Nhập môn An toàn thông tin - Assignment 1

Họ và tên: Lê Hữu Đức Anh

Mssv: 20215304

1. **Nguồn tham khảo:**

**Lý thuyết:**

<https://www.coursera.org/learn/crypto>

<https://crypto.stackexchange.com/questions/33673/many-time-pad-attack-xor>

**Mã nguồn tham khảo:**

<https://github.com/ashumeow/cryptography-I/blob/master/week-1/assignments/_ExtraCredit/solution.md>

<http://www.chiange.com/hello-world/>

1. **Giải thích quá trình**

Nhận thấy cipher1 **xor** cipher2 = message1 **xor** message2 nên việc kết hợp các cặp ciphertext giúp ta không cần biết về key.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

*Phương pháp tính toán*

Để ý thêm thì việc XOR 1 ký tự chữ với khoảng trắng( space) cho ra kết quả là ký tự chữ, dễ dàng cho việc suy đoán còn các cặp XOR khác thì khó đoán hơn.

A screen shot of a computer code

Description automatically generated

Thực hiện nhân từng cặp ciphertext. Bắt đầu từ ciphertext1 với 10 ciphertext còn lại, với kết quả thu được là ký tự chữ thì tăng biến possible\_space của kí tự thứ k lên 1 đơn vị.

A computer screen shot of a code

Description automatically generated

Với possible\_space ở vị trí k có giá trị đủ lớn, lớn hơn số lượng ciphertext trừ đi 3 = 7, tương đương với số lần xuất hiện ký tự chữ ở vị trí k. Khi đó ta tính toán giá trị key[k] = a[s] XOR 0x20(space).

A screen shot of a computer

Description automatically generated

Kết quả thu được của key(dự đoán):

*66396e89c9dbd8cb9874352acd6395102eafce78aa7fed28a0006bc98d29c50b69b0339a19f8aa401a9c6d708f80c066c763fef0123148cdd8e802d05ba98777335daefcecd59c433a6b268b60bf4ef03c9a611000bb009a3161edc70004a3*

A black screen with white text

Description automatically generated

Kết quả thu được của bản rõ là kết quả phép XOR key và target ciphertext:

The secuet message is: Whn using a stream cipher, never use the key more than once

Tạm dịch:

The secret message is: When using a stream cipher, never use the key more than once

A screenshot of a computer

Description automatically generated