

HILL CIPHER CRYPTANALYSIS COMPLEMENT

STUDENTS: BASTIDA PRADO JAIME ARMANDO

SOLORIO PAREDES DANIEL

PROFESSOR: DÍAZ SANTIAGO SANDRA

SUBJECT: CRYPTOGRAPHY

GROUP: 3CM6

March 13th 2019

1. Hill Cipher Cryptanalysis Complement

As told by the teacher we exchange a pair of ciphertext and plaintext with the other team and proceeded to do the cryptanalysis.

1.1. Technical Problems

In the way to find the key we had several problems, first our program did not validate the key at that time. So when we thought the key was correct we soon found it was not the case, since several times its determinant was not valid i.e. it did not satisfy $\gcd(\det, 95) = 1$. Another problem we had is that the other team enciphered the space character and we did not.

1.2. Testing the program

Plaintext taken:

```
Crawl with insects and feed on barren soil!
Or rise above the animal in you!
Find kindness among the unkind!
Slowness ov decrepitude
Like sirens beckoning me to their ruined shores!
Impotent in the eye ov the storm!
Cthonic ore forefathers!
Ravishing sires ov the black hosts!

Feast on their bones!
Feed on their flesh!
Ares!
Adonis!
Astarte!
Prometheus' Rebirth!

Ere constellations were dust!
And thus thou empowered me!
I am legion in company ov seraphs!
At the threshold ov this godless anarchy!
Malediction to all that is Angelic!
Pariah ov collapsing truth!
Crucifixion was not enough!
The alpha ov this mortal whorl!
```

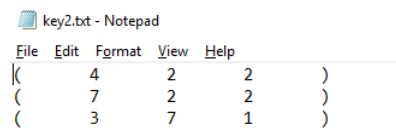
Figura 1: Plaintext

Ciphertext taken:

```
pt22hill.txt - Notepad
File Edit Format View Help
V8.9IIBU8@u;WM+\<%8+2'X0-w[;GNw1``S1vhQ*1 )%sA*OW33)WXc99"C!8+21zpP}C)3W[RLJ(/6{5|
2u~4|TSIR[*]aD+||b{5|2u3bu37>]>'S V2Q/$5nFG*i=zY~8RV?<A~FEE}jTJ~&&GxqcAaXYL'Rs#qe~[
9vNT=J5$%:4xD?bQ/MGgn11"C!u!EF::: b+||1@A/HBym9Da'>67S11B1 +dZ"C!YTNZh?LX$&GxH,Q/<%S
VL'R~>.*v`It@)Y<iV0>yb#XYyoRHAFSXH8E#iV0-w[;GNL'Rs#qU':<P{&hw%:4uz{;<%)oXw1 ^<6UUV}9
{16r!uu:C3iK.:9xS11*nurY7q~tG,-FEE@?.%L0AeHyLSQ[>wH1L'RXXK*|
wwW5a2uqcA&ttG~~R;1Bz"p;BI672)~pQQ_MM07&vBmZ3+2{^+||I?.<P{'':}S VL'R2;;{0sv0xTSI_
%syNrGh^I&i_-oBz"aXY2|0qkNM'i ^GuJQMTg$"{FH7-4_S VI67q~tkm3Q--
9hEsB<3eBG*ari/'==>'7LMdq0kV3?("&b@2|0e~tS VL'R2;;^?.efya-Xi~2"vTwtt'=="C!+99&1s
%:4r@}B89yoRHAF_tLv0x1$u5H[)%s7pfZ3+f=3xW:.|t_23LBfGuu:C3iK.Ai;
```

Figura 2: Plaintext

Key taken:



A screenshot of a Notepad window titled 'key2.txt - Notepad'. The window contains a 3x3 matrix of numbers. The first row is (4, 2, 2), the second row is (7, 2, 2), and the third row is (3, 7, 1). The numbers are enclosed in parentheses and separated by spaces.

File	Edit	Format	View	Help
(4	2	2)
(7	2	2)
(3	7	1)

Figura 3: Key

Program running:

```
C:\Users\James\Documents\ESCOM_SEMESTRE_7\3CM6_CRYPTOGRAPHY\1_Unit\Practices\3_Anal:
|+|+|+| HILL CRYPTANALYSIS |+|+|+|
1. Cryptanalysis
2. Exit
Choose an option: 1
Enter the file name with the plaintext (it may be an absolute path): pt3.txt
Enter the file name with the ciphertext (it may be an absolute path): pt22hill.txt

-/-/-/-/-/-/-/- 1 ATTEMPT -/-/-/-/-/-/-/-
Plaintext sample: C r a w l   w i t
Plaintext sample matrix X ---->
35 82 65
87 76 0
87 73 84
Ciphertext sample: V 8 . 9 I I b U 8
Finding inverse of Matrix X...

-----CALL: find_inverse_matrix()-----
Step One: Determinant = 44
Step Two: Validating determinant gcd(44, 95) = 1

-----CALL: validate_euclid_algorithm()-----
-----RETURN ON SUCCESS: validate_euclid_algorithm()-----
Step Three: Finding inverse of determinant using Extended Euclid Algorithm
```

Figura 4: Program running

```
-----CALL: find_det_inverse()-----
-----RETURN ON SUCCESS: find_det_inverse()-----
Determinant Inverse: 66
Step Four: Transpose Matrix
Step Five: Matrix of Minors
Step Six: Adjugate, Matrix of Cofactors
Step Seven: Applying mod 95 to all entries in the Adjugate Matrix
Step Eight and Final: Multiplying each entry by the inverse of the
Inverse of the matrix:
63 32 0
29 58 16
83 68 79
-----RETURN ON SUCCESS: find_inverse_matrix()-----
Deciphering...
Deciphered
C | C
r | r
a | a
w | w
l | l
|
w | w
i | i
t | t
Key:
4 2 2
7 2 2
3 7 1
```

Figura 5: Program running

Key found:

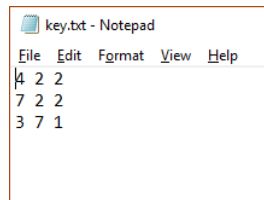


Figura 6: Key found and stored

Deciphered text with that key:

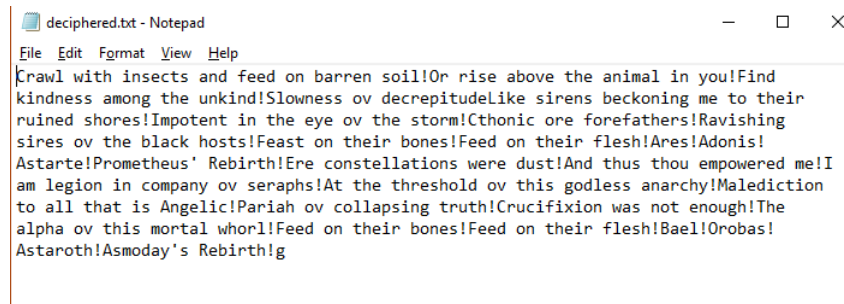


Figura 7: Text deciphered