BÁO CÁO BÀI TẬP 1
TẤN CÔNG MANY TIME PAD

Đàm Ngọc Khánh - 20205207

Ngày 9 tháng 4 năm 2023

1 Đề bài

Ta cùng xem xét về tính không an toàn trong hệ mã dòng khi dùng cùng một khóa để mã hóa nhiều lần. Dưới đây là 11 bản mã ở dạng hexa đã được mã hóa sử dụng cùng một hệ mã dòng và sử dụng cùng một khóa để mã hóa. Mục đích của bạn là giải mã bản mã cuối cùng để tìm ra bản rõ

Yêu cầu: Bạn phải nộp cả mã nguồn cũng như báo cáo chi tiết mô tả cách giải mã.

Bản mã #1

315c4eeaa8b5f8aaf9174145bf43e1784b8fa00dc71d885a804e5ee9fa40b16349c146fb778cdf2d3aff021dff
f5b403b510d0d0455468aeb98622b137dae857553ccd8883a7bc37520e06e515d22c954eba5025b8cc57ee59418
ce7dc6bc41556bdb36bbca3e8774301fbcaa3b83b220809560987815f65286764703de0f3d524400a19b159610b
11ef3e

Bản mã #2

234c02ecbbfbafa3ed18510abd11fa724fcda2018a1a8342cf064bbde548b12b07df44ba7191d9606ef4081ffd
e5ad46a5069d9f7f543bedb9c861bf29c7e205132eda9382b0bc2c5c4b45f919cf3a9f1cb74151f6d551f4480c8
2b2cb24cc5b028aa76eb7b4ab24171ab3cdadb8356f

Bản mã #3

32510ba9a7b2bba9b8005d43a304b5714cc0bb0c8a34884dd91304b8ad40b62b07df44ba6e9d8a2368e51d04e0
e7b207b70b9b8261112bacb6c866a232dfe257527dc29398f5f3251a0d47e503c66e935de81230b59b7afb5f41a
fa8d661cb

Bản mã #4:

32510ba9aab2a8a4fd06414fb517b5605cc0aa0dc91a8908c2064ba8ad5ea06a029056f47a8ad3306ef5021eaf
e1ac01a81197847a5c68a1b78769a37bc8f4575432c198ccb4ef63590256e305cd3a9544ee4160ead45aef52048
9e7da7d835402bca670bda8eb775200b8dabbba246b130f040d8ec6447e2c767f3d30ed81ea2e4c1404e1315a10
10e7229be6636aaa

Bản mã #5:

3f561ba9adb4b6ebec54424ba317b564418fac0dd35f8c08d31a1fe9e24fe56808c213f17c81d9607cee021daf
e1e001b21ade877a5e68bea88d61b93ac5ee0d562e8e9582f5ef375f0a4ae20ed86e935de81230b59b73fb4302c
d95d770c65b40aaa065f2a5e33a5a0bb5dcaba43722130f042f8ec85b7c2070

Bản mã #6:

32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd2061bbde24eb76a19d84aba34d8de287be84d07e7
e9a30ee714979c7e1123a8bd9822a33ecaf512472e8e8f8db3f9635c1949e640c621854eba0d79eccf52ff11128
4b4cc61d11902aebc66f2b2e436434eacc0aba938220b084800c2ca4e693522643573b2c4ce35050b0cf774201f
0fe52ac9f26d71b6cf61a711cc229f77ace7aa88a2f19983122b11be87a59c355d25f8e4

Bản mã #7:

32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd90f1fa6ea5ba47b01c909ba7696cf606ef40c04af
e1ac0aa8148dd066592ded9f8774b529c7ea125d298e8883f5e9305f4b44f915cb2bd05af51373fd9b4af511039

fa2d96f83414aaaf261bda2e97b170fb5cce2a53e675c154c0d9681596934777e2275b381ce2e40582afe67650b
13e72287ff2270abcf73bb028932836fbdecfecee0a3b894473c1bbeb6b4913a536ce4f9b13f1efff71ea313c86
61dd9a4ce
Bản mã #8:
315c4eeaa8b5f8bffd11155ea506b56041c6a00c8a08854dd21a4bbde54ce56801d943ba708b8a3574f40c00ff
f9e00fa1439fd0654327a3bfc860b92f89ee04132ecb9298f5fd2d5e4b45e40ecc3b9d59e9417df7c95bba410e9
aa2ca24c5474da2f276baa3ac325918b2daada43d6712150441c2e04f6565517f317da9d3
Bản mã #9:
271946f9bbb2aeadec111841a81abc300ecaa01bd8069d5cc91005e9fe4aad6e04d513e96d99de2569bc5e50ee
eca709b50a8a987f4264edb6896fb537d0a716132ddc938fb0f836480e06ed0fcd6e9759f40462f9cf57f456418
6a2c1778f1543efa270bda5e933421cbe88a4a52222190f471e9bd15f652b653b7071aec59a2705081ffe72651d
08f822c9ed6d76e48b63ab15d0208573a7eef027
Bản mã #10:
466d06ece998b7a2fb1d464fed2ced7641ddaa3cc31c9941cf110abbf409ed39598005b3399ccfafb61d0315fc
a0a314be138a9f32503bedac8067f03adbf3575c3b8edc9ba7f537530541ab0f9f3cd04ff50d66f1d559ba520e8
9a2cb2a83
Hãy giải mã bản mã sau:
32510ba9babebbbefd001547a810e67149caee11d945cd7fc81a05e9f85aac650e9052ba6a8cd8257bf14d13e6
f0a803b54fde9e77472dbff89d71b57bddef121336cb85ccb8f3315f4b52e301d16e9f52f904

2 Cách giải

Để có được bản mã :
message1$\oplus key = cipher1$
$message2 \oplus key = cipher2$
.....
$message10 \oplus key = cipher10$

Từ đây, ta có thể xor 2 bản mã với nhau để có thể triệt tiêu key để có được kết quả xor 2 bản rõ với nhau

$$cipher1 \oplus cipher2 = message1 \oplus key \oplus message2 \oplus key = message1 \oplus message2$$

Khi xor 1 kí tự là chữ cái từ a-z hoặc từ A-Z với kí tự space thì chữ thường sẽ thành chữ hoa và chữ hoa sẽ thành chữ thường. Từ đây nếu bản rõ cần giải khi xor với 10 mã tại vị trí chỉ số của kí tự nào đó mà ra chữ cái thì có khả năng kí tự đó là chữ cái hoặc là ks tự space.
Ta có thể dự đoán như sau : ta xét 10 kí tự cùng chỉ số khi xor 10 bản rõ của 10 mã với bản rõ cần tìm nếu là chữ cái thì thêm vào 1 list tạm thời. Nếu là chữ cái thì ta thêm vào list tạm thời. Nếu chỉ có 1 chữ cái trong list thì khả năng chữ cái đó sẽ là kí tự tại vị trí đó. Nếu có nhiều hơn 1 chữ cái trong list thì khả năng vị trí đó của bản rõ cần tìm là kí tự space
Ngoài ra, hoàn toàn có những trường hợp ngoại lệ, nhưng ta sẽ thử phương pháp trên để in ra bản rõ tạm thời, sau đó có thể dự đoán tiếp
Kết quả bản rõ cần tìm sau khi dùng phương pháp trên :

Th* secuet mes*age is* *htn us*n* * stream cipher* nev*r use the key more than

on**

Nhìn kết quả trên ta có thể hoàn thiện bản mã ở 1 vài vị trí và được kết quả bản rõ như sau :

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