**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

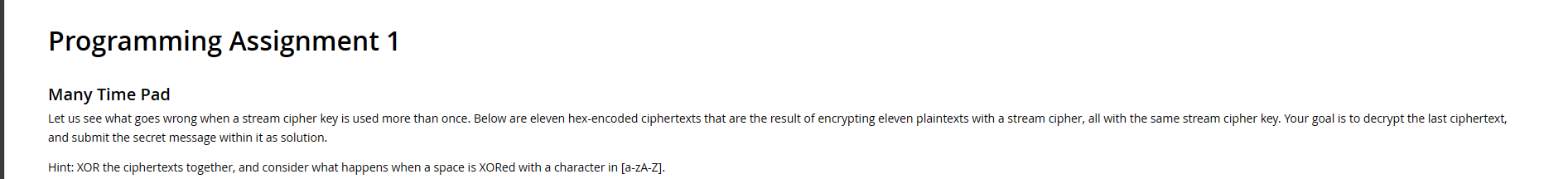
**BÁO CÁO BÀI 1 – IT4015  
Đề tài: MANY TIME PAD ATTACK**

**NGUYỄN TRUNG HIẾU - 20215578**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn:** | Thầy Trần Vĩnh Đức  Chữ ký của GVHD |
| **Mã học phần:** | 149480 |
| **Bộ Môn:**  **Trường/Viện:** | Nhập môn An Toàn Thông Tin  Trường CNTT & TT. |
| **HÀ NỘI, 3/2024** | |

# I. Đề bài

## 



1. Mục tiêu: Giải mã văn bản được mã hóa cuối cùng và gửi thông điệp bí mật bên trong.

2. Phương pháp:

* Sử dụng phép toán XOR để kết hợp các văn bản được mã hóa với nhau.
* Quan sát kết quả XOR của một khoảng trắng và một ký tự trong phạm vi [a-zA-Z].

3. Gợi ý:

* Việc tái sử dụng khóa mã luồng có thể dẫn đến việc lộ thông tin bí mật.
* Phép toán XOR có tính chất giao hoán và kết hợp.
* Khi XOR một khoảng trắng với một ký tự trong phạm vi [a-zA-Z], kết quả sẽ là một ký tự khác trong cùng phạm vi.

4. Yêu cầu:

* Gửi thông điệp bí mật được giải mã dưới dạng câu trả lời.

# II. Phương pháp giải:

1. Hướng giải ban đầu:

Từ gợi ý và các mã ciphertext của đề bài, ta có thể đưa ra các lập luận như sau:

A group of black text

Description automatically generated

* Kĩ thuật One time pad sử dụng 1 key xor các tinh nhắn, tạo ra các ciphertext tương ứng, khi key này chỉ sử dụng 1 lần thì ta không thể nào giải mã ra được tin nhắn gốc là gì. Tuy nhiên, khi cái key này được sử dụng nhiều lần, ta có thể có được nhiều đoạn ciphertext, từ đó xor 2 đoạn ciphertext sẽ ra được 1 đoạn mã mới, bằng xor của 2 tin nhắn gốc ban đầu:

A group of black text

Description automatically generated

* Khi có cảng nhiều đoạn ciphertext, ta sẽ có càng nhiều thông tin về key, và ta có thể đoán 1 đoạn message ban đầu, và từ đó, ta sẽ suy ngược ra được key:

A black text with a white background

Description automatically generated

* Ở các đoạn ciphertext 3,4,6, 7 và đoạn mã target, ta có thể thấy chúng đều được bắt đầu bằng cụm: 0x32510b:

A screenshot of a computer

Description automatically generated

A close up of a text

Description automatically generated

* Cụm này gồm 6 kí tự hexa, tương đương với 3 chữ trong bộ mã Ascii. Từ 3 chữ được lặp lại nhiều nhất ở trong tiếng anh chính là từ “The”, nên ta có thể đoán các kí tự này là chữ “the” được mã hóa bằng OTP.
* Khi ta xor chữ “the” trong hệ mã ascii, tức 0x746865 với 0x32510b, ta sẽ được 1 key ban đầu là 0x46396e:





2. Các bước giải:

* Bước 1: Xor key có được với tất cả các ciphertext, chuyển kết quả về dạng text ascii
* Bước 2: Đoán các thông sau khi xor, và xor ngược lại đoạn ciphertext với thông điêp vừa đoán được sẽ ra 1 key mới.
* Bước 3: Kiểm tra key mới, nếu key mới cho ra các đoạn mã có nghĩa, tức là key đã đúng, đến bước 4, không thì lặp lại bước 2
* Bước 4: Thay key mới cho key cũ và lặp lại bước 1 cho đến khi có được đoạn key hoàn chỉnh:

3. Ví dụ:

* Bước 1: Giả sử ban đầu ta có key là 0x46396e từ bước ở trên, khi ta xor key này với các đoạn ciphertext từ 1-10, ta sẽ được dãy sau:

A black background with white text

Description automatically generated

Đây đều là các đoạn mã có nghĩa, nên có vẻ ta đã đi đúng hướng.

* Bước 2: Ở message #2, ta có thể đoán được chữ được hoàn thiện sẽ là chữ “euler “, ta có thể xor “euler “ dưới dạng ascii là 0x65756c657220 cho ciphertext #2, ta sẽ có được key mới:

A black background with white text

Description automatically generated



Key mới sẽ là 0x46396e89c9db.

* Bước 3: Ta xor key mới với tất cả các đoạn mã ciphertext trong đề bài:

A screenshot of a computer screen

Description automatically generated

Kết quả trả được đều là các đoạn mã có nghĩa, nên ta đã đi đúng hướng.

* Bước 4, ta thay key cũ là 0x46396e bằng key mới 0x46396e89c9db, rồi lặp lại các bước ở trên, cho đến khi ta tìm được mật mã cần giải.

4. Đáp án:

* Key :46396e89c9dbd8cc9874352acd6395102eafce78aa7fed28a07f6bc98d29c50b69b0339a19f8aa401a9c6d708f80c066c763fef0123148cdd8e802d05ba98777335daefcecd59c433a6b268b60bf4ef03c9a611098bb3e9a3161edc7b804a33522cfd202d2c68c57376edba8c2ca50027c61246ce2a12b0c4502175010c0a1ba4625786d911100797d8a47e98b0204c4ef06c867a950f11ac989dea88fd1dbf16748749ed4c6f45b384c9091d41f7d90937b8d.
* Thông điệp ẩn: “the secret message is: When using a stream cipher, never use the key more than once”

A black screen with many small letters

Description automatically generated with medium confidence

III. Source code và các tài liệu tham khảo:

* Many time pad attack (XOR) [duplicate]: <https://crypto.stackexchange.com/questions/33673/many-time-pad-attack-xor>
* Link GitHub chứa source code:

https://github.com/HieuNT-2306/SecurityAssignment