán học.**
12. **Phân tích mật mã:**
    * Phân tích mật mã cổ điển
    * Phân tích kênh kề (SCA - Side Channel Attack)