Understanding Cryptography
Answers of Homework No.1

1.7.

برای حل این مساله Z_4 را در نظر گرفته و جدولی می سازیم که جمع همه المان ها را در حلقه نشان دهد.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	4
2	2	3	4	5
3	3	4	5	6

1. ساخت جدول ضرب برای Z_4

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2. ساخت جدول جمع و ضرب برای Z_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4

2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. ساخت جدول جمع و ضرب برای Z_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. در Z_4 و Z_6 المان‌هایی وجود دارند که معکوس ضربی ندارند این المان ها کدام هستند؟ و چرا یک معکوس ضربی برای همه ی المان های غیر صفر در Z_5 وجود دارد؟

حل:

تعریف معکوس ضربی:

$$a * a^{-1} = a^{-1} * a = e$$

$$a^{-1} \times a \equiv 1 \bmod m \ : a \text{ has multiplicative inverse such } a^{-1} \quad if \ \gcd(a,m) = 1$$

یا به عبارتی دیگر در Z_m هر عدد a که $\gcd(a,m) \neq 1$ باشد معکوس ضربی ندارد.

$Z_4: a = 0, 1, 2, 3$

$\{1, 2, 3\} \rightarrow \emptyset(n) = 2$

منظور از اعداد نشان داده شده با رنگ قرمز اعداد اول نسبت به 4 است. برای عدد صفر هم که معکوس تعریف نمی شود.

$$a^{-1} = 1^{2-1} = 1 \bmod 4 = 1 \qquad \rightarrow 1 * 1 = 1 \bmod 4 = 1 \ \surd$$

$$a^{-1} = 2^{2-1} = 2 \bmod 4 = 2 \quad \rightarrow \quad 2 * 2 \bmod 4 = 0 \quad \times$$
$$a^{-1} = 3^{2-1} = 3 \bmod 4 = 3 \quad \rightarrow \quad 3 * 3 \bmod 4 = 1 \surd$$

پس نتیجه می‌گیریم که در Z_4 المانهای 2 معکوس ضربی ندارد و المانهای 1 و 3 معکوس ضربی دارند.

Z_6: $a = 0, 1, 2, 3, 4, 5$
$\{1, 2, 3, 4, 5\} \rightarrow \emptyset(n) = 2$

منظور از اعداد نشان داده شده با رنگ قرمز اعداد اول نسبت به 6 است.

$$a^{-1} = 1^{-1} = 1^{2-1} = 1 \bmod 6 = 1 \quad \rightarrow 1 * 1 = 1 \bmod 6 = 1 \surd$$
$$a^{-1} = 2^{-1} = 2^{2-1} = 2 \bmod 6 = 2 \quad \rightarrow \quad 2 * 2 \bmod 6 = 4 \quad \times$$
$$a^{-1} = 3^{-1} = 3^{2-1} = 3 \bmod 6 = 3 \quad \rightarrow \quad 3 * 3 \bmod 6 = 3 \quad \times$$
$$a^{-1} = 4^{-1} = 4^{2-1} = 4 \bmod 6 = 4 \quad \rightarrow 4 * 4 \bmod 6 = 4 \quad \times$$
$$a^{-1} = 5^{-1} = 5^{2-1} = 5 \bmod 6 = 5 \quad \rightarrow 5 * 5 \bmod 6 = 1 \surd$$

پس نتیجه می‌گیریم که در Z_6 المان های (2, 3, 4) معکوس ضربی ندارند و المان(1,5) معکوس ضربی دارند. برای عدد صفر هم که معکوس تعریف نمی شود.

Z_5:
$a = 0, 1, 2, 3, 4$
$\{1, 2, 3, 4\} \rightarrow \emptyset(n) = 4$
منظور از اعداد نشان داده شده با رنگ قرمز اعداد اول نسبت به 5 است. برای عدد صفر هم که معکوس تعریف نمی شود.

$$a^{-1} = 1^{-1} = 1^{4-1} = 1 \bmod 5 = 1 \quad \rightarrow 1 * 1 = 1 \bmod 5 = 1 \surd$$
$$a^{-1} = 2^{-1} = 2^{4-1} = 8 \bmod 5 = 3 \quad \rightarrow \quad 3 * 2 \bmod 5 = 1 \surd$$
$$a^{-1} = 3^{-1} = 3^{4-1} = 27 \bmod 5 = 2 \quad \rightarrow \quad 2 * 3 \bmod 5 = 1 \surd$$
$$a^{-1} = 4^{-1} = 4^{4-1} = 64 \bmod 5 = 4 \quad \rightarrow \quad 4 * 4 \bmod 5 = 1 \surd$$

... ...

نتیجه می گیریم چون عدد 5 نسبت به تمام اعضای غیرصفر موجود در حلقه اول است و همه ی المان های غیر صفر کوچکتر از 5 نسبت به 5 اول هستند پس معکوس ضربی وجود دارد.

1.8.

همانطور که می دانیم معکوس یک عدد integer در یک حلقه کاملا وابسته به آن حلقه است. اگر پیمانه تغییر کند معکوس هم تغییر می‌کند. یعنی معکوس یک المان به تنهایی معنایی ندارد و باید حتما پیمانه آن ذکر گردد.

$$5^{-1} \bmod 11 \equiv ?$$

$$5^{-1}\ mod\ 12 \equiv ?$$
$$5^{-1}\ mod\ 13 \equiv ?$$

طبق این نکته که $a^{-1} = a^{\emptyset(n)-1}\ mod\ n$

$$Z_n^* = \{\ a \in Z_n \parallel \gcd(a,n) = 1\ \}$$

$\emptyset(n)$ تابع فی اویلر برابر تعداد اعدادی از مجموعه ی $\{1, \ldots, n\}$ است که نسبت به n اول هستند.

$$\emptyset(11) = 10 \qquad \{1,2,3,4,5,6,,7,8,9,10,11\}$$

منظور از اعداد قرمز رنگ اعداد کوچکتر از 11 است که نسبت به 11 اول هستند.

$$\emptyset(12) = 4 \qquad \{1,2,3,4,5,6,7,8,9,10,11,12\}$$

منظور از اعداد قرمز رنگ اعداد کوچکتر از 12 است که نسبت به 12 اول هستند.

$$\emptyset(13) = 12 \qquad \{1,2,3,4,5,6,,7,8,9,10,11,12,13\}$$

منظور از اعداد قرمز رنگ اعداد کوچکتر از 13 است که نسبت به 13 اول هستند.

1. $5^{-1} = 5^{10-1} = 5^9\ mod\ 11 = 5^3 \times 5^3 \times 5^3\ mod\ 11$
$= 4 \times 4 \times 4\ mod\ 11 = 64\ mod\ 11 = 9\ mod\ 11$

2. $5^{-1} = 5^{4-1} = 5^3\ mod\ 12 = 125\ mod\ 12 = 5\ mod\ 12$

3. $5^{-1} = 5^{12-1} = 5^{11}\ mod\ 13 = 5^4 \times 5^4 \times 5^3\ mod\ 13$
$= 1 \times 1 \times 8\ mod\ 13 = 8\ mod\ 13$

1.9.

هدف یافتن مقدار x است.

1. $3^2\ mod\ 13 = 9\ mod\ 13$

2. $7^2\ mod\ 13 = 49\ mod\ 13 = 10\ mod\ 13$

3. $3^{10}\ mod\ 13 = (3^2)^5\ mod\ 13 = 9^5\ mod\ 13 = 9^2 \times 9^2 \times 9^1\ mod\ 13$
$= 81 \times 81 \times 9\ mod\ 13 = 3 \times 3 \times 9\ mod\ 13 = 3^2 \times 9\ mod\ 13$
$= 81\ mod\ 13 = 3\ mod\ 13$

or

3. $3^{10}\ mod\ 13\ =\ 3^9 \times 3\ mod\ 13 = (3^3)^3 \times 3\ mod\ 13 = 1^3 \times 3\ mod\ 13$
$= 3\ mod\ 13$

4. $7^{100}\ mod\ 13\ =\ (7^2)^{50}\ mod\ 100 =\ 49^{\ 50}\ mod\ 13 =\ 10^{50}\ mod\ 13$
$=\ (10^2)^{25}\ mod\ 13 = 100^{25}\ mod\ 13 =\ 9^{25}\ mod\ 13$
$=\ (9^2)^{12}\ \times 9\ mod\ 13 =\ 81^{12} \times 9\ \ mod\ 13 =\ 3^{12}\ \times 9\ mod\ 13$
$=\ (3^3)^4\ \ \times 9\ mod 13 =\ 27^4 \times 9\ mod\ 13 =\ 1^4\ \times 9\ \ mod\ 13$
$= 9\ mod\ 13$

5. $7^x = 11 mod\ 13 \quad \rightarrow x = 5$

با روش سعی و خطا مقدار $x = 5$ می شود. این یک مساله لگاریتم گسسته است .

1.10.

$m = 4 \quad \{1,2,3,4\} \quad \emptyset(4) = 2$

$\gcd(1,4) = 1$
$\gcd(3,4) = 1$

$\emptyset(m)$ برابر است با تعداد اعدادی از مجموعه ی $\{1, \dots, m\}$ که نسبت به m اول هستند.

$m = 5 \qquad \{1,2,3,4,5\} \qquad \emptyset(5) = 4$

$\gcd(1,5) = 1$
$\gcd(2,5) = 1$
$\gcd(3,5) = 1$
$\gcd(4,5) = 1$

$m = 9 \qquad \{1,2,3,4,5,6,7,8,9\} \qquad \emptyset(9) = 6$

$\gcd(1,9) = 1$
$\gcd(2,9) = 1$
$\gcd(4,9) = 1$
$\gcd(5,9) = 1$
$\gcd(7,9) = 1$
$\gcd(8,9) = 1$

$m = 26 \qquad \{1,3,5,7,9,11,15,17,19,21,23,25\} \qquad \emptyset(26) = 12$

1.13.

$$\forall\, x, y, a, b \;\in\; Z_{26}$$

در $Affine\ cipher$ داریم:

$$y = e_k(x) = ax + b \mod 26$$
$$x = d_k(y) = a^{-1}(y - b) \mod 26$$

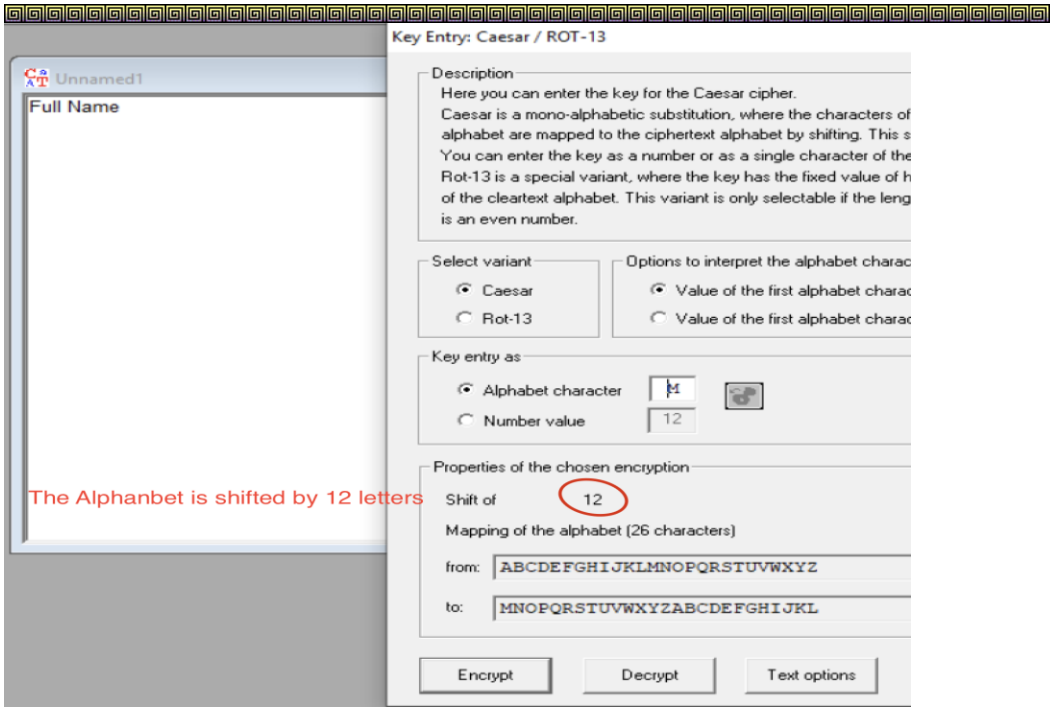
$$k = (a, b)$$

$$= \begin{cases} y_1 - a\,x_1 = b \\ y_2 - a\,x_2 = b \end{cases} \rightarrow \begin{cases} -y_1 + a\,x_1 = -b \\ y_2 - a\,x_2 = b \end{cases}$$

$$a = (x_1 - x_2)^{-1}(y_1 - y_2) \mod m$$
$$b = (y_1 - (x_1 - x_2)^{-1}(y_1 - y_2)x_1) \mod m = y_1 - ax_1 \mod m$$

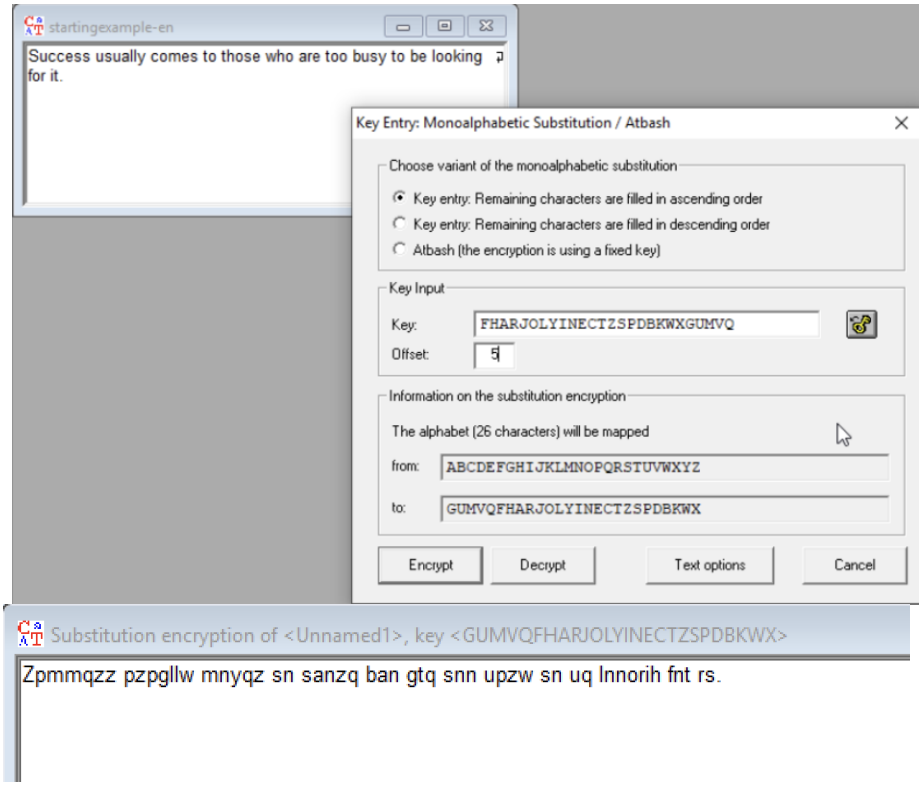
نکته : حتما باید معکوس $(x_1 - x_2)$ در پیمانه m و $\gcd((x_1 - x_2), m) = 1$ باشد.

2.

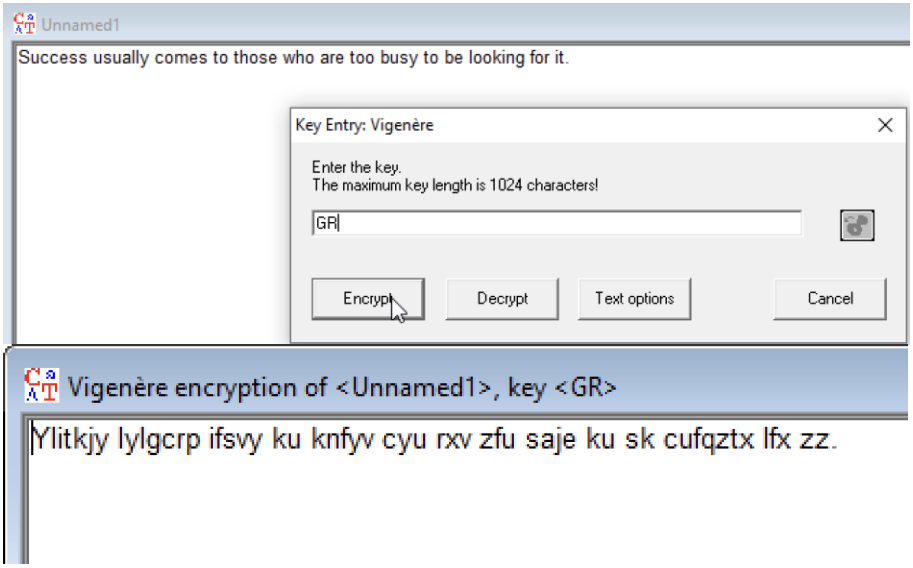


2.

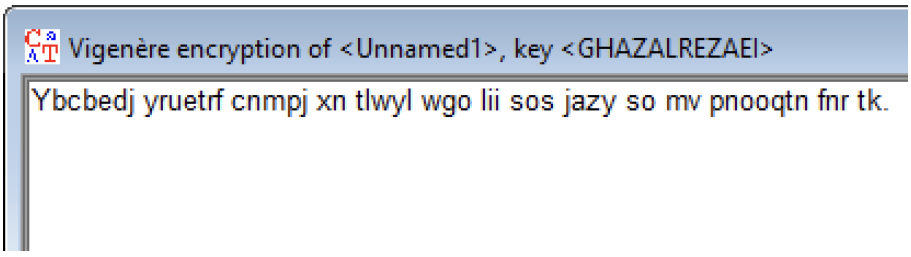
My Student No is 9527393 which equals 26*366438+5. Meaning that I should use the number 5 as my offset to the substitution cipher.


startingexample-en
Success usually comes to those who are too busy to be looking for it.
Key Entry: Monoalphabetic Substitution / Atbash
Choose variant of the monoalphabetic substitution
Key entry: Remaining characters are filled in ascending order
Key entry: Remaining characters are filled in descending order
Atbash (the encryption is using a fixed key)
Key Input
Key: FHARJOLYINECTZSPDBKWXGUMVQ
Offset: 5
Information on the substitution encryption
The alphabet (26 characters) will be mapped
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ
to: GUMVQFHARJOLYINECTZSPDBKWX
Encrypt
Decrypt
Text options
Cancel
Substitution encryption of <Unnamed1>, key <GUMVQFHARJOLYINECTZSPDBKWX>
Zpmmqzz pzpgllw mnyqz sn sanzq ban gtq snn upzw sn uq lnnorih fnt rs.

3.

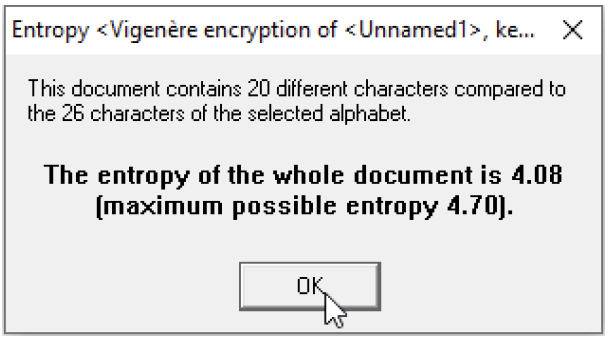

Unnamed1
Success usually comes to those who are too busy to be looking for it.
Key Entry: Vigenère
Enter the key.
The maximum key length is 1024 characters!
GR
Encrypt
Decrypt
Text options
Cancel
Vigenère encryption of <Unnamed1>, key <GR>
Ylitkjy lylgcrp ifsvy ku knfyv cyu rxv zfu saje ku sk cufqztx lfx zz.

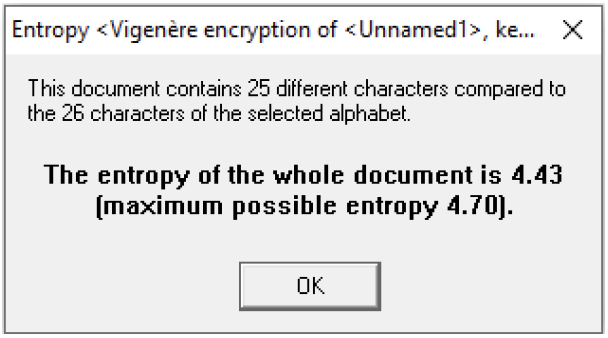
b.


Vigenère encryption of <Unnamed1>, key <GHAZALREZAEI>
Ybcbedj yruetrf cnmpj xn tlwyl wgo lii sos jazy so mv pnooqtn fnr tk.

c.

As observable in the following pictures the entropy of the document encrypted with the shorter key is 4.08, which is way smaller compared to the ciphertext with the longer key (4.43).

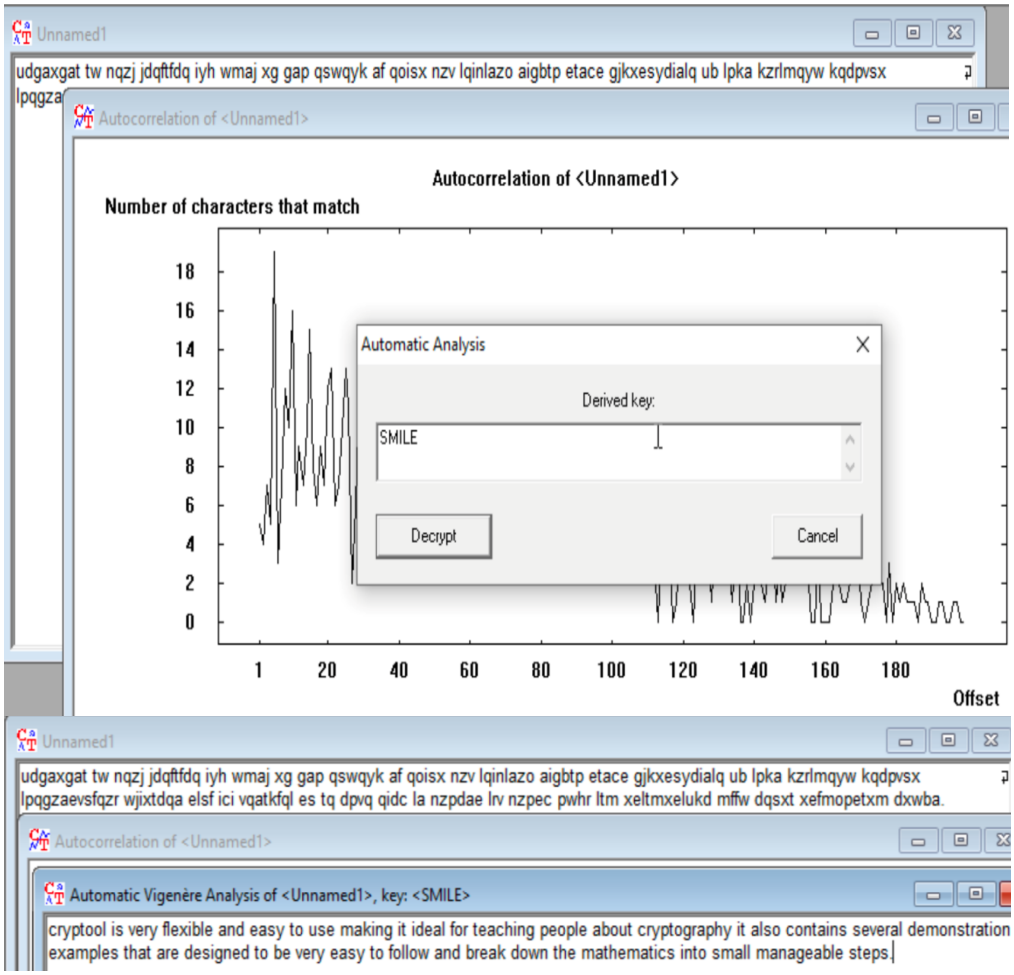




Entropy is a measure of the "randomness" of the data in a file, where typical text files will have a low value, and encrypted or compressed data will have a high measure. If data is encrypted, it will have a higher entropy value compared to one that isn't. Actually, in encrypted files, character distribution is random, or at least much more random than a "normal" data file. Therefore, the lower its entropy, the more probable a file is a normal or weakly encrypted one.

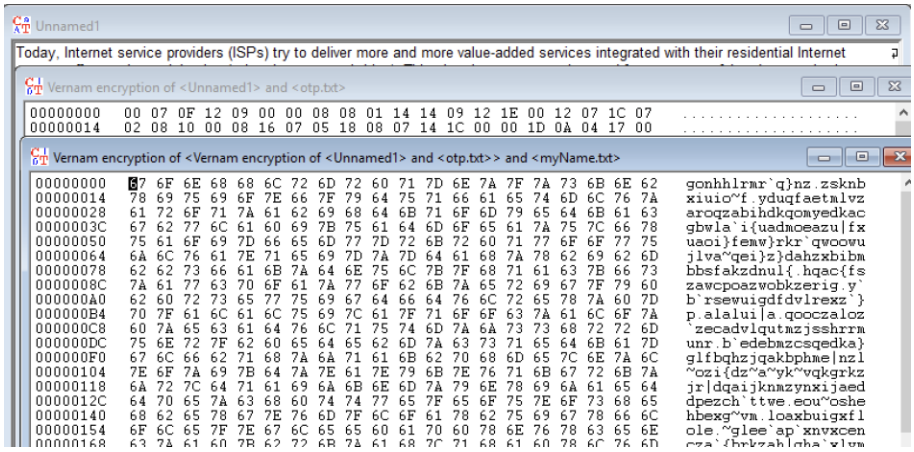
4.

The autocorrelation tool analyses different sections of a message and compares them to find similarities. It is possible to derive the length of the key using this tool, when the message is encrypted with the Vigenère cipher.



5. a&b.

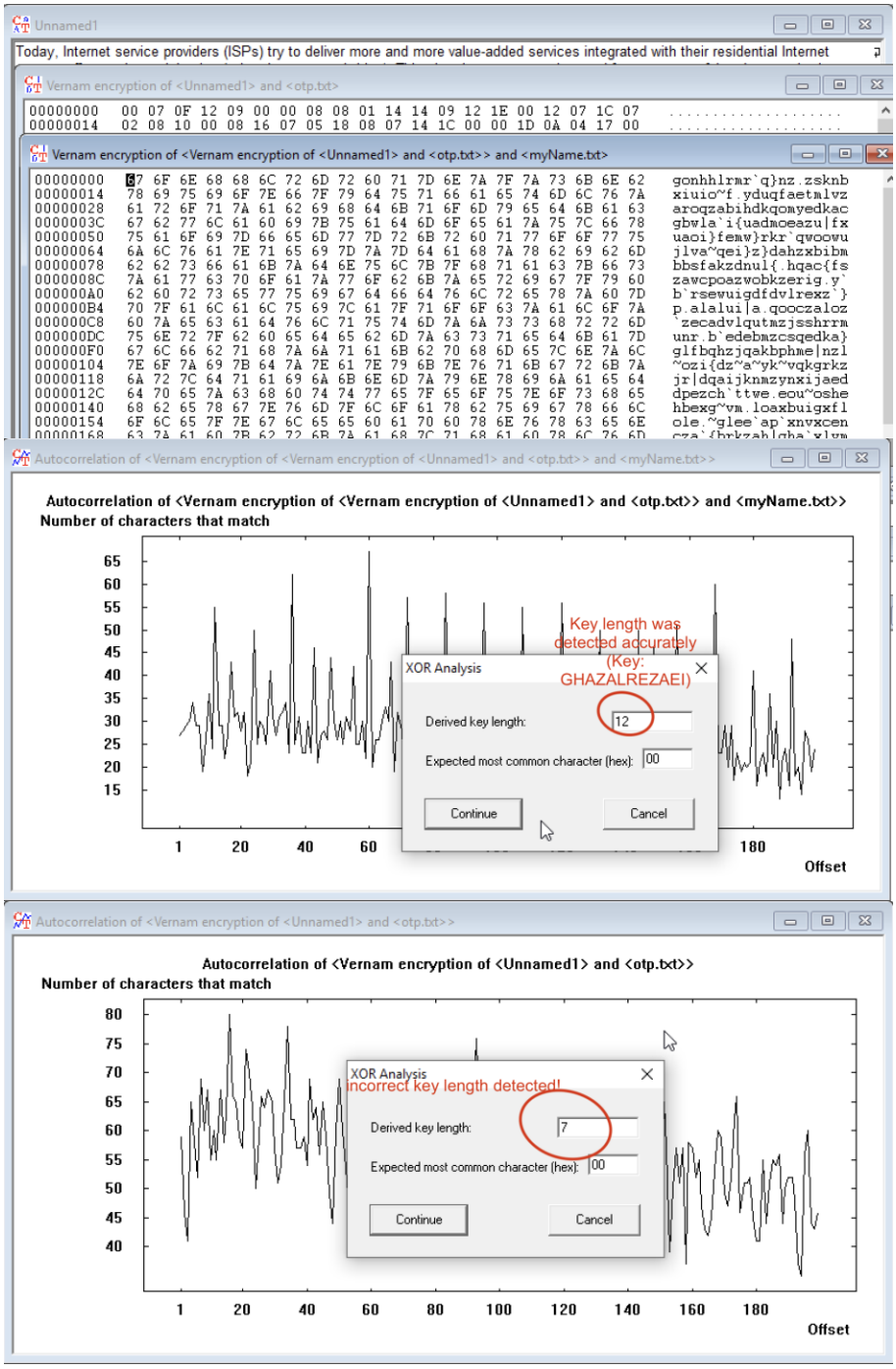
Simply follow the instructions in the question.

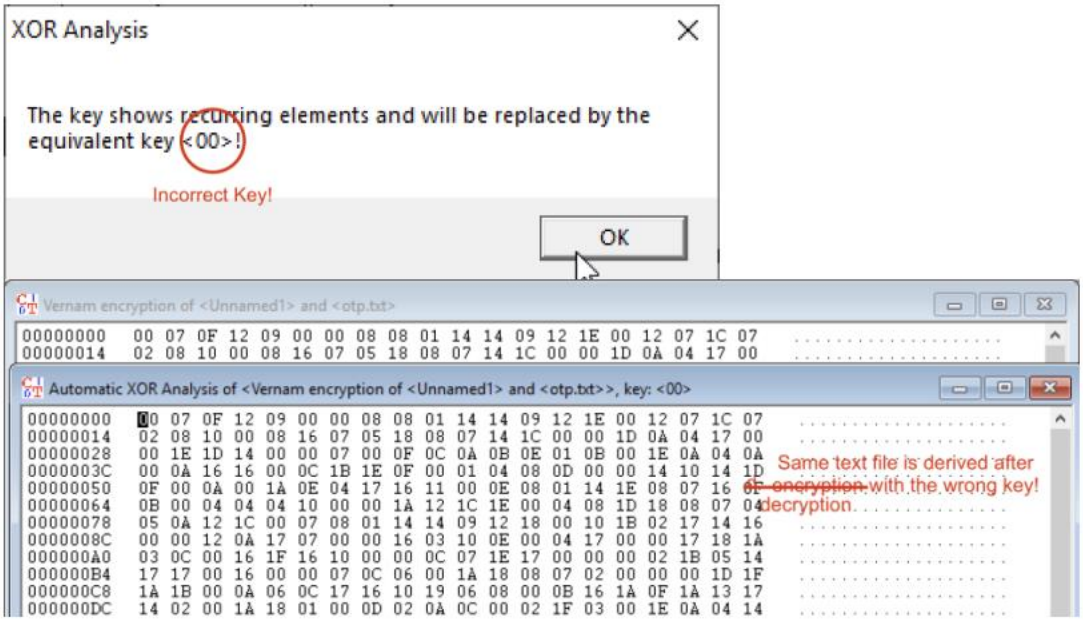


c.

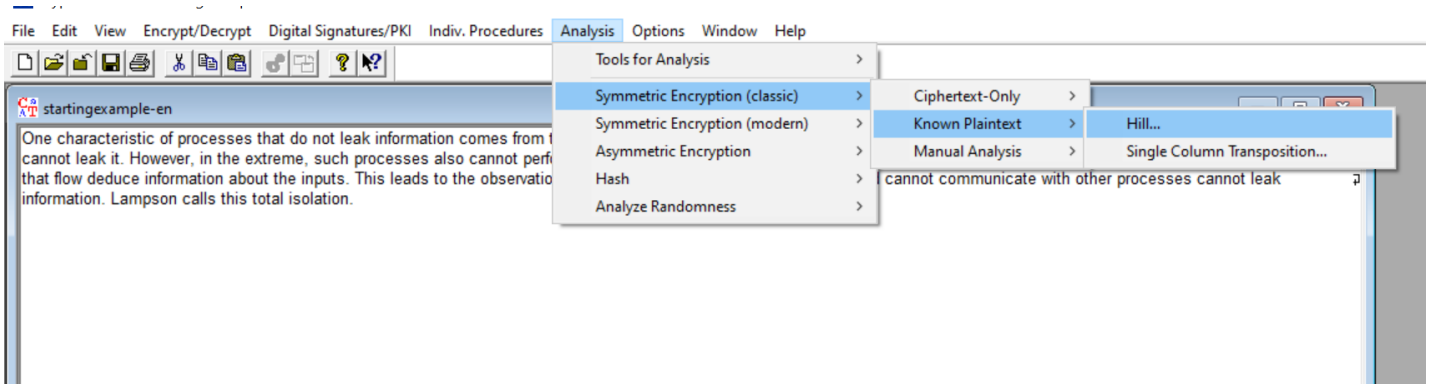
In One Time Pad, if key is shorter than message, it means that some part of text will be encrypted with same part of key, two or more time. In this case, by XORing two part

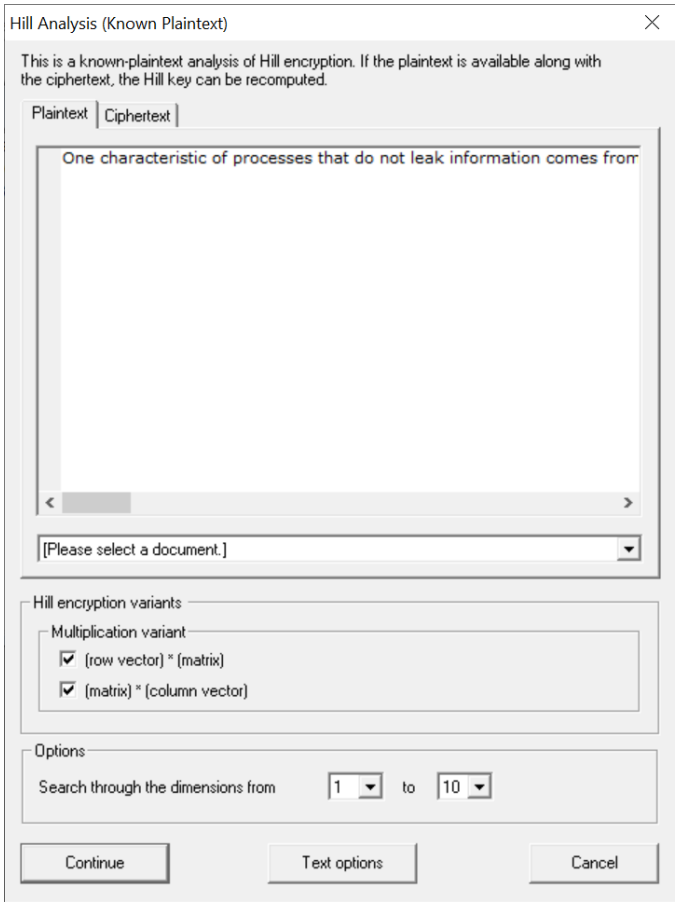
encrypted with the same key, adversary can receive tiny pieces of information about plaintext. If key is significantly shorter than plaintext, adversary can apply frequency analysis to discover the whole message, or a part of it. As displayed in below figure, the frequency analysis tool has successfully discovered the key length of the shorter OTP key.

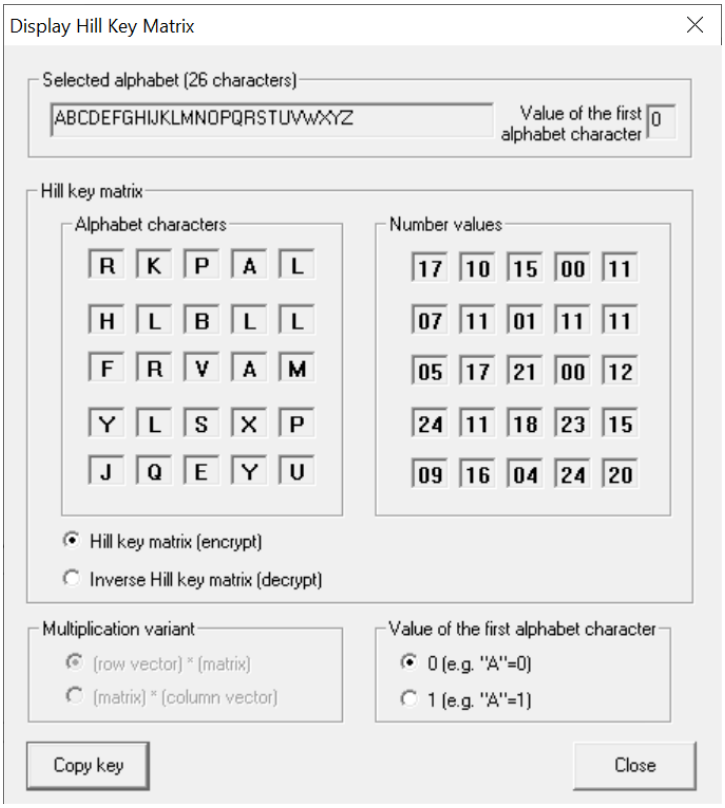


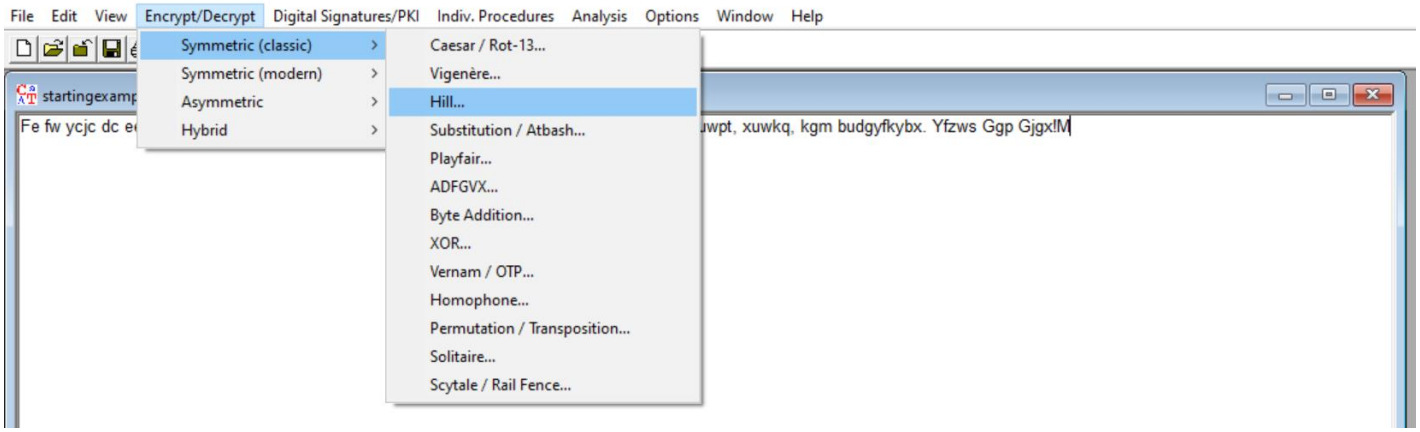

XOR Analysis
The key shows recurring elements and will be replaced by the equivalent key <00>!
Incorrect Key!
OK
Vernam encryption of <Unnamed1> and <otp.txt>
00000000 00 07 0F 12 09 00 00 08 08 01 14 14 09 12 1E 00 12 07 1C 07
00000014 02 08 10 00 08 16 07 05 18 08 07 14 1C 00 00 1D 0A 04 17 00
Automatic XOR Analysis of <Vernam encryption of <Unnamed1> and <otp.txt>>, key: <00>
00000000 00 07 0F 12 09 00 00 08 08 01 14 14 09 12 1E 00 12 07 1C 07
00000014 02 08 10 00 08 16 07 05 18 08 07 14 1C 00 00 1D 0A 04 17 00
00000028 00 1E 1D 14 00 00 07 00 0F 0C 0A 0B 0E 01 0B 00 1E 0A 04 0A
0000003C 00 0A 16 16 00 0C 1B 1E 0F 00 01 04 08 0D 00 00 14 10 14 1D
00000050 0F 00 0A 00 1A 0E 04 17 16 11 00 0E 08 01 14 1E 08 07 16 0F
00000064 0B 00 04 04 04 10 00 00 1A 12 1C 1E 00 04 08 1D 18 08 07 04
00000078 05 0A 12 1C 00 07 08 01 14 14 09 12 18 00 10 1B 02 17 14 16
0000008C 00 00 12 0A 17 07 00 00 16 03 10 0E 00 04 17 00 00 17 18 1A
000000A0 03 0C 00 16 1F 16 10 00 00 0C 07 1E 17 00 00 00 02 1B 05 14
000000B4 17 17 00 16 00 00 07 0C 06 00 1A 18 08 07 02 00 00 00 1D 1F
000000C8 1A 1B 00 0A 06 0C 17 16 10 19 06 08 00 0B 16 1A 0F 1A 13 17
000000DC 14 02 00 1A 18 01 00 0D 02 0A 0C 00 02 1F 03 00 1E 0A 04 14
Same text file is derived after ~~en~~decryption with the wrong key!

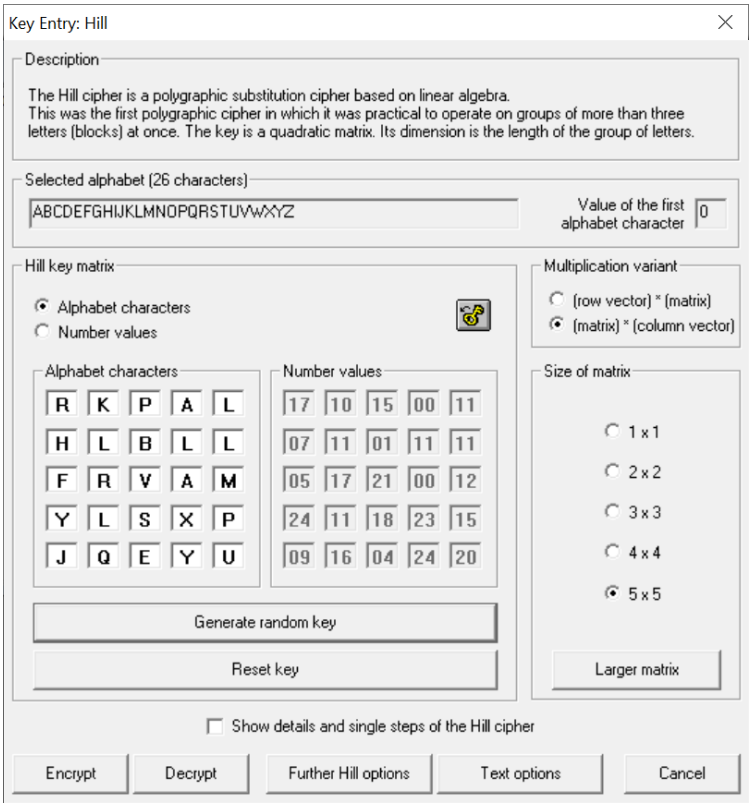
6.

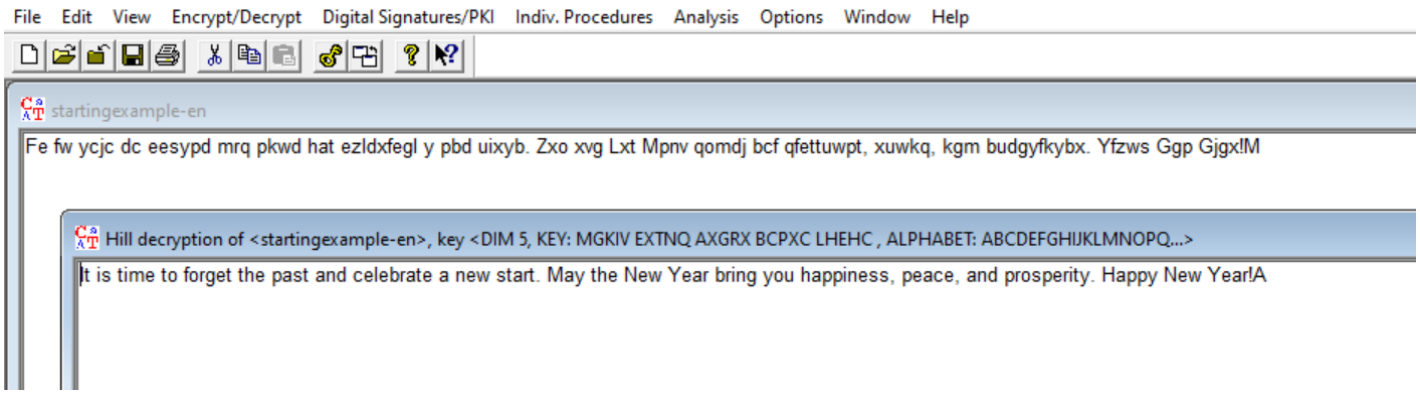

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Tools for Analysis
Symmetric Encryption (classic)
Symmetric Encryption (modern)
Asymmetric Encryption
Hash
Analyze Randomness
Ciphertext-Only
Known Plaintext
Manual Analysis
Hill...
Single Column Transposition...
startingexample-en
One characteristic of processes that do not leak information comes from t
cannot leak it. However, in the extreme, such processes also cannot perf
that flow deduce information about the inputs. This leads to the observatio
information. Lampson calls this total isolation.
cannot communicate with other processes cannot leak


Hill Analysis (Known Plaintext)
This is a known-plaintext analysis of Hill encryption. If the plaintext is available along with the ciphertext, the Hill key can be recomputed.
Plaintext
Ciphertext
One characteristic of processes that do not leak information comes from
[Please select a document.]
Hill encryption variants
Multiplication variant
(row vector) * (matrix)
(matrix) * (column vector)
Options
Search through the dimensions from
1
to
10
Continue
Text options
Cancel


Display Hill Key Matrix
Selected alphabet (26 characters)
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Value of the first alphabet character
0
Hill key matrix
Alphabet characters
R K P A L
H L B L L
F R V A M
Y L S X P
J Q E Y U
Number values
17 10 15 00 11
07 11 01 11 11
05 17 21 00 12
24 11 18 23 15
09 16 04 24 20
Hill key matrix (encrypt)
Inverse Hill key matrix (decrypt)
Multiplication variant
(row vector) * (matrix)
(matrix) * (column vector)
Value of the first alphabet character
0 (e.g. "A"=0)
1 (e.g. "A"=1)
Copy key
Close


File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
Caesar / Rot-13...
Vigenère...
Hill...
Substitution / Atbash...
Playfair...
ADFGVX...
Byte Addition...
XOR...
Vernam / OTP...
Homophone...
Permutation / Transposition...
Solitaire...
Scytale / Rail Fence...
startingexamp
Fe fw ycjc dc e
uwpt, xuwkq, kgm budgyfkybx. Yfzws Ggp Gjgx!M


Key Entry: Hill
Description
The Hill cipher is a polygraphic substitution cipher based on linear algebra.
This was the first polygraphic cipher in which it was practical to operate on groups of more than three letters (blocks) at once. The key is a quadratic matrix. Its dimension is the length of the group of letters.
Selected alphabet (26 characters)
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Value of the first alphabet character
0
Hill key matrix
Alphabet characters
Number values
Alphabet characters
R K P A L
H L B L L
F R V A M
Y L S X P
J Q E Y U
Number values
17 10 15 00 11
07 11 01 11 11
05 17 21 00 12
24 11 18 23 15
09 16 04 24 20
Generate random key
Reset key
Multiplication variant
(row vector) * (matrix)
(matrix) * (column vector)
Size of matrix
1 x 1
2 x 2
3 x 3
4 x 4
5 x 5
Larger matrix
Show details and single steps of the Hill cipher
Encrypt
Decrypt
Further Hill options
Text options
Cancel


File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Fe fw ycjc dc eesypd mrq pkwd hat ezldxfegl y pbd uixyb. Zxo xvg Lxt Mpnv qomdj bcf qfettuwpt, xuwkq, kgm budgyfkybx. Yfzws Ggp Gjgx!M
Hill decryption of <startingexample-en>, key <DIM 5, KEY: MGKIV EXTNQ AXGRX BCPXC LHEHC , ALPHABET: ABCDEFGHIJKLMNOPQ...>
It is time to forget the past and celebrate a new start. May the New Year bring you happiness, peace, and prosperity. Happy New Year!A