1. Mật mã Caesar là gì?

a) Một hệ mật mã hoán vị

b) Một hệ mật mã thay thế

c) Một hệ mật mã pha trộn

d) Một hệ mật mã Vigenère

2. Hệ mật mã Caesar sử dụng phương pháp gì để mã hóa thông điệp?

a) Hoán vị

b) Pha trộn

c) Thay thế

d) Tất cả các phương pháp trên

3. Trong mật mã Caesar, bao nhiêu lựa chọn khác nhau để dịch chuyển ký tự?

a) 13

b) 25

c) 26

d) 27

4. Mật mã Vigenère sử dụng gì để mã hóa thông điệp?

a) Pha trộn

b) Hoán vị

c) Thay thế

d) Kết hợp cả pha trộn và thay thế

5. Mật mã Vigenère được đặt tên theo cái tên của ai?

a) Julius Caesar

b) Blaise Pascal

c) Leonhard Euler

d) Giovan Battista Bellaso

6. Mật mã Vigenère sử dụng một khóa thay đổi sau mỗi ký tự để làm gì?

a) Đảm bảo tính bảo mật

b) Tạo ra sự khó khăn cho việc giải mã

c) Tạo sự ngẫu nhiên trong thông điệp mã hóa

d) Tăng độ dài của thông điệp mã hóa

7. Trong mật mã Vigenère, để giải mã thông điệp, người giải cần biết gì?

a) Khóa

b) Mật khẩu

c) Số nguyên tố

d) Mật khẩu và khóa

8. Trong mật mã Vigenère, khóa có thể có độ dài bao nhiêu ký tự?

a) Không giới hạn

b) Chỉ có thể là một ký tự

c) Phải bằng độ dài của thông điệp

d) 26 ký tự

9. Mật mã Caesar với khóa k = 3 sẽ mã hóa chữ "HELLO" thành chữ gì?

a) KHOOR

b) HFOOR

c) HEKKE

d) LIPPS

10. Mật mã Vigenère được phát minh vào thời kỳ nào?

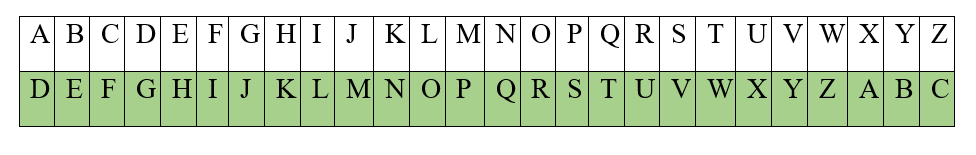
a) Thời kỳ cổ đại

b) Trung đại

c) Thời kỳ Phục hưng

d) Thế kỷ 19

11. Bảng ký tự hoán vị sau đã được tạo ra bằng cách nào?



=> bằng cách dịch chuyển sang trái 3 ký tự (giống cách mã hóa Caesar)

12. Alice và Pop và 2 nhân viên của công ty chuyên lừa đảo người dân mua hàng và có trúng thưởng. Alice muốn gửi cho Pop thông tin gồm “Tên” của những khách hàng đã liên lạc trong ngày. Tuy nhiên, để đảm bảo an toàn cho thông tin, Alice muốn mã hóa các thông tin bằng phương pháp sử dụng Mã thay thế. Alice gửi cho Pop một danh sách đã được mã hóa và một số n là số nguyên tố nhỏ nhất có 1 chữ số (sử dụng cho tạo khóa k bằng cách dịch chuyển n kí tự). Em hãy cho biết danh sách tên khách hàng mà Pop nhận được.

**Input: Output: ?**

|  |  |
| --- | --- |
| n (số nguyên tố nhỏ nhất có 1 chữ số) | 2 |
| Bao | Dcq |
| Hung | Jwpi |
| Jack | Lcem |

13. Alice và Pop và 2 nhân viên của công ty chuyên lừa đảo người dân mua hàng và có trúng thưởng. Alice muốn gửi cho Pop thông tin gồm “Tên”, “SĐT”, “Email” của những khách hàng đã liên lạc trong ngày. Tuy nhiên, để đảm bảo an toàn cho thông tin, Alice muốn mã hóa các thông tin bằng phương pháp sử dụng Mã thay thế đa tự, Alice gửi cho Pop một danh sách đã được mã hóa và một số n là số nguyên tố nhỏ nhất có 1 chữ số (sử dụng cho tạo khóa k bằng cách dịch chuyển n kí tự). Em hãy cho biết danh sách tên khách hàng mà Pop nhận được.

**Input: Output: ?**

|  |  |
| --- | --- |
| Khanh Tram | Mjcpj Vtco |
| 0346847272 | ihkmomnng |
| [tram.nguyenthikhanh@phenikaa-uni.edu.vn](mailto:tram.nguyenthikhanh@phenikaa-uni.edu.vn) | vtco. piwagpvjkmjcpj@rjgpkmcc-wpk.gfw.xp |

14. Sử dụng mã Vigenere, mã hóa bản rõ sau “*encryption*” với khóa K=CIPHER

=> gvrycgvqdu

15. Cho văn bản gốc P=<NguyenVanA>. Giải thích các bước thực hiện mã hóa P và giải mã sử dụng các thuật toán sau:

a. Mã hóa cộng với khóa K=18 (Z26)

b. Mã hóa Affine với khóa K1=7, K2=11 trên Z26

c. Mã hóa Vigenere với K=attack

=>

a. Mã hóa cộng với khóa K=18 (Z26)

\* mã hóa

- chuyển đổi các kí tự trong văn bản thành các số tương ứng trong Z26

- thực hiện phép toán : Y = (X + K) mod 26. Trong đó Y, X lần lượt là vị trí của kí tự đã mã hóa và kí tự cần mã hóa trong bảng chữ cái, K là khóa.

- chuyển đổi các số đã được mã hóa thành chữ cái tương ứng

=> ở đây “NguyenVanA” được mã hóa thành “FymqwfNsfS”

\*giải mã

- chuyển đổi các kí tự thành số tương ứng

- thực hiện phép toán: Y = (X – K) mod 26

- chuyển các số đã được mã hóa thành chữ cái tương ứng.

=> với bản mã ở câu a khi giải mã sẽ ra bản rõ là “NguyenVanA”

b. Mã hóa Affine với khóa K1=7, K2=11 trên Z26

\* Mã hóa:

Đầu tiên, chuyển đổi văn bản gốc P thành các ký tự trong bảng chữ cái tiếng Anh viết thường và loại bỏ các ký tự không phải là chữ cái.

Bước 1: Chuyển đổi mỗi ký tự thành một số nguyên tương ứng trong khoảng từ 0 đến 25. Ví dụ, "N" được chuyển đổi thành 13 và "g" được chuyển đổi thành 6.

Bước 2: Áp dụng phép biến đổi Affine cho mỗi số nguyên:

Mã hóa: C = (K1 \* P + K2) mod 26

Trong trường hợp này, K1=7 và K2=11.

Bước 3: Chuyển đổi số nguyên đã mã hóa trở lại thành ký tự trong bảng chữ cái tiếng Anh viết thường. Kết quả sau khi mã hóa từng ký tự là:

"N" -> "C" (13 -> 2)

"g" -> "x" (6 -> 23)

Kết quả của quá trình mã hóa là chuỗi "CxtrtKtpX".

\* Giải mã Affine:

- Chuyển đổi chuỗi đã mã hóa thành các ký tự trong bảng chữ cái tiếng Anh viết thường.

- Giải mã từng ký tự trong chuỗi đã mã hóa bằng cách sử dụng công thức giải mã Affine ngược:

Giải mã: P = (K1\_inv \* (C - K2)) mod 26

Trong đó, K1\_inv là modular multiplicative inverse của K1 (7) trong hệ thống Z26. Để tính K1\_inv, chúng ta sử dụng định lý Euclid mở rộng hoặc bảng lookup cho modular multiplicative inverses. Trong trường hợp này, K1\_inv ≡ 15 (mod 26), vì 7 và 15 có tích mod 26 bằng 1.

Áp dụng công thức giải mã và chuyển đổi số nguyên đã giải mã trở lại thành ký tự trong bảng chữ cái tiếng Anh viết thường. Kết quả sau khi giải mã từng ký tự là:

"C" -> "N" (2 -> 13)

"x" -> "g" (23 -> 6)

Kết quả của quá trình giải mã là văn bản gốc "NguyenVanA".

c. Mã hóa Vigenere với K=attack

\*mã hóa vigenere

- Chuyển đổi văn bản gốc P thành các ký tự trong bảng chữ cái tiếng Anh viết thường và loại bỏ các ký tự không phải là chữ cái.

Bước 1: Chuyển đổi mỗi ký tự trong khóa "attack" và từng ký tự của chuỗi thành các số nguyên tương ứng trong khoảng từ 0 đến 25. Ví dụ, "a" chuyển thành 0, "t" chuyển thành 19, "a" lại chuyển thành 0, "c" chuyển thành 2, "k" chuyển thành 10.

Bước 2: Áp dụng phép mã hóa Vigenère cho mỗi ký tự trong chuỗi đã chuyển đổi:

Mã hóa: C = (P + K) mod 26

Trong đó, C là ký tự đã mã hóa, P là ký tự gốc, và K là ký tự từ khóa tương ứng.

Bước 3: Chuyển đổi số nguyên đã mã hóa trở lại thành ký tự trong bảng chữ cái tiếng Anh viết thường.

Kết quả của quá trình mã hóa là chuỗi "NflgecVgrA".

\*Giải mã Vigenère:

- Chuyển đổi chuỗi đã mã hóa thành các ký tự trong bảng chữ cái tiếng Anh viết thường.

Bước 1: Chuyển đổi mỗi ký tự trong khóa "attack" và từng ký tự của chuỗi đã mã hóa thành các số nguyên tương ứng trong khoảng từ 0 đến 25.

Bước 2: Áp dụng phép giải mã Vigenère ngược cho mỗi ký tự trong chuỗi đã mã hóa:

Giải mã: P = (C - K) mod 26

Trong đó, P là ký tự gốc, C là ký tự đã mã hóa, và K là ký tự từ khóa tương ứng.

Bước 3: Chuyển đổi số nguyên đã giải mã trở lại thành ký tự trong bảng chữ cái tiếng Anh viết thường.

Kết quả của quá trình giải mã là văn bản gốc "NguyenVanA".