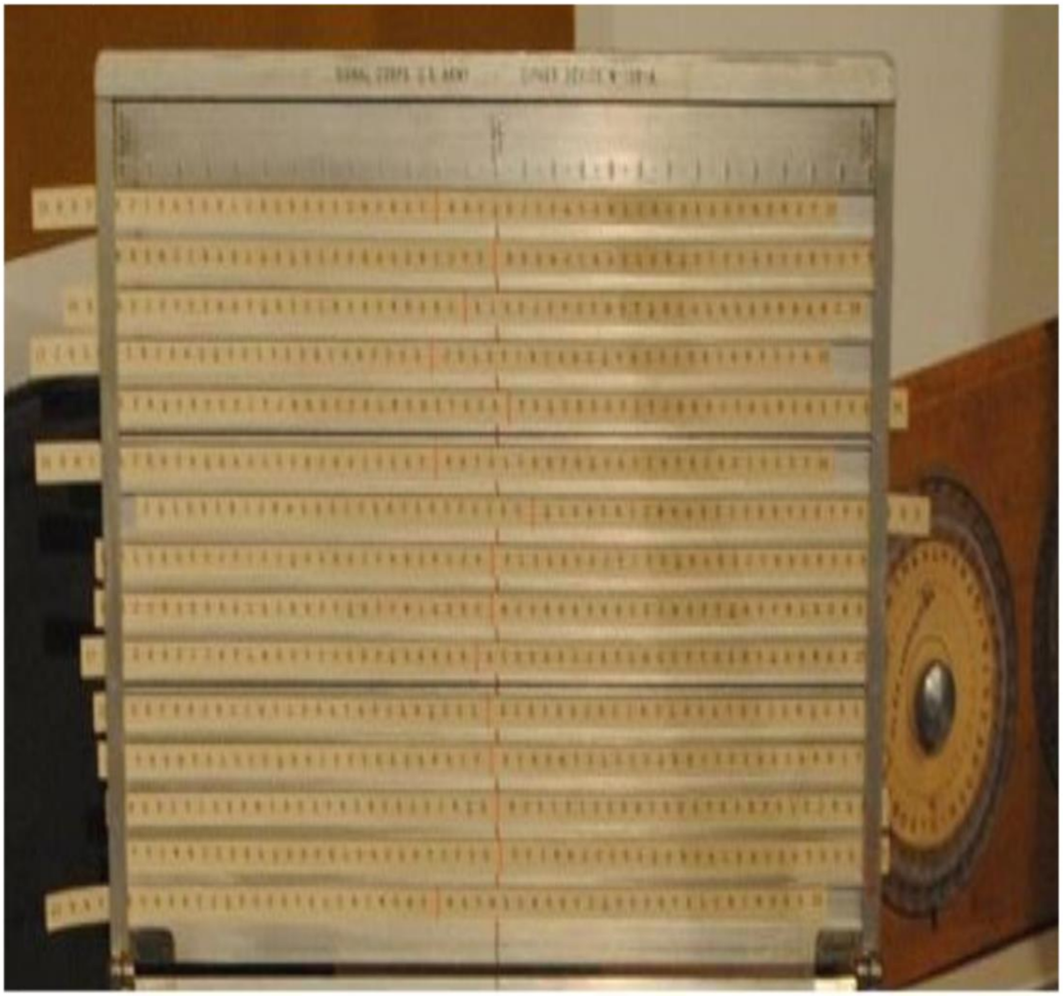


Cryptanalysis Project

M-138 CIPHER

Ketki Kulkarni & Pratikshya Mishra | CS265: Cryptography and network security | March 19, 2016

Pratikshya Mishra
Pratikshya.Mishra@sjsu.edu

Ketki Kulkarni
Ketki.Kulkarni@sjsu.edu

Table of Contents

1. Introduction

Strip Ciphers played an important role before and during World War II due to the shortage of other cipher systems. M-138 otherwise known as CSP-845 was developed in the year 1916 by Colonel Parker Hitt. The purpose of M-138 was to provide cipher security at low cost. Moreover, M-138 was easy to carry and operate.

2. Challenge Description

The challenge uses a fictitious model of M-138, which consists of a total of 100 strips which are different from those of M-138 strips. On each strips there are 26 letters in a random order. For encryption, up to 25 strips are chosen from the strip set and placed in the frame. The strips arranged in such a way that the strip number and the offset is the key. Offset is the difference between the position of the ciphertext and plaintext. For e.g. to encrypt CRYPTO, the key is (66, 11, 52, 55, 04, 90/11). [1]

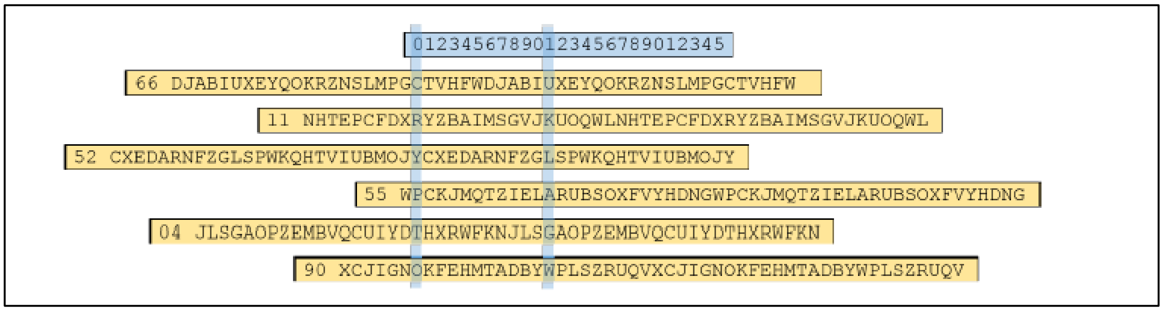

01234567890123456789012345
66 DJABIUXEYQOKRZNSLMPGCTVHFWDJABIUXEYQOKRZNSLMPGCTVHFW
11 NHTEPCFDXRYZBAIMSGVJKUOQWLNHTEPCFDXRYZBAIMSGVJKUOQWL
52 CXEDARNFZGLSPWKQHTVIUBMOJYCXEDARNFZGLSPWKQHTVIUBMOJY
55 WPCKJMQTZIELARUBSOXFVYHDNGWPCKJMQTZIELARUBSOXFVYHDNG
04 JLSGAOPZEMBVQCUIYDTHXRWFKNJLSGAOPZEMBVQCUIYDTHXRWFKN
90 XCJIGNOKFEHMTADBYWPLSZRUQVXCJIGNOKFEHMTADBYWPLSZRUQV

Fig 1: Example of the M-138

The number of strips used cannot exceed 25 (only 25 strips fit into the frame) and no strip can be used more than once. This means that a key like (20, 12, 20. . .) cannot be used. If the plaintext is longer than 25 letters, it must be divided into blocks of 25 letters. Each of the blocks is encrypted in the same way as in the smaller example above. The key remains the same for all blocks of the plaintext.

Given Information

- The plaintext and ciphertext consists of 100 letters.
- The 100 strips used for the challenge. Each strip has 26 letters arranged randomly.
- The first 48 letters of the plaintext is known.
  Plaintext = TWO THINGS ARE INFINITE THE UNIVERSE AND HUMAN

STUPIDITY.

Ciphertext = BBQGF HSDXN FKLXR REYYP ADREW TFRJG JDCBG DZFXI NXMWY LHTGP AXHOL THXPR CTTAD FWOJY XAEYR NKRXR XDKHS FDUVP XQGWM KMYKZ.

- Block Size is 25.

3. Problem Statement

To find the last 52 letters of the plaintext.

4. Analysis

Steps for Analysis:

1. Reading and storing the data of the 100 strips from the given file.

- We used a structure having two members one for storing the strip number and the other for storing the strip characters. The given file had strip consisting of 26 letters arranged randomly.
- We used an array of struct of size 100 to store the strips read from file.

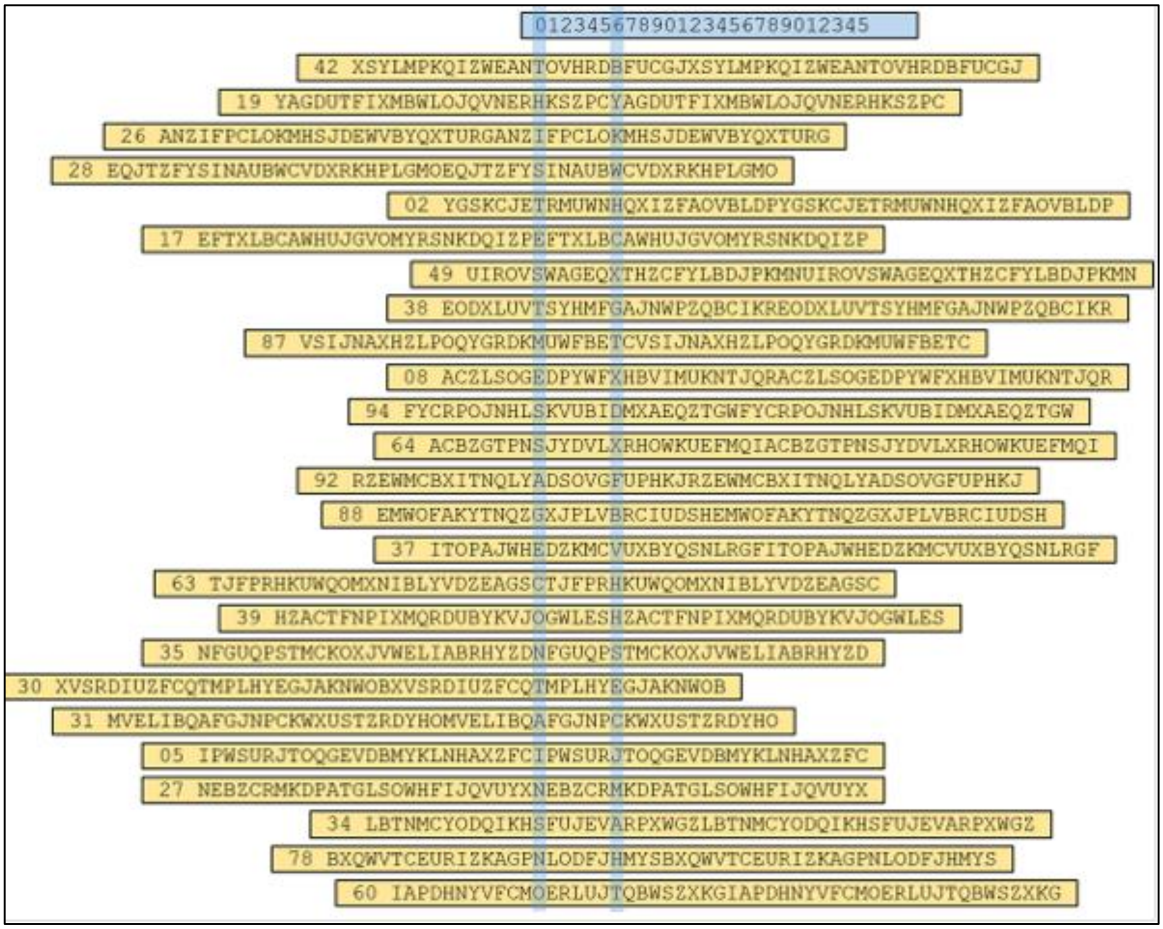
2. Finding the offset.

After having the strips we had to find the offset. For finding the offset we can use the following:

- The first 48 character of the plaintext.
- The first 48 character of the ciphertext.

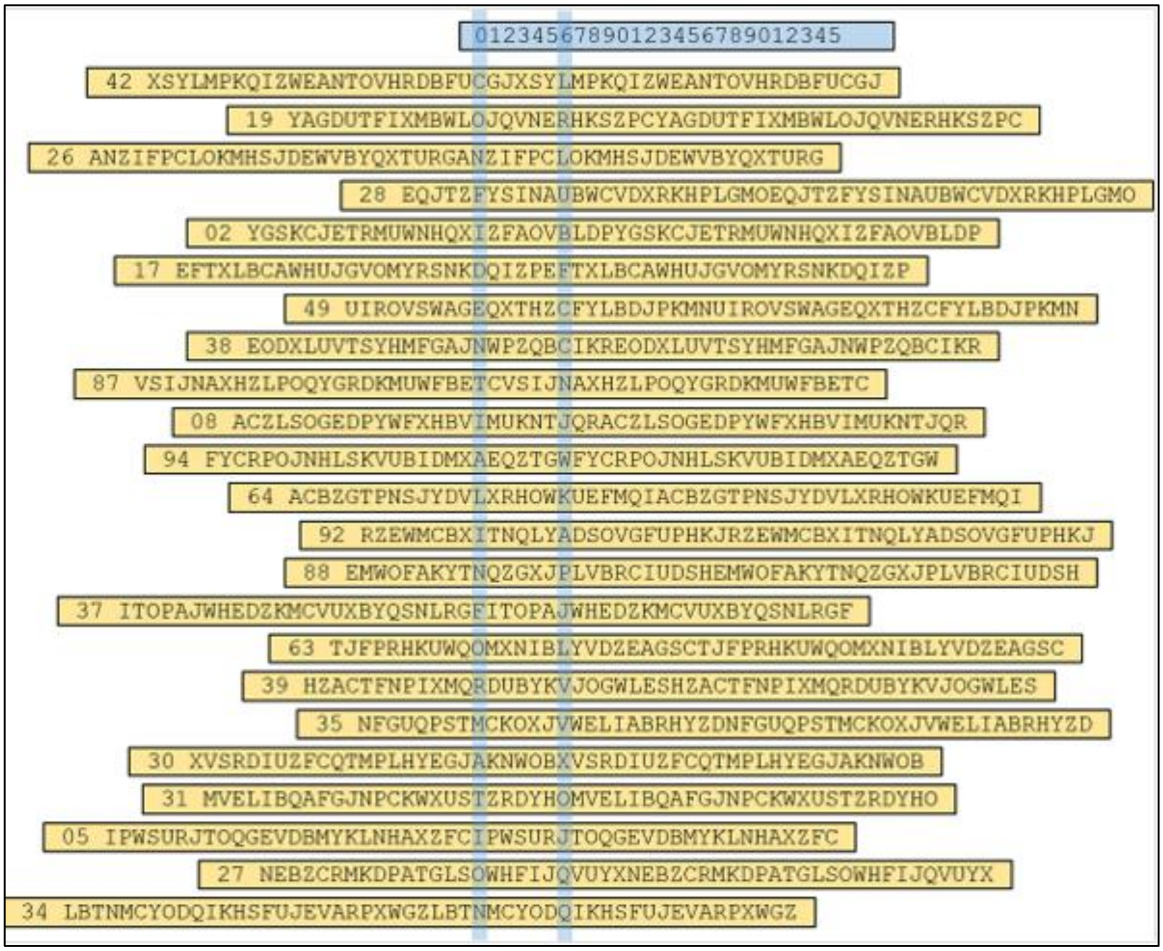
But since there are 48 plaintext characters. So we can use the Strips from 0-22 are same as 25-47 as we cannot divide it into two blocks of 25 characters (since the frame can have 25 strips). We will find the offset using these two blocks of 23 letters of ciphertext and plaintext.

Strip of the place at 0 = 25, at 1 = 26, …, at 22 = 47. So, the distance between the character of plaintext and the corresponding character of ciphertext is equal. For e.g. for the plaintext = "THIS TEST MESSAGE CONTAINS NO CONFIDENTIA ", has 48 letters. The key is (42, 19, 26, 28, 02, 17, 49, 38, 87, 08, 94, 64, 92, 88, 37, 63, 39, 35, 30, 31, 05, 27, 34, 78, 60 / 6). The strip has 52 characters i.e. two set of the 26 letters arranged randomly.[1]



```
01234567890123456789012345
42 XSYLMPKQIZWEANTOVHRDBFUCGJXSYLMPKQIZWEANTOVHRDBFUCGJ
19 YAGDUTFIXMBWLOJQVNERHKSZPCYAGDUTFIXMBWLOJQVNERHKSZPC
26 ANZIFPCLOKMHSJDEWVBYQXTURGANZIFPCLOKMHSJDEWVBYQXTURG
28 EQJTZFYSINAUBWCVDXRKHPLGMOEQJTZFYSINAUBWCVDXRKHPLGMO
02 YGSKCJETRMUWNHQXIZFAOVBLDPYGSKCJETRMUWNHQXIZFAOVBLDP
17 EFTXLBCAWHUJGVOMYRSNKDQIZPEFTXLBCAWHUJGVOMYRSNKDQIZP
49 UIROVSWAGEQXTHZCFYLBDJPKMNUIROVSWAGEQXTHZCFYLBDJPKMN
38 EODXLUVTSYHMFGAJNWPZQBCIKREODXLUVTSYHMFGAJNWPZQBCIKR
87 VSIJNAXHZLPOQYGRDKMUWFBETCVSIJNAXHZLPOQYGRDKMUWFBETC
08 ACZLSOGEDPYWFXHBVIMUKNTJQRACZLSOGEDPYWFXHBVIMUKNTJQR
94 FYCRPOJNHLSKVUBIDMXAEQZTGWFYCRPOJNHLSKVUBIDMXAEQZTGW
64 ACBZGTPNSJYDVLXRHOWKUEFMQIACBZGTPNSJYDVLXRHOWKUEFMQI
92 RZEWMCBXITNQLYADSOVGFUPHKJRZEWMCBXITNQLYADSOVGFUPHKJ
88 EMWOFAKYTNQZGXJPLVBRCIUDSHEMWOFAKYTNQZGXJPLVBRCIUDSH
37 ITOPAJWHEDZKMCVUXBYQSNLRGFITOPAJWHEDZKMCVUXBYQSNLRGF
63 TJFPRHKUWQOMXNIBLYVDZEAGSCTJFPRHKUWQOMXNIBLYVDZEAGSC
39 HZACTFNPIXMQRDUBYKVJOGWLESHZACTFNPIXMQRDUBYKVJOGWLES
35 NFGUQPSTMCKOXJVWELIABRHYZDNFGUQPSTMCKOXJVWELIABRHYZD
30 XVSRDIUZFCQTMPLHYEGJAKNWOBXVSRDIUZFCQTMPLHYEGJAKNWOB
31 MVELIBQAFGJNPCKWXUSTZRDYHOMVELIBQAFGJNPCKWXUSTZRDYHO
05 IPWSURJTOQGEVDBMYKLNHAXZFCIPWSURJTOQGEVDBMYKLNHAXZFC
27 NEBZCRMKDPATGLSOWHFIJQVUYXNEBZCRMKDPATGLSOWHFIJQVUYX
34 LBTNMCYODQIKHSFUJEVARPXWGZLBTNMCYODQIKHSFUJEVARPXWGZ
78 BXQWVTCEURIZKAGPNLODFJHMYSBXQWVTCEURIZKAGPNLODFJHMYS
60 IAPDHNYVFCMOERLUJTQBWSZXKGIAPDHNYVFCMOERLUJTQBWSZXKG
```

Fig 2a: Example of blocks in M-138



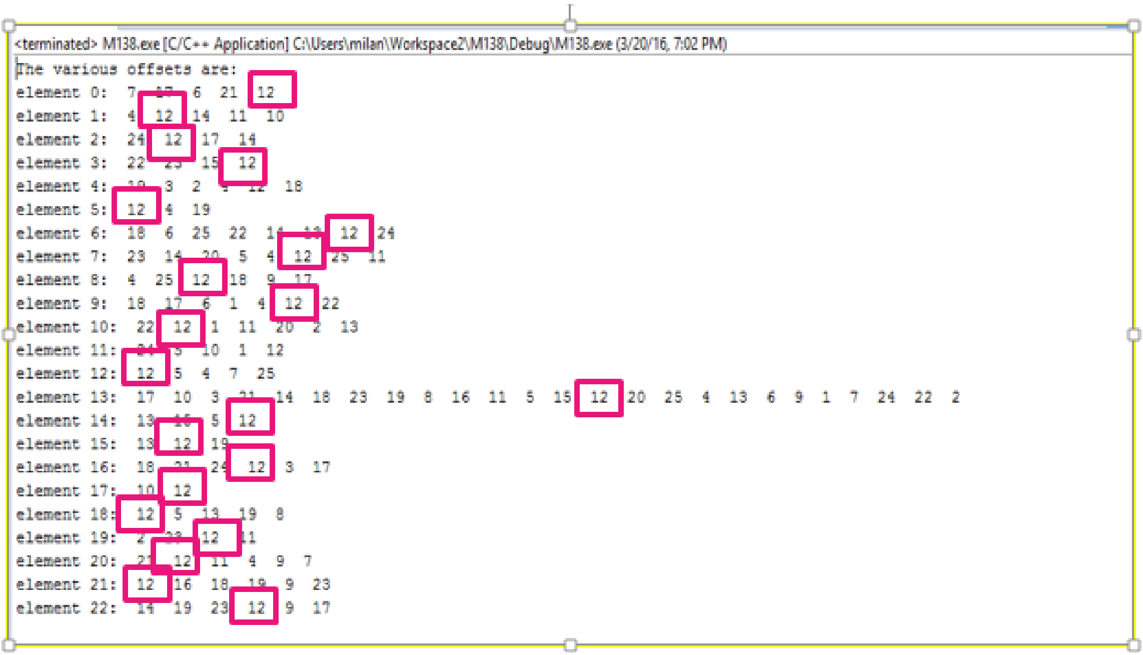
```
01234567890123456789012345
42 XSYLMPKQIZWEANTOVHRDBFUCGJXSYLMPKQIZWEANTOVHRDBFUCGJ
19 YAGDUTFIXMBWLOJQVNERHKSZPCYAGDUTFIXMBWLOJQVNERHKSZPC
26 ANZIFPCLOKMHSJDEWVBYQXTURGANZIFPCLOKMHSJDEWVBYQXTURG
28 EQJTZFYSINAUBWCVDXRKHPLGMOEQJTZFYSINAUBWCVDXRKHPLGMO
02 YGSKCJETRMUWNHQXIZFAOVBLDPYGSKCJETRMUWNHQXIZFAOVBLDP
17 EFTXLBCAWHUJGVOMYRSNKDQIZPEFTXLBCAWHUJGVOMYRSNKDQIZP
49 UIROVSWAGEQXTHZCFYLBDJPKMNUIROVSWAGEQXTHZCFYLBDJPKMN
38 EODXLUVTSYHMFGAJNWPZQBCIKREODXLUVTSYHMFGAJNWPZQBCIKR
87 VSIJNAXHZLPOQYGRDKMUWFBETCVSIJNAXHZLPOQYGRDKMUWFBETC
08 ACZLSOGEDPYWFXHBVIMUKNTJQRACZLSOGEDPYWFXHBVIMUKNTJQR
94 FYCRPOJNHLSKVUBIDMXAEQZTGWFYCRPOJNHLSKVUBIDMXAEQZTGW
64 ACBZGTPNSJYDVLXRHOWKUEFMQIACBZGTPNSJYDVLXRHOWKUEFMQI
92 RZEWMCBXITNQLYADSOVGFUPHKJRZEWMCBXITNQLYADSOVGFUPHKJ
88 EMWOFAKYTNQZGXJPLVBRCIUDSHEMWOFAKYTNQZGXJPLVBRCIUDSH
37 ITOPAJWHEDZKMCVUXBYQSNLRGFITOPAJWHEDZKMCVUXBYQSNLRGF
63 TJFPRHKUWQOMXNIBLYVDZEAGSCTJFPRHKUWQOMXNIBLYVDZEAGSC
39 HZACTFNPIXMQRDUBYKVJOGWLESHZACTFNPIXMQRDUBYKVJOGWLES
35 NFGUQPSTMCKOXJVWELIABRHYZDNFGUQPSTMCKOXJVWELIABRHYZD
30 XVSRDIUZFCQTMPLHYEGJAKNWOBXVSRDIUZFCQTMPLHYEGJAKNWOB
31 MVELIBQAFGJNPCKWXUSTZRDYHOMVELIBQAFGJNPCKWXUSTZRDYHO
05 IPWSURJTOQGEVDBMYKLNHAXZFCIPWSURJTOQGEVDBMYKLNHAXZFC
27 NEBZCRMKDPATGLSOWHFIJQVUYXNEBZCRMKDPATGLSOWHFIJQVUYX
34 LBTNMCYODQIKHSFUJEVARPXWGZLBTNMCYODQIKHSFUJEVARPXWGZ
```

Fig 2b: Example of blocks in M-138

We represent the ciphertext characters a C and plaintext as P.

We use a 2d array to store all the possible offset such that C0-P0 == C25-P25, C1 – P1 = C26 – P26, C2 –P2 = C27-P27.....C23 –P38 against all the strip 0-25. The given strips has 26 character arranged randomly.

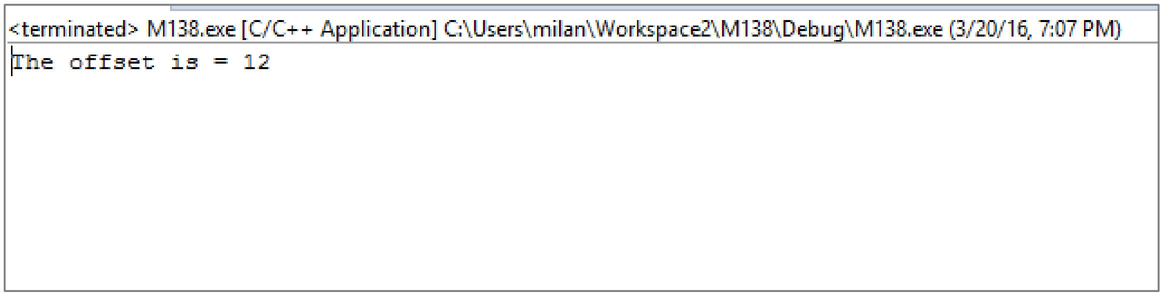
So for each 23 element we iterate for all the 100 strips and check if the difference between C_i and P_i is same as C_{i+25} and P_{i+25} by iterating through the 26 letters on the strip. The following is the output of all the possible offsets.



```
<terminated> M138.exe [C/C++ Application] C:\Users\milan\Workspace2\M138\Debug\M138.exe (3/20/16, 7:02 PM)
The various offsets are:
element 0:  7  17  6  21  12
element 1:  4  12  14  11  10
element 2:  24  12  17  14
element 3:  22  23  15  12
element 4:  10  3  2  4  12  18
element 5:  12  4  19
element 6:  18  6  25  22  14  13  12  24
element 7:  23  14  20  5  4  12  25  11
element 8:  4  25  12  18  9  17
element 9:  18  17  6  1  4  12  22
element 10:  22  12  1  11  20  2  13
element 11:  24  5  10  1  12
element 12:  12  5  4  7  25
element 13:  17  10  3  21  14  18  23  19  8  16  11  5  15  12  20  25  4  13  6  9  1  7  24  22  2
element 14:  13  16  5  12
element 15:  13  12  19
element 16:  18  21  24  12  3  17
element 17:  10  12
element 18:  12  5  13  19  8
element 19:  2  23  12  11
element 20:  21  12  11  4  9  7
element 21:  12  16  18  19  9  23
element 22:  14  19  23  12  9  17
```

Fig 3: Output of all possible offset

Then we find the common offset i.e. the final offset will have a count of 23 (after removing the duplicates).This offset is the key.



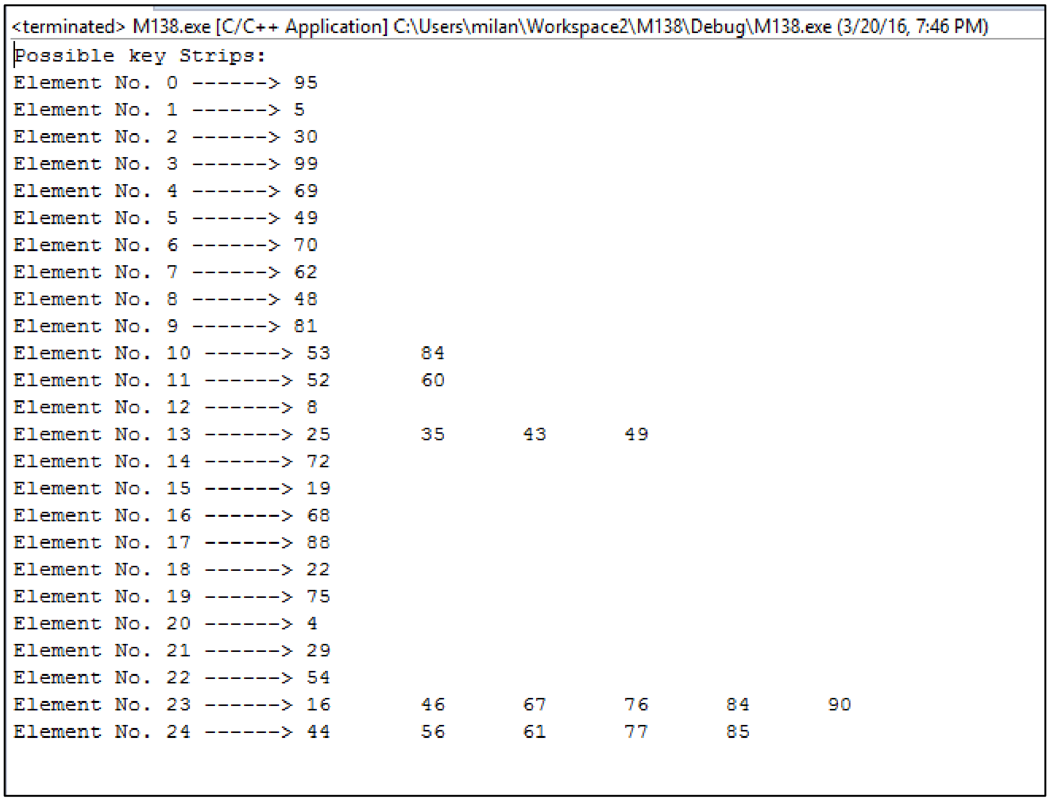
```
<terminated> M138.exe [C/C++ Application] C:\Users\milan\Workspace2\M138\Debug\M138.exe (3/20/16, 7:07 PM)
The offset is = 12
```

Fig 4: Output showing the final offset

3. Finding the Key strips.

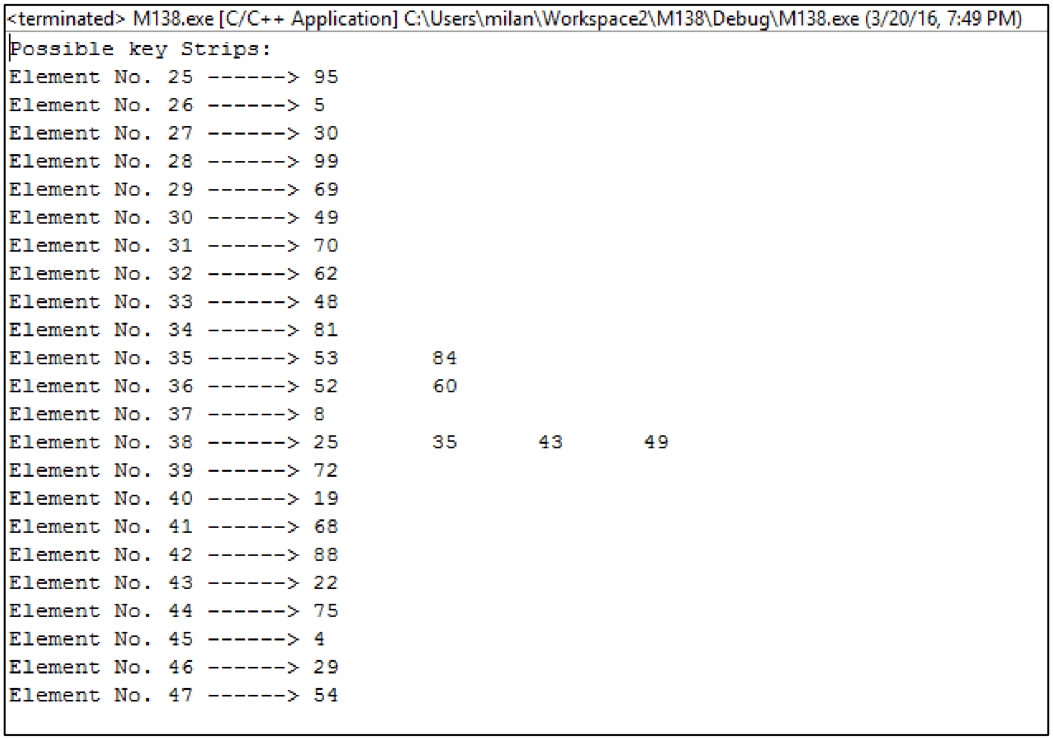
After finding the offset now we had to find the possible strips used for the block of 23 elements. We store all the strips for each character in block 1 and block 2 such that position of cipher text character minus offset gives position of respective plain text character. Then we select the strips that are common in both the blocks.

Then we find the strips for the last two characters of the first block i.e. for the character C24 and C25 by finding the strips such that position of the cipher text character minus offset gives position of respective plain text character.



```
<terminated> M138.exe [C/C++ Application] C:\Users\milan\Workspace2\M138\Debug\M138.exe (3/20/16, 7:46 PM)
Possible key Strips:
Element No. 0 ------> 95
Element No. 1 ------> 5
Element No. 2 ------> 30
Element No. 3 ------> 99
Element No. 4 ------> 69
Element No. 5 ------> 49
Element No. 6 ------> 70
Element No. 7 ------> 62
Element No. 8 ------> 48
Element No. 9 ------> 81
Element No. 10 ------> 53       84
Element No. 11 ------> 52       60
Element No. 12 ------> 8
Element No. 13 ------> 25       35      43      49
Element No. 14 ------> 72
Element No. 15 ------> 19
Element No. 16 ------> 68
Element No. 17 ------> 88
Element No. 18 ------> 22
Element No. 19 ------> 75
Element No. 20 ------> 4
Element No. 21 ------> 29
Element No. 22 ------> 54
Element No. 23 ------> 16       46      67      76      84      90
Element No. 24 ------> 44       56      61      77      85
```

Fig 5: Output of the possible Key Strips for first 25 elements



```
<terminated> M138.exe [C/C++ Application] C:\Users\milan\Workspace2\M138\Debug\M138.exe (3/20/16, 7:49 PM)
Possible key Strips:
Element No. 25 ------> 95
Element No. 26 ------> 5
Element No. 27 ------> 30
Element No. 28 ------> 99
Element No. 29 ------> 69
Element No. 30 ------> 49
Element No. 31 ------> 70
Element No. 32 ------> 62
Element No. 33 ------> 48
Element No. 34 ------> 81
Element No. 35 ------> 53       84
Element No. 36 ------> 52       60
Element No. 37 ------> 8
Element No. 38 ------> 25       35      43      49
Element No. 39 ------> 72
Element No. 40 ------> 19
Element No. 41 ------> 68
Element No. 42 ------> 88
Element No. 43 ------> 22
Element No. 44 ------> 75
Element No. 45 ------> 4
Element No. 46 ------> 29
Element No. 47 ------> 54
```

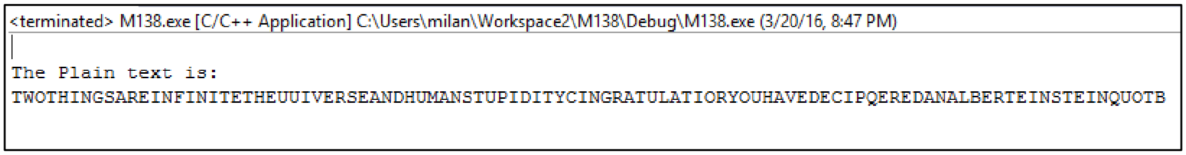
Fig 6: Output of the possible Key Strips for second 23 elements

We got the key strip to be

95, 5, 30, 99, 69, 49, 70, 62, 48, 81, (53/84), (52/60), 8, (25/35/43/49), 72, 19, 68, 88, 22.75, 4, 29, 54, (16/46/67/76/84/90), (44/56/61/77/85)

4. Decrypting the ciphertext.

Using the possible key strips and the offset we get the plaintext by finding the position on the key strip of the plaintext by subtracting the offset from the position of the ciphertext.



```
<terminated> M138.exe [C/C++ Application] C:\Users\milan\Workspace2\M138\Debug\M138.exe (3/20/16, 8:47 PM)

The Plain text is:
TWOTHINGSAREINFINITETHEUUIVERSEANDHUMANSTUPIDITYCINGRATULATIORYOUHAVEDECIPQEREDANALBERTEINSTEINQUOTB
```

Fig 7: Output of the plaintext

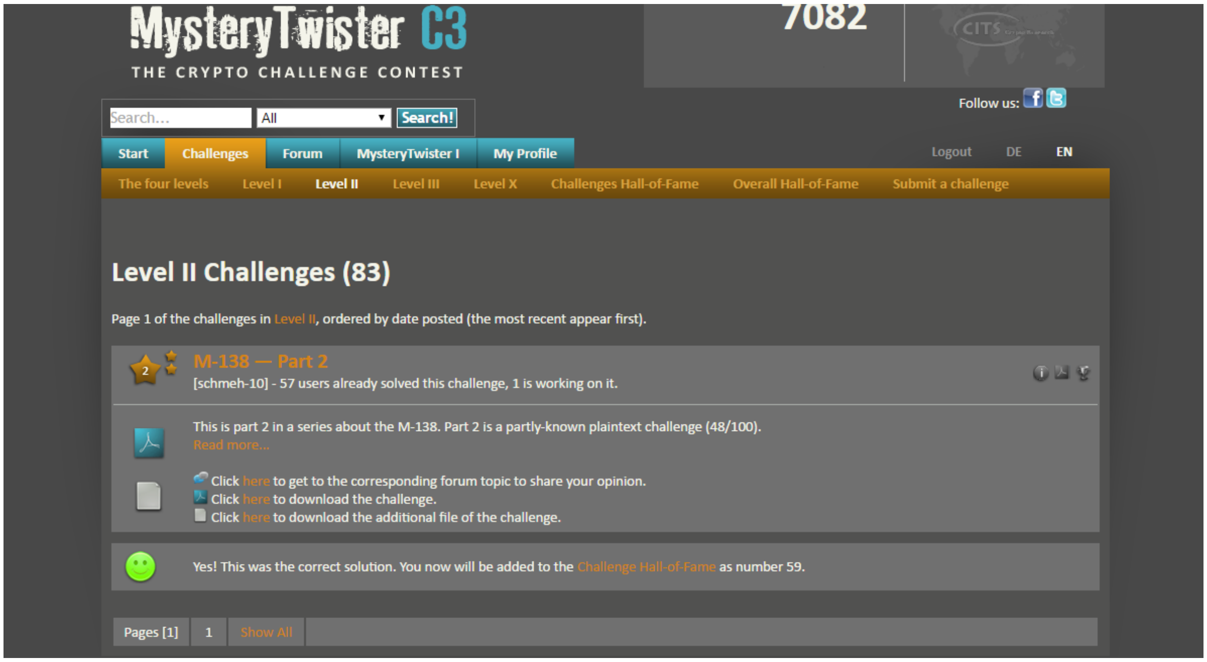
We deduced the output to be:

"TWOTHINGSAREINFINITETHEUNIVERSEANDHUMANSTUPIDITYCONGRATULATIONYOUHAVEDECIPHEREDANALBERTEINSTEINQUOTE"

And the last 52 characters are

"CONGRATULATIONYOUHAVEDECIPHEREDANALBERTEINSTEINQUOTE"

5. Uploaded the result in MysteryTwister challenge.



Level II Challenges (83)

Page 1 of the challenges in Level II, ordered by date posted (the most recent appear first).

M-138 — Part 2

[schmeh-10] - 57 users already solved this challenge, 1 is working on it.

This is part 2 in a series about the M-138. Part 2 is a partly-known plaintext challenge (48/100).
Read more...

Click here to get to the corresponding forum topic to share your opinion.
Click here to download the challenge.
Click here to download the additional file of the challenge.

Yes! This was the correct solution. You now will be added to the Challenge Hall-of-Fame as number 59.

Fig 8: Result after submission

5. Challenges

We got the wrong offset (offset =5) in the first implementation as we did not remove duplicate vales of the offset.

We had a lot of common strip for the last 2 strips in the block and got different plaintext for different combination of the strips and were not able to get the exact plaintext.

6. Bibliography

[1] http://scienceblogs.de/klausis-krypto-kolumne/m-138-challenge/

[2] http://maritime.org/tech/csp845.htm

[3] https://en.wikipedia.org/wiki/Jefferson_disk

[4] https://www.mysterytwisterc3.org/en/challenges/level-i?controller=downloader&task=download&file=mtc3-schmeh-09-M138-01-en.pdf

[5] https://www.mysterytwisterc3.org/en/challenges/level-ii?controller=downloader&task=download&file=mtc3-schmeh-10-M138-02-en.pdf