HILL CIPHER CRYPTANALYSIS

STUDENTS: BASTIDA PRADO JAIME ARMANDO

SOLORIO PAREDES DANIEL

PROFESSOR: DÍAZ SANTIAGO SANDRA

SUBJECT: CRYPTOGRAPHY

GROUP: 3CM6

March 13th 2019

1. Hill Cipher Cryptanalysis

This program is an implementation of the cryptanalysis for Hill cipher considering the set of printable ASCII characters.

1.1. Cryptanalysis

To do the cryptanalysis the program receives a pair of plaintext and ciphertext (also called by the program 'sample'). Then it calculates the inverse of the matrix 'X' formed from the plaintext and multiplies it by the ciphertext 'Y' to obtain the key.

```
119     {
120         printf("Finding K by doing  ->  X^(-1)Y = K\n");
121         for(i = 0; i < 3; i++)
122             for(j = 0; j < 3; j++)
123                 key[i][j] = 0;
124
125         for(i = 0; i < 3; i++)
126             for(j = 0; j < 3; j++)
127             {
128                 for(k = 0; k < 3; k++)
129                 {
130                     key[i][j] += x_inverse[i][k] * y[k][j];
131                 }
132                 key[i][j] = key[i][j] % 95;
133             }
134
135         printf("Proposed key: \n");
136         for(i = 0; i < 3; i++)
137         {
138             for(j = 0; j < 3; j++)
139                 printf("%d ", key[i][j]);
140             printf("\n");
141         }
```

Figura 1: Calculating the key doing $X^{-1}Y = K$

1.2. Testing the Key

After finding the proposed key matrix 'K' the program resolves whether it is the correct one by taking an extract from the ciphertext file. Then deciphers it and compares character by character to the plaintext file. If the characters are exactly the same then the key is correct and is stored in a file called 'key.txt'.

```
//Testing
if((ciphertext_fp2 = fopen(deciphered_fn, "rb")) == NULL)
    printf("|+|ERROR: Can't open: %s. Try again.\n", deciphered_fn);

if((plaintext_fp2 = fopen(plaintext_fn, "rb")) == NULL)
    printf("|+|ERROR: Can't open: %s. Try again.\n", plaintext_fn);

valid_determinant = true;
i = 0;
while(i < 9)
{
    decipheredtext[i] = getc(ciphertext_fp2);
    plaintext_test[i] = getc(plaintext_fp2);
    printf("%c | %c \n", decipheredtext[i], plaintext_test[i]);
    if(decipheredtext[i] != plaintext_test[i])
    {
        printf("|+|ERROR: Key found is not the right one. Trying again...\n\n");
        //exit(EXIT_FAILURE);
        no_attempts++;
        valid_determinant = false;
        break;
    }
    else
        i++;
}
```

Figura 2: Testing whether the key is correct.

If the found key is not correct then we are return to take another sample (i.e. take the next nine characters) of plaintext and ciphertext and begin the whole process again.

```
67                  if(no_attempts != 0)
68                      low += 9;
69
70                  printf("\n-/-/-/-/-/-/-/-/-/ %d ATTEMPT /-/-/-
71                  //Moving offset in plaintext and ciphertext fi
72                  move_offset(&plaintext_fp, low);
73                  move_offset(&ciphertext_fp, low);
74
75                  //Reading a sample of 9 chars from plaintext a
76                  plaintext = read_sample(&plaintext_fp, 9L);
77                  ciphertext = read_sample(&ciphertext_fp, 9L);
78
```

Figura 3: Taking another sample

1.3. Pairs of plaintext and ciphertext tested

Plaintext 1:

```
Children:

Elohim! - I shall not forgive!
Adonai! - I shall not forgive!
Living God! - I shall not the forgive!
Jesus Christ! - I forgive thee not!

Enthronef thyself, O Archuman
O how thou shineth in the realm above
As planetsc rumble when thou descended upon this globe
To walk thisk Earth like a shimmering god

Lets it be forever heard
We losta our Eden to own the world
Let itn be forever known
We lost ourd battle to win the wara

Come all ye, Wolves ov Siberia
We hail the flame, we hail the ice
Beyond bosom, beyond materia
We reject! We fucking deny!
```

Figura 4: Plaintext 1

Ciphertext 1:

```
M-MtHA$D?

KagZ_NpmNT"5qF0l 3FG1ZreI^ktL(
+m:xxrpmNT"5qF0l 3FG1ZreI^ktL(
8X1\7-5W7)v*~1pfJ/[C|yKwVQND3 J=I'h|
" ah(Mr$j}8Xr*ev{U.KxmL/"<.^QI[fSFG1

`NxV;!4\t#"~'KFn$dT|U\JC1\nQz~
Yw#\:`_}7qVdWI'(0(E>{^QIp_~Up7F0S=)P
#rZr<b`-E+V1GBTON(aPyw-}^QI1,,gb]^#s501>fHEZ4qCcec Lyx
U2K[B,txxqCc^``;1P/:`aGXDY|fJ/RjF5k,e:M-C

^hR_71-as5Jwsx}?coh?DC_u
(7$x zghh4-Lf}4rF VkX04^^QIaPy^=*
<)Tw& ^d>r:'J=I!!rA{S=dz
u+i*=Cu@-4-L)Tfb*sEN;VkXCgE^QIaPyLB,

hegDY|1 3<D#sh[jhZMqd+l`cn`Q^[
(7$G yTzwD3 6"X9R1OINt8"$Sf}<AfrM
E1\Co`)TfMa.J*P%_S7r<L[En&2
6~.p_~",Wn|X2'eHM9=\Ve:Mvqb
```

Figura 5: Ciphertext 1

Plaintext 2:

```
There's a serpent coiling around my neck
The adoring crescent moon in blazing night
The holy river Ganga flowing through my muddled hair
In the ancient times before I learned ov who I am

If I am a missing link between the pig and the divine
I shall cast the pearls before the swine

I am no good shepherd on an ox
But a solitude ov the loneliest star
Like a thousand shrines subsumed into the void
Like a dead space in between the suns
```

Figura 6: Plaintext 2

Ciphertext 2:

```
'kipyx/Z2 V"?U]Em^yF`bXOMlbcb0=?DJqv9/e
jW~Roj//e_uhtCt'M)f7&"_:orh~{!P1c?CvJ(oIm:
$yZ_Yq~SGd`H\nTTee_L~VVg_K=n$=3VU$- Z>j_T&Dul[Jn5Yw
Ry!X~Y|?:^!%8Q%IuATN)Lr30fsc0q[%'U|bVGf07\yz[yZ*A<T

k559:{>cJ2.4SiVn$=bXO`~SaIzBW5H6b*[yK[Q{9&H6bJXm>]w
?XKw?%EMrb'ch6J6;HNq)HvdLr30fsc0q6;HO+4%Ef

9:{;~W)2H)z+w?%("5snLe5T^TUjg^
b\#ppfIv#|rh'EJs*u6;HQh\!Injj*,]@_6&
[@mRojH6bc0,{9&w?%SO7[TEGmjiXu$|h\1u&MU|?:yYs
e3/Ej.T^};ITBA-cU!bkbG1*mr%)"16;HtZ2
```

Figura 7: Ciphertext 2

Plaintext 3:

```
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!
```

Figura 8: Plaintext 3

Ciphertext 3:

```
bwaN4)hthd<zIvj/;9%LI6Xb2:=T<Sx{4Vx^'*,*3%
\/:lI:j X#_dg51@@X%LI2AX`XF,xel5
5KrJ:bS#|e~'r!]f| ~eau2)=sRS#|
rI~;=B>/G;E@y%iencoCd$>-
\N70JB_9t?LDDw+hn:&Ji?Q}Ol#Ypo9;"v'MD0V1CO/.(9y4
/$|785.f{:e0@@XY&Alu{oo\u2)[w`38{
6H$a/.ng6kxe1 BN-(@@X,uI
97E!z9&Ji[cqa;R;E@Ypoq+/~UIpDy%#]

zX"S6~] vw7eC1ud'D>Zg
zX"2:=T<SYpo9;"MU,%^m
-?09y4
!q8!(E
}LiS3@Z4%
Ak=W%mMn)s#bcYc<>t
```

Figura 9: Ciphertext 3

1.4. EXERCISES

Jaime

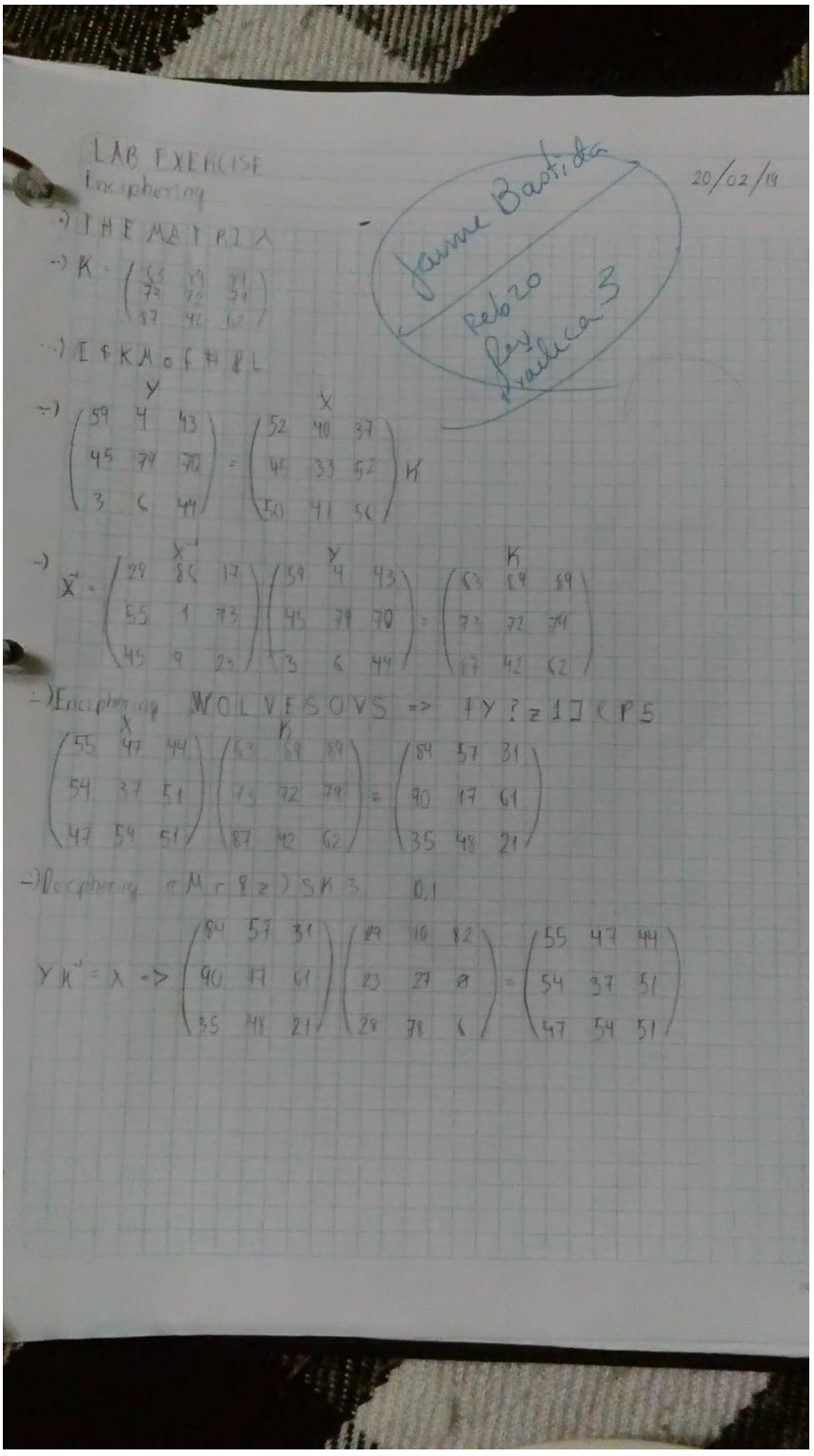

Figura 10: Exercise

Daniel

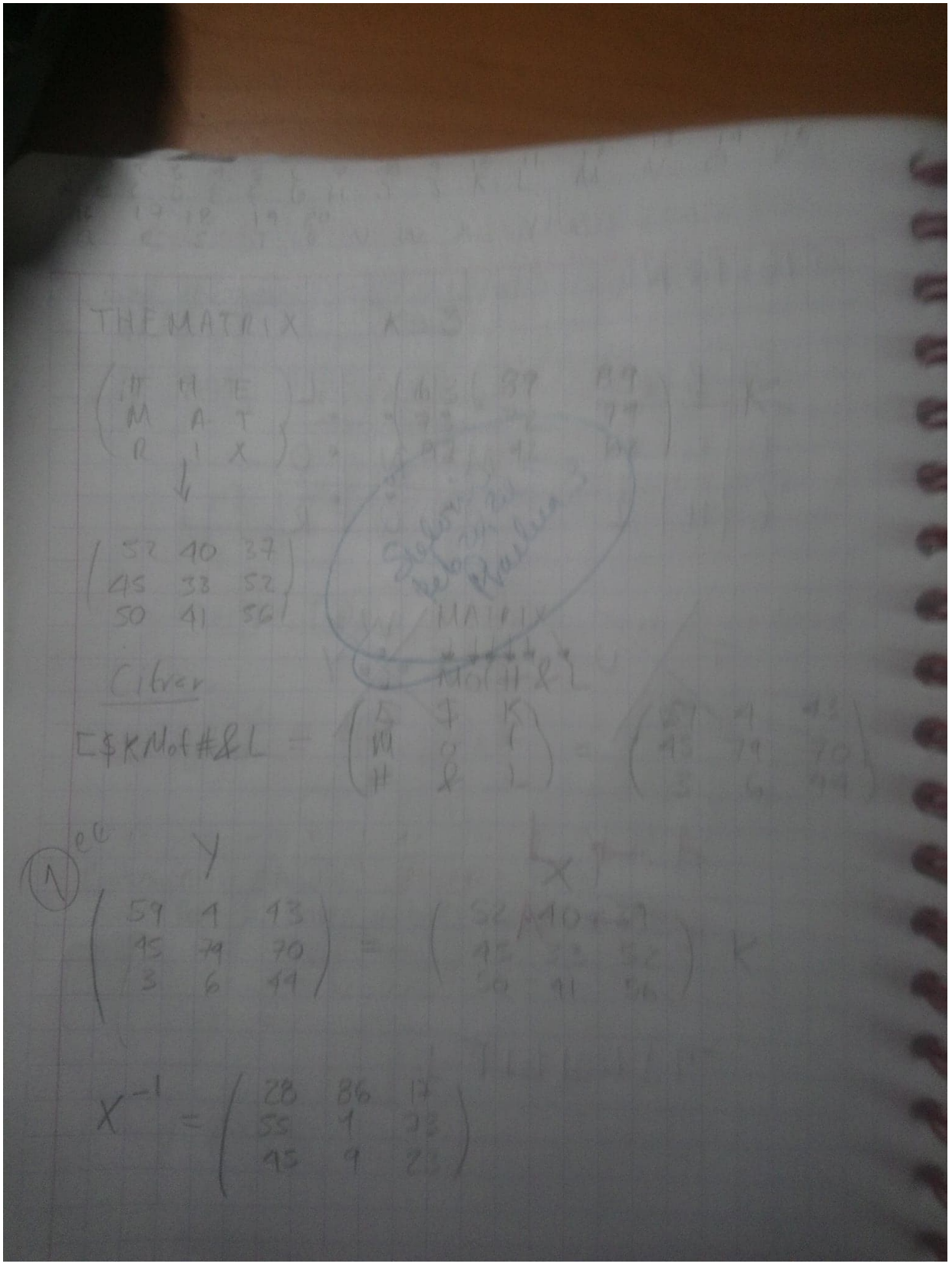

Figura 11: Exercise