Bài tập assignment 2

Họ và tên: Phạm Văn Nam

MSSV: 20183599

Ta có khi XOR các bản mã với nhau, kết quả thu được cũng chính là kết quả khi XOR các bản rõ tương ứng với nhau.

Khi XOR 1 kí tự trong bảng chữ cái (a-z, A-Z) với kí tự space thì kết quả thu được cũng là một kí tự trong bảng chữ cái (a-z, A-Z).

Các bản rõ là các đoạn văn bản bao gồm kí tự chữ cái, kí tự space, và các kí tự dấu câu. Vậy nếu mang XOR 2 bản rõ bất kì, đoạn text thu được sẽ có những vị trí xuất hiện kí tự trong bảng chữ cái, điều này có nghĩa rằng tại vị trí tương ứng của 1 trong 2 bản rõ đem XOR là kí tự space.

Chúng ta có 11 bản mã (bao gồm cả thông điệp cần giải mã), ta sẽ đem XOR 1 bản mã Yi với 10 bản mã còn lại. Xét tại cùng 1 vị trí của 10 kết quả từ phép XOR, nếu vị trí này có nhiều kết quả là kí trong bảng chữ cái thì rất có khả năng vị trí này trong bản rõ Xi là kí tự Space. Cụ thể trong code của em, nếu tại một vị trí mà có ít nhất 6/10 kết quả đều là kí tự trong bảng chữ cái thì em sẽ cho kí tự tại vị trí đó trong bản rõ là Space.

Biết được kí tự trong bản rõ là kí tự Space, ta dễ dàng tìm được khóa tại vị trí đó:

Key[j] = 0x20 XOR Yi[j]

Kết quả:

**The secuet message is: Whtn using aa~tream cipher, never use the key more than once**

Ta có thể dễ dàng đoán được thông điệp ban đầu là:

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