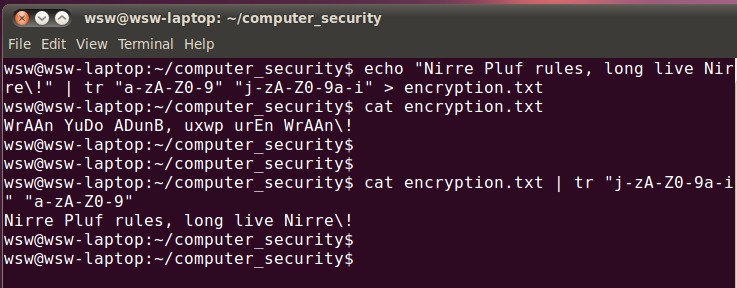
CSC648 Homework 1

Shuowen Wei

1.



2.

First of all, if we directly rewrite the plaintext with its corresponding ideographic writing for encryption purpose, then this is already letting out the original meaning of the plaintext; secondly, using ideographic writing is very limited to cryptography, can’t apply to encrypt massive information nowadays, and in the end, ideographic writing can’t get rid of human language’s redundancy, it is relatively easy to analyze and be decrypted.

3.

Based on the hints and some analysis, I think the most possible value of the keyword’s length is 12, but I still don’t break the cipher, it’s really embarrassing. ☹

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **a** | **d** | **g** | **i** | **k** | **m** | **o** | **q** | **s** | **u** | **w** | **y** |
| s |  |  |  |  |  |  |  |  |  |  |  |
| **b** | **e** | **h** | **j** | **l** | **n** | **p** | **r** | **t** | **v** | **x** | **z** |
| h | l | m | n | o | p | q | r | t |  |  |  |
| **c** | **f** |  | | | | | |  | |  | |
|  |  |  | |

where , twip

guess: “-ee-”, like “eem” “een” “eer” etc.

>> for i=2:(length(a)-2)

if( (a(i)=='l')&&(a(i+1)=='l') )

XeeX\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ XeeX=a(i-1:i+2)

end

end

XeeX\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_XeeX =

wllr

XeeX\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_XeeX =

rlla

Guess: m -> a

Some other guesses: c -> y, f -> z

a =

ejitpspawsqlejitaiulrtwllrflrllaoatwsqqjatgackthlsiraoatwlplqjatwjufrhlhutsqataqitatsaittkstqfjcae

v =

```tnanm`ape```tm``ert`eer`ereemlmt`app`mt`mY`tbea`rmlmt`enep`mt````rbeb`tapmtmp`tmtam`tt`atp``Ym`

4.

I tried several different columns of matrices (2-by-45, 3-by-30, 5-by-18, 6-by-15, 9-by-10, 10-by-9 etc) and it turns out that the 6-by-15 matrix works:

>> n=length(aa);

aa='aauancvlrerurnndltmeaeepbytusticeatnpmeyiicgogorchsrsocnntiiimihaoofpagsivttpsitlbolrotoex';

for i=1:6

for j=1:15

matrix(j,i)=aa(i\*15-15+j);

end

end

matrix

matrix =

adigit

alcomp

uteris

amachi

nethat

cansol

veprob

lemsfo

rpeopl

ebycar

ryingo

utinst

ructio

nsgive

ntoitx

5.

(a).

>> p=7;q=11;

n=(p-1)\*(q-1);

d=13;

gcd(d,n)

ans =

1

>> d=17;

gcd(d,n)

ans =

1

(b).

>> p=13;q=31;d=7;

n=(p-1)\*(q-1);

for k=1:100

if(mod(k\*n+1,d)==0)

k

break;

end

end

e=(k\*n+1)/d

k =

2

e =

103

(c).

>> p=5;q=11;d=27;

n=(p-1)\*(q-1);

for k=1:100

if(mod(k\*n+1,d)==0)

k

break;

end

end

e=(k\*n+1)/d

k =

2

e =

3

>> mod(1^e,n)

mod(2^e,n)

mod(3^e,n)

ans =

1

ans =

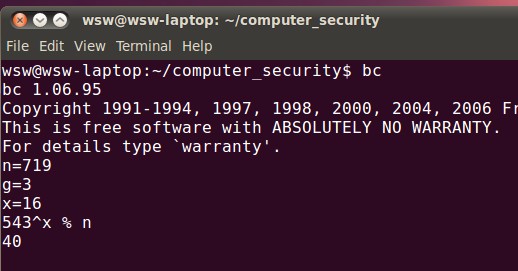
8

ans =

27

So, the e is 3 and encrypt {123}, we get {1,8,27}

6.



Thus the secret key is 40. We also computed the value of y and verified this:

>> for y=1:200

if(mod(3^y,719)==543)

y

end

end

y =

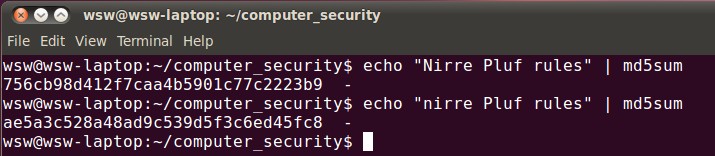
15



8.

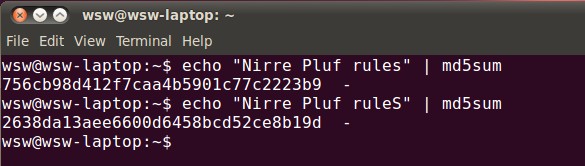
Since the Vigenere Cipher method uses multiple monoalphabetic substitution alphabets, so it’s harder just to analyze the frequency of each letter in the ciphertext, but we can focus some very common digrams or trigrams like ‘in’ ‘of’ ‘the’ ‘and’ ‘ing’ ‘ing’ etc. Through analyzing their repetitions in the ciphertext and the distance between each two repetitions, we can roughly narrow down their repetitions’ period, which is the length of the keyword. Once knowing the length of keyword, breaking Vigenere Cipher is equivalent to break a single monoalphabetic substitution by shifting the original ciphertext according to the period. We can then start to analyze the frequency of each letter.

9.



The percentage of characters in the two hashes is 100%, nothing remain the same with the previous output though the only difference is just the first letter of the input. And this is what we expect.

Even though when we merely change the last letter of the input, we still get the totally different output.



This is because “md5” employ a hash function to operate on the message, the whole is divided into several blocks each of which is 512 bits, and the output of transforming of last round is the input of next round, thus even a small change in the original message will affect the final output of the md5 hash function.