Attack of multiplicative inverse without using extended Euclid's algorithm

By
Adel Abed AL Gani Abed AL Wahab
Dyala University College of education / AL-Razy Computer science department

Abstract

The multiplicative cipher is one of the substitution cipher types so it is modified in this paper by extend the mod scale with 190 instead of 26, then utilized to do encryption for a plaintext. Therefore it produces a variation of symbols with more randomized cipher text so that it is enhanced. Then the major work in the paper is to attack the produced cipher text by search about the key inverse which found by an invented and effective equation, instead of the tradition Euclid's algorithm therefore successful attack was done.

1. Introduction

The encryption is used over centuries to kept security for the messages or the important information and data which must be kept and hide in some way faraway from unauthorized people .One of these encryption methods is a substitution cipher method in which letters are represented by other letters , then it can be deciphered by some one knowing the order of the cipher alphabet .Now we have a type of substitution cipher which known as a multiplicative cipher , this depend on multiplying the plain text by a key number then take it's mod for (26) [5]. In another hand there is a trying to break this cipher text without knowing the multiplicative key , This process is called an attack and it's require to find the multiplicative key inverse in some way without knowing the multiplicative key.In this paper the multiplicative cipher method is modified by change the mod space to (190) instead of (26) which equal to the difference between the numerical representation for the capital letter "A" and the last symbol numerical representation in computer, and that to obtain a more variant cipher text symbols , then we ignore this multiplicative key to try to attack the cipher text by find the multiplicative key inverse without using the Euclid's algorithm .

2. Substitution cipher

A system of encryption in which each letter of a message is replaced with another character, but retains its position within the message.

Monoalpbabetic

A substitution cipher system is the system that uses one alphabet throughout encryption. Simple substitution cipherSimple substitution ciphers replaced. Each character of plaintext with the corresponding character of the cipher text; a single one-to-one mapping from plaintext tocipher text characters is used to encipher an entire message [1].

2.1. Direct standard

The Caesar cipher is the one most famous and simplest of all ciphers. It is classified as a substitution cipher because the sender replaces the letters in the actual message with a new set of letters. In the Caesar cipher, each letter is replaced with the third letter following it in the alphabet. The alphabet wraps around, so if the letter in the actual message were X, Y, or Z, it would be replaced with A, B, or C, respectively. The modern English alphabet actually contains several letters not in the Roman alphabet, but we will demonstrate the cipher using the modern English alphabet.

Plaintext alpha:

A B C D E F GHIJKLMNOPQ R S T U V W X y Z

It's numerical representation

012345 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Cipher text alpha:

D E F GHIJKLMNOPQ R S T U V W X y Z A B C

It's numerical representation

345 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 012

Note that the key to deciphering a message encoded with a Caesar cipher (also called a Caesar shift) is knowing t he number of letters by which the alphabet is shifted. As we see, in Caesar cipher the key is k=3, we can choose a different value to the key in the range between 0 and 25.

C=Ek(m)=(25-m+k) mod 26

For example in the above example E3(A) = E3(0) = (0+3) mod 26 = 3 =D and E3(y) = E3(24) = (24+3) mod 26 = 1 = B and so on.

If the adversary received the cipher text and he know that the sender used the shift method, the only thing he need to do, is to try all the possibilities that equal to 25trials [1].

2.2. Standard reverse

This method is similar to the direct standard, except that the cipher text alphabet is written in reversed order from Z to A.

C=Ek(m)=(25-m+k) mod 26

For example if k=0 then,

Plaintext alpha:

A B C D E F GHIJKLMNOPQ R S T U V W X y Z

012345 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Cipher text alpha:

25	**24**	**23**	**22**	**21**	**20**	**19**	**18**	**17**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Z	**Y**	**X**	**W**	**V**	**U**	**T**	**S**	**R**	**Q**	**P**	**O**	**N**	**M**	**L**	**K**	**J**	**I**	**H**	**G**	**F**	**E**	**D**	**C**	**B**	**A**

2.3. Multiplicative cipher

Ciphers based on multiply each character by a key k; that is,

Ek(m)=(m*k) mod 26

Where k and 26 are relatively prime (GCD(k,26)=l), so that the letters of the alphabet produce a complete set of residues, so that in this cijse tie key must be an odd number and not equal to 13. So, if k=9 then, Plaintext alpha:

A	B	C	D	E	F	GHIJKLMNOPQ	R	S	T	U	V	W	X	y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher text alpha:

0	**9**	**18**	**1**	**10**	**19**	**2**	**11**	**20**	**3**	**12**	**21**	**4**	**13**	**22**	**5**	**14**	**23**	**6**	**15**	**24**	**7**	**16**	**25**	**8**	**17**
A	**J**	**S**	**B**	**K**	**T**	**C**	**L**	**U**	**D**	**M**	**V**	**E**	**N**	**W**	**F**	**O**	**X**	**G**	**P**	**Y**	**H**	**Q**	**Z**	**I**	**R**

For example in the above example E9(A) =E9(0) = (0*9) mod 26 = 0 =A and E9(Y) = E9(24) = (24*9) mod 26 = 8 = I and so on [4].

3. Modified multiplicative Ciphers

It is evident from the relative Multiplicative Cipher - or its encryption depending on the number 26 as a mod space, that such a system isn't offer a Varity of resulted cipher character. Let us think up a different method of enciphering a message. Instead of depending on 26 mod space, we shall depend on (190) mod space and multiply by the key number where

gcd(key,190)=1

Multiplicative cipher is done by multiply the value of a plain text character by the multiplicative key number then found it's mod to 190 as mode space, as in the following equation

C=(M×K) MOD 190

Where:

M: the value of the plain text character

K: the multiplicative key number where gcd (k,190)=1

C: the resulted cipher text character value

So let us suppose the following values for the alphabet

Letter	Value	Letter	Value	Letter	Value	Letter	Value	Letter	Value	Letter	Value
A	0	F	5	K	10	P	15	U	20	Z	25
B	1	G	6	L	11	Q	16	V	21		
C	2	H	7	M	12	R	17	W	22		
D	3	I	8	N	13	S	18	X	23		
E	4	J	9	O	14	T	19	Y	24		

We can suppose the multiplicative key as any number which educate the condition gcd(k,190)=1

For example K=3, 7, 9, 11, 13, 17, 21…

Example 1:

Now let us see what's happen when we take the following plaintext (fig-1) with different values of K as a multiplicative key

Hello dear how can I help you
Please just listen to me and tell me about your problem to find the best solution for it and good bye

Fig.1: Plain text

Then the cipher text with k=3 will be as in (fig-2)

VMbbkJMAtVk*f*GAhYVMbn‰k}
nbMAwM\}wzbYwzkhzkeMAhJzMbbeMADk}z‰k}tntkDbMezkPYhJzVMDMzwkb}zYkhPkt
YzSkkJD‰M

Fig.2: Cipher text with k=3

Now let us see what's happen for the cipher text (fig -3) when we take the value of K=9 to cipher the same above plaintext (fig-1)

€e¤¤¿\eAÚ€¿ISA¶‰€e¤È[¿õ
È¤eAãe'õãì¤‰ãì¿¶ì¿-eA¶\ìe¤¤-eAJ¿õì[¿õÚÈÚ¿J¤e-ì¿n‰¶\ì€eJeìã¿¤õì‰¿¶n¿Ú
‰ìw¿¿\J⌈e

Fig.3: The cipher text with k=9

4. Multiplicative Key inverse:

The multiplicative inverse "k-1" of "k" is such that k × k-1 = 1 mod m: An element "k" has a multiplicative inverse "k-1" if and only if gcd(k,m) = 1.

Definition: If gcd (k,m) = 1, then k and m are "relatively prime" and the multiplicative inverse of k exists [3].

Example:

i) Question: does multiplicative inverse exist with 3 mod 190?

Answer: yes because the gcd(3, 190) = 1

ii) Question: does multiplicative inverse exist with 5 mod 190?

Answer: No because the gcd(5, 190) ≠ 1

In this paper we invent the following equation to find the multiplication inverse (k-1).

k-1 = (190*i+1) / k where : i = 1,2,3,….. and (k-1) is an integer number

by using the ability of the computer iteration we can begin to submit (1) as a value of (i) in above , then check the result of k-1 if it is an integer number . if so , that's mean it is a correct multiplicative inverse value , else we try to submit (2) for the value of (i) , and so on until we find an integer k-1 to be a correct inverse , then can used to try to attack the cipher text .

That's scheme can be represented in algorithm-1 bellow

Algorithm -1 (to find the key inverse)

```
Function inverse(k, m As Long) As Long
Dim i As Long
 i = 1
 Do
  v = (m * i + 1) / k
  i = i + 1
 Loop Until Int(v) = v
 inverse = v
End Function
```

Now let us display in table -1 the following multiplicative keys with it inverse which found by the above scheme program

Table .1: Number of keys and its inverse depend on mod scale=190

Key	inverse	Key	inverse	Key	inverse
3	127	31	141	69	179
7	163	33	167	71	91
9	169	37	113	73	177
11	121	39	39	77	153
13	117	51	41	79	89
17	123	53	147	81	61
21	181	59	29	83	87
23	157	61	81	87	83
27	183	63	187	89	79
29	59	67	173	91	71

Respectively, there are several keys that we can found and use in the encryption process, therefore we have a wide chance for hide our message.

5. Attack

General ways in which a cryptanalyst may try to "break" or penetrate the secrecy of a cipher. These are not algorithms; they are just approaches as a starting place for constructing specific algorithms. In normal cryptanalysis we start out knowing plaintext, ciphertext, and cipher construction. The only thing left unknown is the key. A practical attack must recover

the key. (Or perhaps we just know the cipher text and the cipher, in which case a practical attack would recover plaintext.) Simply finding a distinguisher (showing that the cipher differs from the chosen model) is not, in itself, an attack. If an attack does not recover the key (or perhaps the particular key-selected internal state used in ciphering), it is not a real attack. In cryptography, when someone says they have "an attack," the implication is that they have a successful attack (a break) and not just another failed attempt. It is obviously much easier to simply claim to have an attack than to actually analyze, innovate, build and test a working attack, which makes it necessary to back up such claims with evidence. Arrogant claims, with "proof left as an exercise for the student" or "read the literature" responses, deserve jeers instead of the cowed respect they often get.

A claim to have an attack can be justified by:

1. Describing the process in such detail that others can understand it and could use it to break the cipher,
2. Actually performing the attack in practice and showing the claimed results (e.g., finding the unknown key, given known plaintext), or
3. demonstrating the ability to do something fundamental which should be impossible (like finding several strings which each have the same cryptographic hash result) [2].

6. Attack for multiplicative cipher of key space (190)

The attack for a multiplicative cipher text is divided into three steps and can be summarized in bellow

Generate a suggested multiplicative key which educate the condition gcd(key,190)=1

Find the inverse for the suggested key to be used in the next decipher step

Submit the found inverse in the bellow decipher equation , to try to find the plaintext

$M=(C\times k\text{-}1) \text{ MOD } 190$

Where:

M: the value of the resulted plain text character

k-1: the multiplicative key inverse number

C: the cipher text character value

Then if the attack is fail, we will return to the first step again to generate another multiplicative key and so on This attack method is still be done until the plain text be found.

Example2:

Now, let us suppose a plain text (fig-4), and encrypt it with multiplicative cipher method, depending on a key value (9), after that we will ignore the used multiplicative key and try to attack the cipher text by using the previous explained attack method

FINDING OUT ABOUT A PROGRAMMING LANGUAGE IS NOT A SPECTATOR SPORT I WILL TRY TO MAKE IT AS PAINLESS AS POSSIBLE BUT YOU HAVE TO POWER UP THE PC AND GET DOWN TO SOME SERIOUS PROGRAMMING LIMBER UP THE FIGUERS BREAK THE SPINE ON THE BOOK SO THAT IT LIES FLAT NEXT TO THE KEYBOARD AND SO THAT YOU CAN NOT TAKE IT BACK TO THE

Fig .4: The plain text

Now we will encrypt it with key value=9 to obtain a cipher text in (fig-5)

n‰¶\‰¶w¿õìAJ¿õìAÈÚ¿wÚA--‰¶w¤A¶wõAwe‰ã¶¿ìAãÈeSìAì¿ÚãÈ¿Úì‰I‰¤¤ìÚ[
ì¿-A›e‰ìAãÈA‰¶¤eããAãÈ¿ãã‰J¤eJõì[¿õ€Aþeì¿È¿IeÚõÈì€eÈSA¶\weì
\¿I¶ì¿ã¿-eãeÚ‰¿õãÈÚ¿wÚA--‰¶w¤‰-JeÚõÈì€en‰wõeÚãJÚeA›ì€eãÈ‰¶e¿¶ì€e
J¿¿›ã¿ì€Aì‰ì¤‰eãn¤Aì¶eRìì¿ì€e›e[J¿AÚ\A¶\ã¿ì€Aì[¿õSA¶¶¿ìiA›e
‰ìJAS›ì¿ì€eJ¿¿›ãì¿Úe

Fig.5: The cipher text with key value=9

Note: The resulted cipher characters are take a different symbol, so the space character is deleted from the cipher text to increase it's ambiguity.

Now we will try to attack the cipher text with a suggest keys and it's inverse.

When we suppose a multiplicative key =3 then it's inverse =127. The resulted text will be as in (fig-6)

PYhJYhSk}zADk}zAntkStAeeYhSbAhS}ASMYwhkzAwnMGzAzktwnktzY*f*Ybbzt‰
zkeA_MYzAwnAYhbMwwAwnkwwYDbMD}z‰k}VA€Mzknk*f*Mt}nzVMnGAhJSMz
Jk*f*hzkwkeMwMtYk}wntkStAeeYhSbYeDMt}nzVMPYS}MtwDtMA_zVMwnYhMkhzVM
Dkk_wkzVAzYzbYMwPbAzhM†zzkzVM_M‰DkAtJAhJwkzVAz‰k}GAhhkzzA_M
YzDAG zkzVMDkk wzktM

Fig.6: A wrong plain text

When we suppose a multiplicative key =7 then it's inverse =163. The resulted text will be as in (fig-7)

´Óˆ`Óˆ S‘ÆAÊS‘ÆAÜrS rA½½Óˆ òAˆ ‘A éÓûˆSÆAûÜé•ÆAÆSrûÜSrÆÓåÓòòÆr{
ÆS½AiéÓÆAûÜAÓˆòéûûAûÜSûûÓÊòéÊ‘Æ{S‘JA\éÆSÜSåér‘ÜÆJéÜ•Aˆ` éÆ
`Såˆ ÆSûS½éûérÓS‘ûÜrS rA½½Óˆ òÓ½Êér‘ÜÆJé´Ó ‘érûÊréAiÆJéûÜÓˆéSˆÆJé
ÊSSiûSÆJAÆÓÆòÓéû´òAÆˆé°ÆÆSÆJéié{ÊSAr`Aˆ`ûSÆJAÆ{S‘•Aˆ^SÆÆAié
ÓÆÊA•iÆSÆJéÊSSiûÆSré

Fig.7: A wrong plain text

When we suppose a multiplicative key =9 then it's inverse =169. The resulted text will be as in (fig-8)

FINDINGOUTABOUTAPROGRAMMINGLANGUAGEISNOTASPECTATORSPORTIWILLTRY
TOMAKEITASPAINLESSASPOSSIBLEBUTYOUHAVETOPOWERUPTHEPCANDGET
DOWNTOSOMESERIOUSPROGRAMMINGLIMBERUPTHEFIGUERSBREAKTHESPINEONTHE
BOOKSOTHATITLIESFLATNEXTTOTHEKEYBOARDANDSOTHATYOUCANNOTTAKE
ITBACKTOTHEBOOKSTORE

Fig.8: A successful plain text

Note: A successful plain text characters are appeared and we can recognize it's words easily.

7. The implementation:

We use the following visual basic program to execute our cipher and attack method:-

```
Dim key As Integer
Dim cx As String
Function inverse(k, m As Long) As Long
Dim i As Long
```

```
 i = 1
 Do
  v = (m * i + 1) / k
  i = i + 1
 Loop Until Int(v) = v
 inverse = v
End Function
Function gcd(a, key As Integer) As Integer
  b = key
 Dim q, r1, r2 As Integer
  q = Int(a / b)
  r1 = a Mod b
  If r1 = 0 Then
     gcd = b
     Exit Function
  End If
  Do
  a = b
  b = r1
  q = Int(a / b)
  r2 = a Mod b
  If r2 <> 0 Then r1 = r2
  Loop Until r2 = 0
  gcd = r1
End Function


Private Sub Command3_Click()
Do
key = key + 2
Loop Until gcd(190, key) = 1
Text1.Text = key
inv = inverse(key, 190)
Text2.Text = inv
X2 = ""
For i = 1 To Len(cx)
  ch = Mid(cx, i, 1)
   If Asc(ch) <> 10 And Asc(ch) <> 13 Then
     c = Asc(ch) - 65
     m = (c * inv) Mod 190
     ch = Chr(m + 65)
   End If
   X2 = X2 + ch
Next i
Text5.Text = X2
End Sub

Private Sub Command4_Click()
key = 1
Command3.Enabled = True
cx = Text5.Text
End Sub

Private Sub Command5_Click()
Dim s As String
Open "d:\aa.txt" For Input As #1
Do
```

```
Input #1, s
Text5.Text = Text5.Text + s + Chr(13) + Chr(10)
Loop Until EOF(1)
Close #1
End Sub

Private Sub Command6_Click()
End
End Sub

Private Sub Command7_Click()
Dim x As String
If Text6.Text = "" Then
  MsgBox ("please give your suggested key")
  Exit Sub
End If
k = Val(Text6.Text)
m = 190
X2 = ""
X1 = Text5.Text
For i = 1 To Len(X1)
 ch = Mid(X1, i, 1)
 If ch <> " " Then
  If ch >= "A" And ch <= "Z" Then
    n = Asc(ch) - 65
    c = (n * k) Mod m
    ch = Chr(c + 65)
  End If
  X2 = X2 + ch
 End If
Next i
Text5.Text = X2
End Sub

Private Sub Command8_Click()
s = Text5.Text
Open "d:\dd.text" For Output As #1
Print #1, s
Close #1

End Sub

Private Sub Command9_Click()
Text5.Text = ""
End Sub
```

8. Conclusions:

We can obtain a good cipher text with more randomization by extend the mod scale to 190 instead of just 26 in a modified multiplicative cipher text. The number of the probable keys, which can be used in a multiplicative cipher, is be larger if we extend the mod scale. Key

inverse which will be used in decipher or to attack the cipher text is can be found by utilize the computer ability in iteration and apply an invented equation.

9. Discussions:

There is an idea to develop the multiplicative cipher method by merge it with another cipher algorithm , that's mean we apply multiplicative cipher method then consider the resulted cipher text as an input to another cipher method , so that the cipher text will be stronger , then the attack operation will be more difficult , Choosing another mod scale number to increase the number of possible keys according to its conditions. Using an automatic text test method to check if it is a plain text or not ,that's can be done by take some small words in the tested text and compare it with such possible words in the language , this idea will increase the speed to attack that developed in this paper.

References

[1]. APPLIED CRYPTOGRAPHY AND DATA SECURITY, Prof. Christof Paar (version 2.5 — January 2005)

[2]. Gilles Brassard, Modern Cryptology, Lecture Notes in Computer Paual B. Garrett, Cryptology and Number Theory, Course notes, 1999.

[3]. Douglas S. Stinton, Cryptography: Theory and Practice, 2002.

[4]. D. R. Hankerson, et. al, Coding Theory and Cryptography: the Essentials, 2000

[5]. Technology of information security and protection system د. علاء الحمامي 2007.