Title: BCR CODE (BOOK-CAESAR-RSA)

Author: George Theofanidis August 2012; update April 2015

Abstract:

This project required us to select any one of the crypto challenges on the website www.mysterytwisterc3.org from level 2 and above. While we as a team were looking for challenges to be taken, we came this interesting challenge which made use of 3 different ciphers in it. We thought of it as an opportunity to deep dive into three different ciphers and thus, we selected the BCR CODE challenge for our Crypto project. We have collaborated on the various logical, technical and documentation aspects of the challenge as a team and here is a report of our work.

Introduction:

BCR Code project is a crypto challenge, the aim of which is to help pirates Alice and Bob in finding the treasure location using a treasure map and encrypted instructions. The treasure map has points A,B,C,D,E marked on it, which are potential starting points of the hunt. In this cryptosystem, location of the treasure is a secret and information about the location has been encrypted using three staged cascade BCR cipher : Book-Caeser-RSA cipher

Study of Cryptosystem:

BCR cipher is a three-staged cipher, the first stage of which is an altered book cipher(B). The second one is Caesar cipher(C) and the last one is RSA(R) cipher. Output of one cipher acts as an input to other cipher.

1. Book cipher

A book cipher uses a large piece of text i.e the code book to encode a secret message. Without the key (the piece of text) it is very difficult to decrypt the secret message

2. Caesar cipher

Caesar cipher is a type of substitution cipher in which each letter or digit in the plaintext is shifted a certain number of places up/down or left/right.

3. RSA cipher

RSA cipher is an asymmetric key cipher with a public and a private key used. It is based on finding two prime factors of the number and using them as the key to encrypt the plaintext. It is an np-hard problem.

Design of Cryptosystem:

We have incorporated following three classes to design the BCR code cryptosystem:

a) Book Class

This class is responsible for decoding given book text for BCR challenge.

Challenge Book Text:

SIERRA-ZERO-JULIET-SIX-YANKEE-ONE-ROMEO-PAPPA-EIGHT-KILO-FIVE-UNIFORM-XRAY-XXX-BRAVO-VICTOR-TWO-FOUR-TANGO-MIKE-OSCAR-HOTEL-DELTA-QUEBECK-FOXTROT-ALPHA-YYY-LIMA-INDIA-THREE-WHISKEY-NOVEMBER-ECHO-CHARLIE-GOLF-ZULU

After analyzing the text, we know that words like “ZERO”, “ONE” or “TWO” have obvious substitutions corresponding to digits 0,1,2 and so on. The words represent the first letter as in the NATO phonetic alphabet, i.e. “SIERRA” represents “S”, “JULIET” represents “J” and so on. After applying these substitutions to book text, we get the output of this cipher as,

Output after using given Codebook:

S-0-J-6-Y-1-R-P-8-K-5-U-X-**XXX**-B-V-2-4-T-M-O-H-D-Q-F-A-**YYY**-L-I-3-W-N-E-C-G-Z

In given book text, substitutions for unknowns XXX and YYY need to be determined. After thorough analysis of above decoded text, it can be concluded that all alphabets A to Z are present. It also contains digits in range 0-9 except the fact that digits **“7”** & “**9”** are missing. This is the link to our unknowns XXX and YYY.

Now we have two possibilities,
[XXX, YYY] = [7,9]
[XXX, YYY] = [9,7]
After applying these two possibilities to decoded text, we get two possible decoding:

1st possible decoding:

S-0-J-6-Y-1-R-P-8-K-5-U-X-**7**-B-V-2-4-T-M-O-H-D-Q-F-A-**9**-L-I-3-W-N-E-C-G-Z

2nd possible decoding:

S-0-J-6-Y-1-R-P-8-K-5-U-X-**9**-B-V-2-4-T-M-O-H-D-Q-F-A-**7**-L-I-3-W-N-E-C-G-Z

The above decoded texts are mapped to the positions below,
01-02-03-04-05-06-07-08-09-10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-25-26-27-28-29- 30-31-32-33-34-35-36

Now, the question arises as to where to use this decoded text substitutions. Apart from the book text, we are given a final number as mentioned below,

Final number:

021924042408112707191406022411040104040408301814190407180714121224190719170912062406270107062704143004080918170602120819140406140809081718140427181808300604080907141706172717092430240909120819170914270124041130070604190624090111091806191118 02270619

This final number for decoding can be seen as,

02-19-24-04-24-08-11-27-07-19-14-06-02-24-11-04-01-04-04-04-08-30-18-14-19-04-07-18-07-14-12-12-24-19-07-19-17-09-12-06-24-06-27-01-07-06-27-04-14-30-04-08-09-18-17-06-02-12-08-19-14-04-06-14-08-09-08-17-18-14-04-27-18-18-08-30-06-04-08-09-07-14-17-06-17-27-17-09-24-30-24-09-09-12-08-19-17-09-14-27-01-24-04-11-30-07-06-04-19-06-24-09-01-11-09-18-06-19-11-18-02-27-06-19

Using the substitution mapping based on the positions of the text we substitute 02 as 0, 19 is T and so on. In the end, two final number substitutions are derived based on two possible decoded book texts.

1st possibility:

0-T-Q-6-Q-P-5-9-R-T-7-1-0-Q-5-6-S-6-6-6-P-3-4-7-T-6-R-4-R-7-U-U-Q-T-R-T-2-8-U-1-Q-1-9-S-R-1-9-6-7-3-6-P-8-4-2-1-0-U-P-T-7-6-1-7-P-8-P-2-4-7-6-9-4-4-P-3-1-6-P-8-R-7-2-1-2-9-2-8-Q-3-Q-8-8-U-P-T-2-8-7-9-S-Q-6-5-3-R-1-6-T-1-Q-8-S-5-8-4-1-T-5-4-0-9-1-T

2nd possibility:

0-T-Q-6-Q-P-5-7-R-T-9-1-0-Q-5-6-S-6-6-6-P-3-4-9-T-6-R-4-R-9-U-U-Q-T-R-T-2-8-U-1-Q-1-7-S-R-1-7-6-9-3-6-P-8-4-2-1-0-U-P-T-9-6-1-9-P-8-P-2-4-9-6-7-4-4-P-3-1-6-P-8-R-9-2-1-2-7-2-8-Q-3-Q-8-8-U-P-T-2-8-9-7-S-Q-6-5-3-R-1-6-T-1-Q-8-S-5-8-4-1-T-5-4-0-7-1-T

The above two acts as an input to next stage cipher in BCR i.e. Caesar cipher.

Mayuri Wadkar | Pratik Surana
mayuri.wadkar@sjsu.edu | pratik.surana@sjsu.edu
SJSU ID – 012447851 | SJSU ID - 012115402

b) **Caesar Class**

This class is responsible for shifting the plaintext (here, the ouput of codebook cipher above) to left or right by certain offset. In our BCR challenge, the offset for digits is given as 7 and the offset for letters needs to be determined. We also must determine the directions in which the letters or digits must be shifted in order to decipher the input.

After careful analysis of output of stage1 Book cipher, following observations has been made:

- Input to this stage has only letters in range P to U (P, Q, R, S, T, U).
- Treasure Map has only six potential starting points (A, B, C, D, E, F).

The challenge of finding an offset for letters based on above observations becomes easy. We know one fact for sure that the final secret message has one or more alphabets from A, B, C, D,E or F as these are the potential starting points marked on the map. Thus, letters in this stage (P to U) must shift in some direction (left or right) by certain offset, to get desired result i.e. letters in range A to E. In order to map this relation, letters must shift by an offset of 15 to right. With this approach, the resulting decoded text will have letters in range A-F.

Now, we have the required **Caesar key = 1507**
Where,

Offset for letters = **15** (Direction - to right)
Offset for digits = **07** (Direction - unknown)

Two inputs to this stage are decoded by Caesar cipher as below,

Shifting digits by 7 to left & shifting letters by 15 to right for 1st possibility from stage1:
7-E-B-3-B-A-2-6-C-E-4-8-7-B-2-3-D-3-3-3-A-0-1-4-E-3-C-1-C-4-F-F-B-E-C-E-9-5-F-8-B-8-6-D-C-8-6-3-4-0-3-A-5-1-9-8-7-F-A-E-4-3-8-4-A-5-A-9-1-4-3-6-1-1-A-0-8-3-A-5-C-4-9-8-9-6-9-5-B-0-B-5-5-F-A-E-9-5-4-6-D-B-3-2-0-C-8-3-E-8-B-5-D-2-5-1-8-E-2-1-7-6-8-E

Shifting digits by 7 to right & shifting letters by 15 to right for 1st possibility from stage1:
3-E-B-9-B-A-8-2-C-E-0-4-3-B-8-9-D-9-9-9-A-6-7-0-E-9-C-7-C-0-F-F-B-E-C-E-5-1-F-4-B-4-2-D-C-4-2-9-0-6-9-A-1-7-5-4-3-F-A-E-0-9-4-0-A-1-A-5-7-0-9-2-7-7-A-6-4-9-A-1-C-0-5-4-5-2-5-1-B-6-B-1-1-F-A-E-5-1-0-2-D-B-9-8-6-C-4-9-E-4-B-1-D-8-1-7-4-E-8-7-3-2-4-E

Shifting digits by 7 to left & shifting letters by 15 to right for 2nd possibility from stage 1:
7-E-B-3-B-A-2-4-C-E-6-8-7-B-2-3-D-3-3-3-A-0-1-6-E-3-C-1-C-6-F-F-B-E-C-E-9-5-F-8-B-8-4-D-C-8-4-3-6-0-3-A-5-1-9-8-7-F-A-E-6-3-8-6-A-5-A-9-1-6-3-4-1-1-A-0-8-3-A-5-C-6-9-8-9-4-9-5-B-0-B-5-5-F-A-E-9-5-6-4-D-B-3-2-0-C-8-3-E-8-B-5-D-2-5-1-8-E-2-1-7-4-8-E

Shifting digits by 7 to right & shifting letters by 15 to right for 2nd possibility from stage1:
3-E-B-9-B-A-8-0-C-E-2-4-3-B-8-9-D-9-9-9-A-6-7-2-E-9-C-7-C-2-F-F-B-E-C-E-5-1-F-4-B-4-0-D-C-4-0-9-2-6-9-A-1-7-5-4-3-F-A-E-2-9-4-2-A-1-A-5-7-2-9-0-7-7-A-6-4-9-A-1-C-2-5-4-5-0-5-1-B-6-B-1-1-F-A-E-5-1-2-0-D-B-9-8-6-C-4-9-E-4-B-1-D-8-1-7-4-E-8-7-3-0-4-E

Above four outputs from Caesar cipher act as a HEX input to next stage of BCR i.e. RSA cipher.

c) RSA Class

RSA class is responsible for finding RSA key, plaintext and the secret message which will help Alice and Bob find the treasure location before Eve.

In order to start decoding inputs, we must convert the HEX inputs to Decimal system.

HEX to decimal conversion on four inputs:

Input1 converted to decimal system:
10125618422340944610778902186896347440473218475784486820423433199011323089135148931639772117572447203345511051525238349179878007824759616764595781390 2

Input2 converted to decimal system:
50128190848621962191008658423392530960013653964008820122341404311217561165537455254144570149659309053721142936464401700360179699485409768697057718862

Input3 converted to decimal system:
10125618412816449967609269493654458268309006116478734313708016008480492509835046720043811098847076415870830404144254101254506496174649217956064745588 6

Input4 converted to decimal system:
50128190753377015759312331490973639238371530370951295055187232405909255372536433138184959962405601178974336462654559221106464582984305780611747360846

The first challenge at this stage is to find the RSA key, i.e. n – modulus, e-exponent and c-ciphertext. Also, one cannot ignore the fact that exponent **e** is usually of the form **2^k+1 (e.g. 3,5,17, 257, 65537,…).**

Thus, our analysis based on the above fact made us realize that the most common exponent value is hidden in one of our above 4 options.
Input2 has exponent value **e = 65537** at the middle of the string. Thus, on splitting the string we get our RSA key.

Input2:
5012819084862196219100865842339253096001365396400882012234140431121756116553745525414457014965930905372114293646440170036017969948540976869705771886 2

RSA key and ciphertext are recovered below:
N = 501281908486219621910086584233925309600136539640088201223414043112175611
e = 65537
c = 455254144570149659309053721142936464401700360179699485409768697057718862

Next challenge at this stage is to find plaintext m, which can be achieved by following basic RSA principle steps as mentioned below:

Step1: Find two large primes p & q by factorizing n.

Step2: Find (p-1) *(q-1), as e is relatively prime to (p-1) *(q-1).
Thus, we get gcd(e, (p-1)(q-1)) = 1, then there exists d such that
d = e^ (-1) mod ((p-1) *(q-1))

Step3: Find plaintext message m by decrypting c as,
m = c^ d mod n

Applying above steps to our cryptosystem,

Step1: We used https://factordb.com/index.php tool to factorize 72 digit N-value and the resulting factors p & q are mentioned below,
p = 578455732137135466812346681323546443
q = 866586465716584657165746753876546577

Step2: Compute (p-1)*(q-1) and d,
(p-1)*(q-1) =
501281908486219621910086584233925308155094341786368077245320607912082592
Computing d by taking multiplicative modular inverse, d = e^ (-1) mod ((p-1) *(q-1))
d = 298082873119252710460625055681222869281660460407961156878212145977719009

Mayuri Wadkar | Pratik Surana
mayuri.wadkar@sjsu.edu | pratik.surana@sjsu.edu
SJSU ID – 012447851 | SJSU ID - 012115402

Step3: Decipher plaintext m as m = c^ d mod n
Thus, we get m as,
M = 700820790770680710790780790820840720510550870690830840500510680730710753

At this point we are just one step away from breaking the secret message.

One last conversion of the decimal m to ASCII needs a special arrangement of digits in m. We must split numbers in m into groups of three digits. Each group represents the decimal equivalent of a character in ASCII code.
m = 700-820-790-770-680-710-790-780-790-820-840-720-510-550-870-690-830-840-500-510-680-730-710-53

On converting each decimal equivalent to ASCII, we get our most wanted secret message, which Alice and Bob can use to find treasure before Eve finds out.

Decrypted Message - F R O M D G O N O R T H 3 7 W E S T 2 3 D I G 5

This message can be read as,

“FROM D GO NORTH 37 WEST 23 DIG 5”

Attack on cryptosystem:

- Work Factor for attack (decryption) is : **1573** Computations for given crypto challenge
- Work Factor for encryption is : **310** Computations for the same plaintext & codebook

Results:

We have also implemented the cryptosystem that we have in the challenge for encryption of plaintext. Giving the plaintext as **F R O M D G O N O R T H 3 7 W E S T 2 3 D I G 5** using the same keys and the codebook that we have from the challenge data above we implemented the encryption of the plaintext and our resultant output ciphertext matched with the one given in the challenge data. This shows that our cryptosystem implementation or encryption and decryption are computationally and theoretically tallied and verified.

Cryptosystem Improvements:

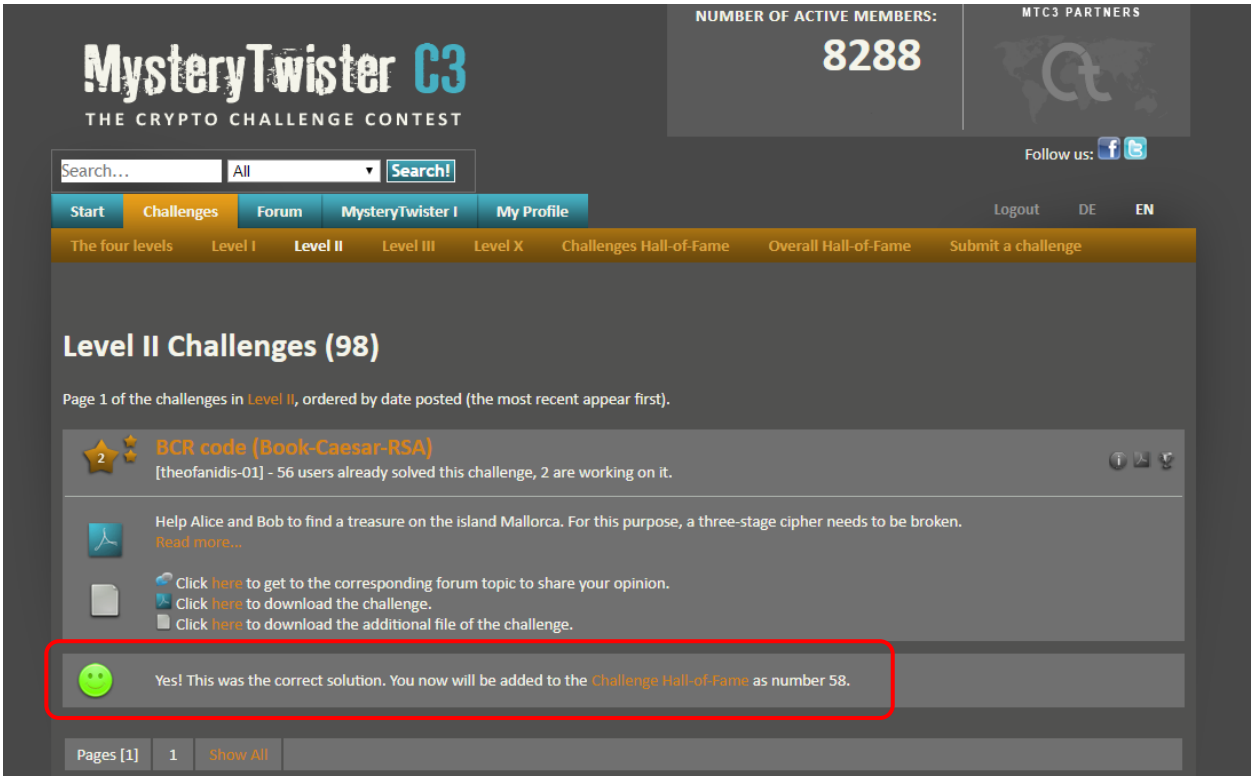
For Code Book Cipher – We can improve the security of the code book crypto system by using additives or an additive codebook to encrypt the data. Also, the pattern for the codebook should not be as obvious as it was in this challenge and should contain a large number of permutations and combinations to confuse the attacker

For Caeser Cipher – We can improve the Caeser cryptosystem by using padding techniques. Also, we can use various permutations and combinations instead of just the simple substitution of the keys by using methods like double transposition.

For RSA Cipher – We can improve and make RSA system more robust by using repeated squaring technique. We can pad random numbers at the end of each iteration to increase the security or the RSA cipher.

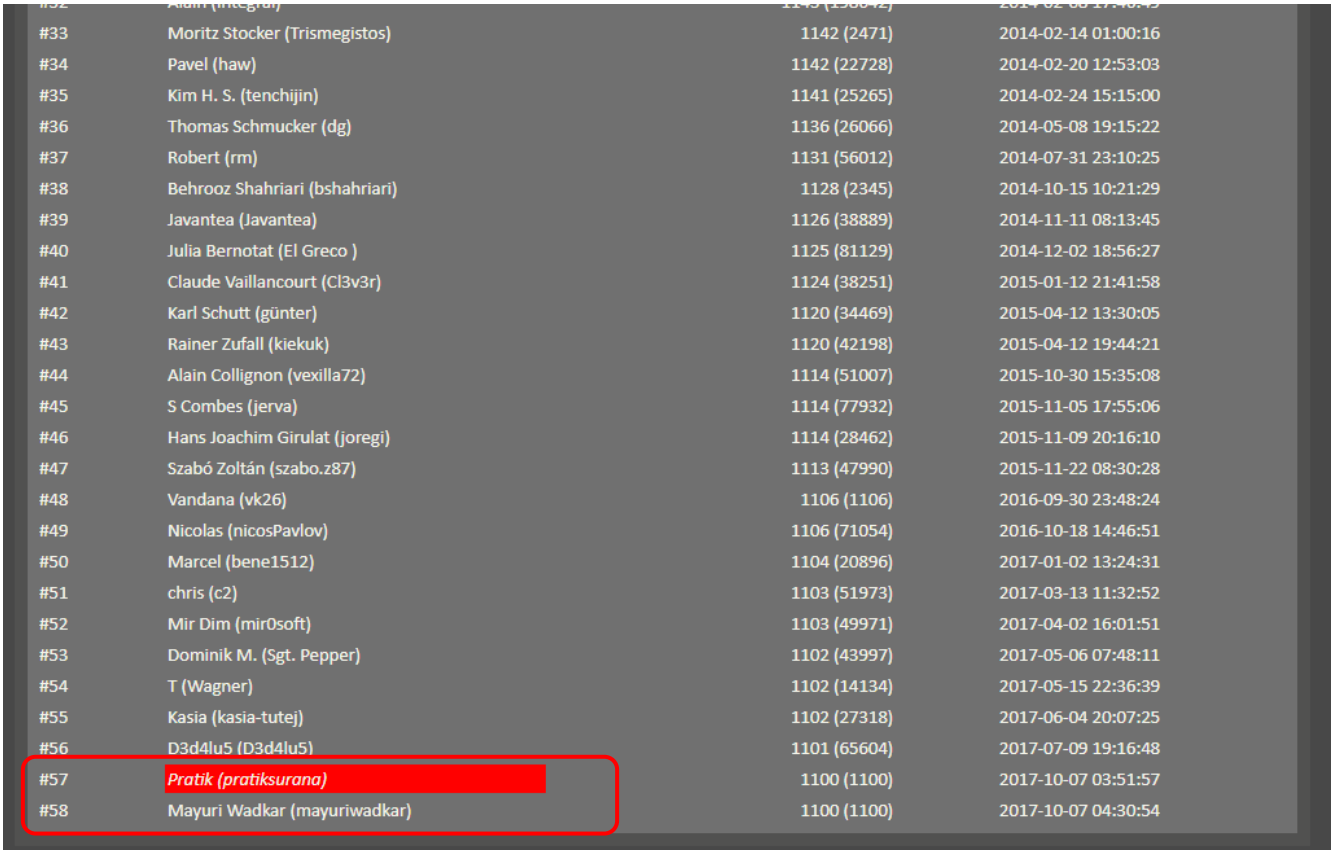
Conclusion:

We have successfully implemented the attack on the BCR (BOOK-CAESER-RSA) Crypto challenge and also successfully implemented the encryption algorithms of all the three ciphers. This project has given us an opportunity to deep dive into three different crypto systems and get to know their working mechanisms, work factors and advantages & disadvantages of the same. We have also attached the screenshots showing the acceptance of our work on the website of the challenge : www.mysterytwisterc3.org below.



Mayuri Wadkar | Pratik Surana
mayuri.wadkar@sjsu.edu | pratik.surana@sjsu.edu
SJSU ID – 012447851 | SJSU ID - 012115402

Screen shot of The Hall of Face for that challenge :



#33	Moritz Stocker (Trismegistos)	1142 (2471)	2014-02-14 01:00:16
#34	Pavel (haw)	1142 (22728)	2014-02-20 12:53:03
#35	Kim H. S. (tenchijin)	1141 (25265)	2014-02-24 15:15:00
#36	Thomas Schmucker (dg)	1136 (26066)	2014-05-08 19:15:22
#37	Robert (rm)	1131 (56012)	2014-07-31 23:10:25
#38	Behrooz Shahriari (bshahriari)	1128 (2345)	2014-10-15 10:21:29
#39	Javantea (Javantea)	1126 (38889)	2014-11-11 08:13:45
#40	Julia Bernotat (El Greco)	1125 (81129)	2014-12-02 18:56:27
#41	Claude Vaillancourt (Cl3v3r)	1124 (38251)	2015-01-12 21:41:58
#42	Karl Schutt (günter)	1120 (34469)	2015-04-12 13:30:05
#43	Rainer Zufall (kiekuk)	1120 (42198)	2015-04-12 19:44:21
#44	Alain Collignon (vexilla72)	1114 (51007)	2015-10-30 15:35:08
#45	S Combes (jerva)	1114 (77932)	2015-11-05 17:55:06
#46	Hans Joachim Girulat (joregi)	1114 (28462)	2015-11-09 20:16:10
#47	Szabó Zoltán (szabo.z87)	1113 (47990)	2015-11-22 08:30:28
#48	Vandana (vk26)	1106 (1106)	2016-09-30 23:48:24
#49	Nicolas (nicosPavlov)	1106 (71054)	2016-10-18 14:46:51
#50	Marcel (bene1512)	1104 (20896)	2017-01-02 13:24:31
#51	chris (c2)	1103 (51973)	2017-03-13 11:32:52
#52	Mir Dim (mir0soft)	1103 (49971)	2017-04-02 16:01:51
#53	Dominik M. (Sgt. Pepper)	1102 (43997)	2017-05-06 07:48:11
#54	T (Wagner)	1102 (14134)	2017-05-15 22:36:39
#55	Kasia (kasia-tutej)	1102 (27318)	2017-06-04 20:07:25
#56	D3d4lu5 (D3d4lu5)	1101 (65604)	2017-07-09 19:16:48
#57	*Pratik (pratiksurana)*	1100 (1100)	2017-10-07 03:51:57
#58	Mayuri Wadkar (mayuriwadkar)	1100 (1100)	2017-10-07 04:30:54

References:

1. https://www.braingle.com/brainteasers/codes/book.php
2. https://www.mysterytwisterc3.org/images/challenges/mtc3-theofanidis-01-bcr-en.pdf
3. https://factordb.com/index.php