BÀI TẬP THỰC HÀNH SỐ 1

MÔN: MẬT MÃ HỌC

1 Mục tiêu

- Thực hiện phá mã Many Time Pad thành công dưới sự hỗ trợ của máy tính.

2 Mô tả

Chúng ta sẽ xem xét điều gì xảy ra với mã dòng khi khóa được sử dụng lại nhiều lần. Giả sử chúng ta có 2 bản mã $c_1 = m_1 \oplus k$ và $c_2 = m_2 \oplus k$ được mã hóa với cùng một khóa k. Khi có 2 bản mã, người tấn công có thể tính được $c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$.

Trong bản mã ASCII, khi một ký tự alphabet (a-z hoặc A-Z) XOR với một khoảng trắng thì sẽ bị chuyển thành chữ hoa (nếu hiện tại là chữ thường) hoặc bị chuyển thành chữ thường (nếu hiện tại là chữ hoa). Như vậy, chỉ cần xét các ký tự alphabet trong $c_1 \oplus c_2$ là có thể khẳng định tồn tại một khoảng trắng thuộc m_1 hoặc m_2 với xác suất rất cao.

Để trả lời khoảng trắng là của m_1 hay m_2 thì phải dựa vào các bản mã c_i còn lại. Khi ta tính $c_1 \oplus c_i$ và thu được vị trí có khoảng trắng trùng với lại vị trí khoảng trắng trong $c_1 \oplus c_2$ thì có khả năng cao khoảng trắng tại vị trí đó là của m_1.

Khi xác định được hầu hết các khoảng trắng trên các bản rõ m_i thì ta có thể suy ra những ký tự của khóa tương ứng tại các vị trí đó. Nếu vị trí các khoảng trắng là so le với nhau thì việc tìm lại khóa sẽ dễ dàng hơn. Nếu không, ta cần suy đoán để tìm ra các bản rõ m_i có nghĩa, rồi mới tìm ra khóa k.

3 Yêu cầu

Cho 10 bản mã được mã hóa bằng phép XOR với cùng một khóa.

Ciphertext #1

```
470becf05721cc5c1f430c1ce5bbef7e163992086f1ab56400fd15a93e0
e0943e094ca3438de4072ab794127168c225bb86da25421ac543fda2112
cf354a93d18b1f492b634b9af0aad66b7cdd73d751678e48388c3896106
014860d1691c3e479494c7d58d4713af328262a4291991f69dd8243f0ec
72d4bef8487d7b4c12c20d3ec038c92b807f
```

Ciphertext #2

```
431ea9e45132c95b5e5c011ce9efe46d1b698f132801a7341cec50fe2c1
e4045e18ec03723d30565ff7b4c2a5ec33013a928a25321b65138ca3146
c0355693cd885c5f307a4d98a2bd9f247bc6659b126f8c42329a75920a6
a099151428cdeeb37494e7649d07b27a92460245ed5c9096fd89f55f0e0
6080a8f90b6c715542d41632d924c82c9030746a2105622a2f0a712a339
f580ef1990cb05270d77f2dcc6ed1e2465ccc0e6724ffb52dc52b88d5b6
bf62a6c3404ce3acdeb0847c5afcba8d623f66ae
```

Ciphertext #3

```
5900ecf3503180484d591b04b1aaaa740760db0f2a07b22d1af25ca9391
a0f06fe81d12638d81321ac64442c53c33714a16de14f2aa6572fcb725b
c73c57c1cf8f08553664059eb1a2d3697189739b1a6b9902779f3b93447
c088d01428dd8f6375148670cca7631ee247223498c990c69dd9e11ede1
27c3b4f1056b7a4801d60d3a9422c3268134746f374b35213e16262a379
2105ae98244a5412c
```

Ciphertext #4

```
5100ecee5524cc515c591945a4bcf46a0f698f15201de62d1ab511e7344
d135ffd94c63f71c81368b16b052e448a321ab86dec572abc052fd13140
d02a4cdacd805c552a2a5195b1ba9f787dcc32d81e638d5b39973696106
0158f014684c3f17e5f5e3e44dc6831a077692649d5ce1a798e9957b9e7
69c9aff50972785842c4113ec638c822d33020682b126221245e676f259
41b08e3820cad526ccd733a91
```

Ciphertext #5

```
4406a9a75b3dd0505a424d08a0bbef70063996093c07e62a1be150eb284
d1243ff95ca2034d94075b02c473b16902118be6db5106fa44b2e9f3b46
89374dc0d6ce1e59796b4791b5eecb6335cf73d71d2e8940239175830c6
c5b80405881c2a5785c0d6a44d83e31ee616b320c82d00f68c18345b9e7
69c3b4f21e7b7a4807d91a3a9a
```

Ciphertext #6

```
514ebfe25b21d25d1f550306b7b6f76b0b76955c3c10ae2119f050e4381
e1406e681d53771dc406aba75052d4682271eec7ca95d3be54c399f3c5d
dd7a4ec6ce80194e38684998f0bad02c70d17ada047d9447219b7584016
8098b4918
```

Ciphertext #7

```
4406a9a7503dd34c50421445aaa9a77c0e78880f2610a72854f01eea3f1
41052e78fcd7222de0864b269567e5f90641dad7ba25521a45123d1351e
893857c7cace0b552d62058fb5bdcf6976dd32cf1e2e944632de3892106
1148c521690c2e0731a4c6d0cca7b38ec2467380c81d11e20c79857f5fb
62ceb8f94871720101c5002fc03ec1379221687a6e0a2c2c6a1d7436268
51914e79a55b35a718379269f39cdf84b4a85086977f8b532d925
```

Ciphertext #8

```
5100ece25637d2414f44040aabeff47c0a7c96196f1ab56407f013fc3f0
8404fe8c0cd3d71dc0477ba7e563f449a6418ad66e15a26ab416acb3a57
89295dd0d08b081c326f5cdda7a6da6235ce7bcd1460c04f779d3c870c6
c099c444e919fa5444f4e760cdc3e30e5626f254581d0146e8e9957b9eb
69c3a9e5186a7d4e0c971a30d921ca2087346c7a6e062b3b391b756f229
91d5af69945ae472c
```

Ciphertext #9

```
5500aff54124d451505e4d16a6a7e2720739920f6f17a3221dfb15ed6d0
f1906fa88d137349d016db8635737428b2908ec4fa45263e56024dc7e12
c8345c93e68b1f10796b56dda7abd36035c8619b102e935e329d3c910d6
a1a9c48598b91ea711a4c3e41d86d27e163636b5f85d8186580
```

Ciphertext #10

```
3029a9e9183dd3185e101d17aaade67d0b75920f3b1aa56415f917e63f0
4144ee3c0d73a30c9406eaa78552b4290641aec63a4456fae0529d73d41
cc3418d2c18d134e3d634b9af0bad02c66c67fde516a895d238c3c95117
d12874f1691d9e4631a446d0cd97b20e5766b224290dd5b62d7d645f1eb
27d3b8f40d73710f
```

Bản mã sau đây được mã hóa sử dụng cùng một khóa với 10 bản mã trên. Hãy giải mã bản mã này.

```
514eafee483cc54a1f5d1816b1efe57a4269891d2c07af2715f91cf0614
d0940ae8ecc2671d00175b769483f428a271aa064b8106fac4b2eda315b
d9325dc1c38c105977
```