BÀI THỰC HÀNH SỐ 1

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: HUỲNH PHẠM PHƯỚC LINH**

**MSSV: 1710165**

**Nhóm: L06**

**Phần 1. Các hệ mã đối xứng truyền thống**

**Câu 1:**

FISHINGFRESHWATERBENDSADMITSWORDFISHRANDOVERHELMINGANYDAY

Key = 5

|  |  |  |
| --- | --- | --- |
| Bảng tần suất | | |
| Kí tự | Tần suất (Table 1) [%] | Tần suất (Plaintext) [%] |
| a | 8.05 | 8.77 |
| b | 1.62 | 1.75 |
| e | 12.31 | 8.77 |
| i | 7.18 | 8.77 |
| r | 6.03 | 8.77 |
| v | 0.93 | 1.75 |
| w | 2.03 | 3.50 |
| z | 0.09 | 0.00 |

🡪 Có thể dò ra được nội dung của thông điệp

Mật mã Caesar rất dễ bị phá, ngay cả trong trường hợp người giải mã chỉ có trong tay các bản mật mã. Có hai tình huống được xem xét:

1. Người giải mã biết (hoặc đoán) rằng một số dạng mật mã thay thế đơn giản đã được sử dụng, nhưng không biết cụ thể đó là mật mã Caesar;
2. Người giải mã biết chính xác mật mã Caesar được sử dụng, nhưng không biết giá trị khóa mã.

**Câu 2:**

|  |
| --- |
| C = (M+K) mod 26 🡪 M = (C-K) mod 26 |

Áp dụng công thức trên, dùng vòng lặp for ta sẽ giải mã được thông điệp và tìm được khóa K

|  |  |
| --- | --- |
| KEY = 4 | PLAINTEXT = WORLDCUP |

**Câu 3:**

|  |
| --- |
| C = (ap+b) mod 26 🡪 P = (a-1 \* (C - b)) % 26 |

Chữ cái xuất hiện nhiều nhất là B, tương ứng với bảng tần suất ở phía trên là E

Tương tự U 🡪 T

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | ư | x | y | z |
| ­ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|  |  |  |  |  | b |  |  |  |  |  |  |  |  |  |  |  |  |  |  | u |  |  |  |  |  |  |
|  |  |  |  |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 20 |  |  |  |  |  |  |

E (p=4) tương ứng với B (c=1)

T (p=19) tương ứng với U (c=20)

Ta có hệ phương trình:

**Câu 4:**

Vấn đề của One-time pad:

1. Vấn đề chia sẻ key: One-time pad có thể được coi là gần như không thể giải mã, tuy nhiên chỉ khi việc trao đổi key giữa người nhận và người gửi được hoàn toàn bảo đảm.
2. Vấn đề tạo key ngẫu nhiên: Việc tạo ra một key một cách hoàn toàn ngẫu nhiên là một điều tương đối khó ở phần lớn các ngôn ngữ lập trình hiện tại.

**Câu 5:**

Plaintext: Must see you over Cadogan West. Coming at once.

Length: 37

Length % 2 = 1 --> thêm X vào cuối plaintext

|  |
| --- |
| 🡪 MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX |

Key:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | F | H | I/J | K |
| U | N | O | P | Q |
| Z | V | W | X | Y |
| E | L | A | R | G |
| D | S | T | B | C |

['M', 'U'] --> ['U', 'Z']

['S', 'T'] --> ['T', 'B']

['S', 'E'] --> ['D', 'L']

['E', 'Y'] --> ['G', 'Z']

['O', 'U'] --> ['P', 'N']

['O', 'V'] --> ['N', 'W']

['E', 'R'] --> ['L', 'G']

['C', 'A'] --> ['T', 'G']

['D', 'O'] --> ['T', 'U']

['G', 'A'] --> ['E', 'R']

['N', 'W'] --> ['O', 'V']

['E', 'S'] --> ['L', 'D']

['T', 'C'] --> ['B', 'D']

['O', 'M'] --> ['U', 'H']

['I', 'N'] --> ['F', 'P']

['G', 'A'] --> ['E', 'R']

['T', 'O'] --> ['H', 'W']

['N', 'C'] --> ['Q', 'S']

['E', 'X'] --> ['R', 'Z']

Kết quả:

|  |
| --- |
| UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ |

**Câu 6:**

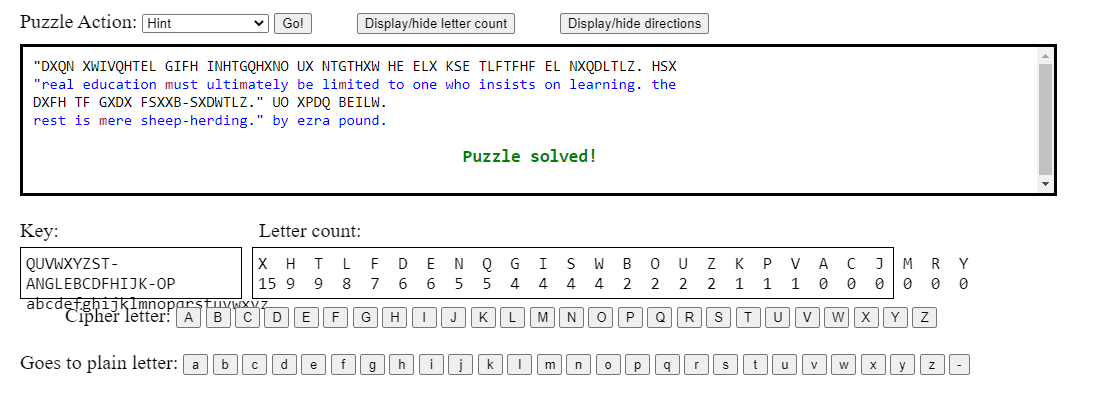
Key1 = Phuoc

Key2 = Linh

Plaintext = spyarrivesonthursday

Cipher text = ysardsiervrpasyunhot

**Câu 7:**



Cách làm

- Dựa vào Letter count, xác định được tần suất xuất hiện của các kí tự

- Dựa vào bảng tần suất của câu 1, ta thử lần lượt thế các kí tự với nhau

- VD: X xuất hiện 15 lần 🡪 khả năng cao đây là chữ E

- Sau khi thay thế từng ký tự, ta nhận được plaintext

**Phần 2. Chuẩn mã hoá dữ liệu DES**

**Câu 1:**

Sự khác biệt chính giữa Mật mã khối và Mật mã dòng:

* Kỹ thuật mã hóa khối liên quan đến mã hóa một khối văn bản tại một thời điểm, tức là đơn lẻ. Tương tự, giải mã văn bản bằng cách lấy hết khối này đến khối khác. Ngược lại, kỹ thuật mã hóa Stream liên quan đến mã hóa và giải mã một byte văn bản tại một thời điểm.
* Mật mã khối sử dụng cả nhầm lẫn và khuếch tán trong khi mật mã luồng chỉ dựa vào nhầm lẫn.
* Kích thước thông thường của khối có thể là 64 hoặc 128 bit trong mật mã khối. Ngược lại, 1 byte (8 bit) tại một thời điểm được chuyển đổi trong mật mã luồng.
* Mật mã khối sử dụng các chế độ thuật toán ECB (Sách mã điện tử) và CBC (Mã hóa chuỗi khối). Ngược lại, mật mã Stream sử dụng các chế độ thuật toán CFB (Phản hồi mật mã) và OFB (Phản hồi đầu ra) .
* Mật mã luồng sử dụng chức năng XOR để chuyển đổi văn bản thuần thành văn bản mã hóa, đó là lý do tại sao nó dễ dàng đảo ngược các bit XORed. Trong khi đó, mật mã khối không sử dụng XOR để làm như vậy.
* Mật mã khối sử dụng cùng một khóa để mã hóa từng khối trong khi mật mã luồng sử dụng một khóa khác nhau cho mỗi byte.

**Câu 2:**

a.

K1 [HEX] = 02 02 67 8B 00 A5

K1 [BIN] = 000000100000001001100111100010110000000010100101

b.

L0 = 11001100000000001100110011111111

R0 = 11110000101010101111000010101010

c.

E[R0] = 011110100001010101010101011110100001010101010101

d.

A = 011110000001011100110010111100010001010111110000

e.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| STT | 6 BIT E[R0] | Row | Col | Row&Col | Index | S - Box | HEX | BIN |
| 1 | 011110 | 00 | 1111 | 001111 | 15 | 0 | 0 | 0000 |
| 2 | 000001 | 01 | 0000 | 010000 | 16 | 10 | A | 1010 |
| 3 | 011100 | 00 | 1110 | 001110 | 14 | 4 | 4 | 0100 |
| 4 | 110010 | 10 | 1001 | 101001 | 41 | 15 | F | 1111 |
| 5 | 111100 | 10 | 1110 | 101110 | 46 | 3 | 3 | 0011 |
| 6 | 010001 | 01 | 1000 | 011000 | 24 | 5 | 5 | 0101 |
| 7 | 010111 | 01 | 1011 | 011011 | 27 | 5 | 5 | 0101 |
| 8 | 110000 | 10 | 1000 | 101000 | 40 | 2 | 2 | 0010 |

f.

B = 00001010010011110011010101010010

g.

P[B] = 11100010010110110011000011001000

h.

R1 = 00101110010110111111110000110111

i.

L1 = R0 = 11110000101010101111000010101010