MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

# BCR Code (Book-Caesar-RSA)

Author: George Theofanidis

August 2012; update April 2015

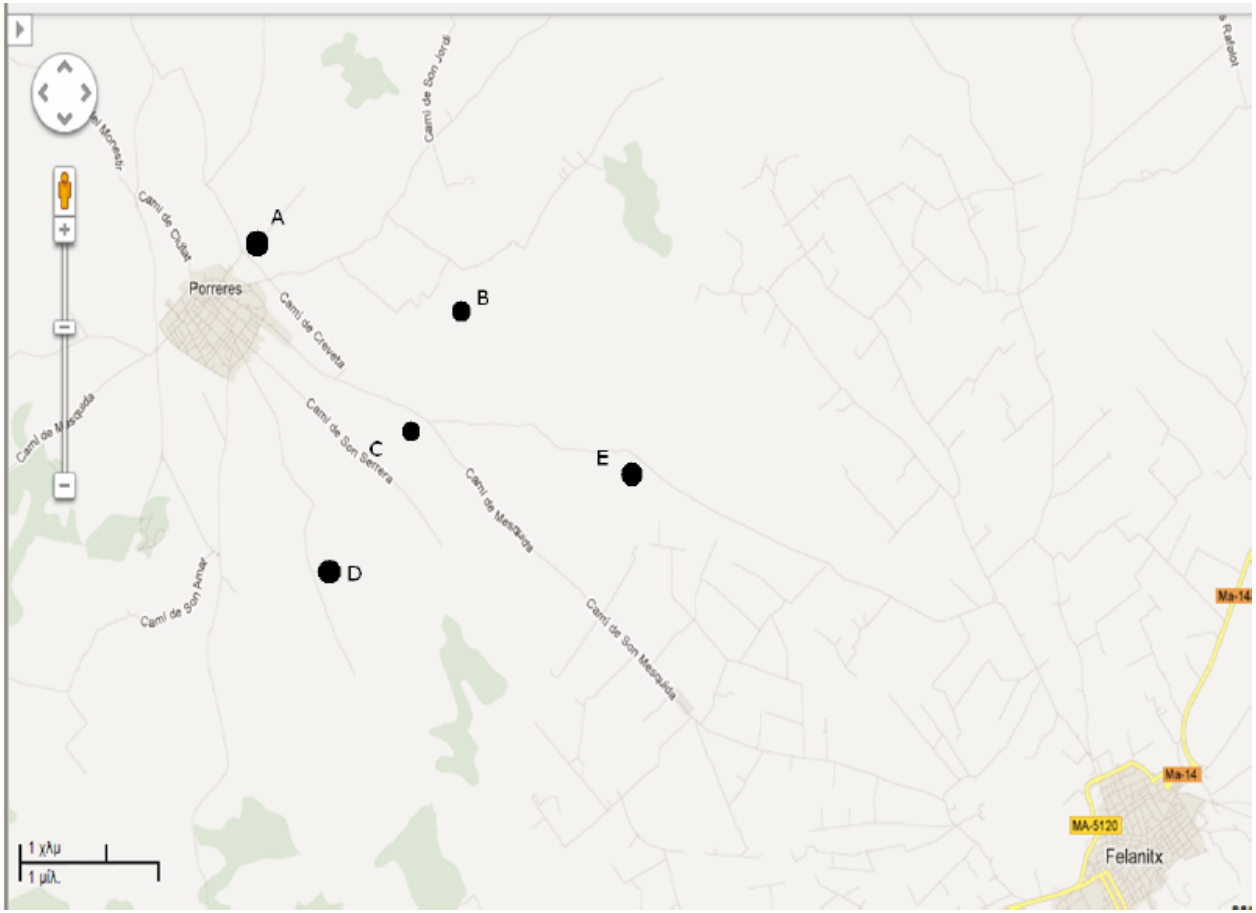
# Introduction

Once upon a time, there have been three pirates: Alice, Bob and Eve. They lived on the island Mallorca near a village called Porreres.

One day, while Alice and Bob were digging in their garden, they found a treasure map. Because they could not figure out how to use the instructions, they asked Eve who was an expert on mysteries and riddles for help.
It turned out that Eve has made copies of the map and the instructions for herself and is trying to find the treasure on her own.

Can you help Alice and Bob to find the treasure before Eve finds the location?

# Treasure Map




The points marked on the map are potential starting points of the treasure hunt.

# Challenge

This cipher (called BCR) consists of a three-stage cascade:
The first stage (B) is an altered book cipher. The second one (C) is a Caesar cipher and the third and last one (R) is an RSA cipher. Each stage uses the output of the previous one as input.

Please submit the text of the last stage (R) in capital letters and with spaces to solve this challenge.

# Challenge Data (1)

**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
Alice and Bob could not read some parts of the text. The two words are marked as XXX and YYY. You have to figure out the correct substitutions.

# Challenge Data (2)

**Caesar Cipher**:
The digits were shifted by 7 during encryption. The offset for the letters needs to be determined.

The **RSA key** is not given.

**Final number**:
021924042408112707191406022411040104040408301814
190407180714121224190719170912062406270107062704
143004080918170602120819140406140809081718140427
181808300604080907141706172717092430240909120819
170914270124041130070604190624090111091806191118
02270619

# Example of a Decryption Using the BCR Code

**RSA key** = 320232
**Caesar key** = 2203
**Book text**:
TWO-ALPHA-NINE-ZULU-ONE-YANKEE-FOXTROT-THREE-GOLF-ECHO-FOUR-LIMA-HOTEL-WHISKEY-NOVEMBER-CHARLIE-SIERRA-FIVE-QUEBECK-INDIA-DELTA-XRAY-OSCAR-TANGO-ROMEO-ZERO-JULIET-UNIFORM-MIKE-PAPPA-SEVEN-BRAVO-KILO-VICTOR-EIGHT-SIX
**Final number:**
183108201027053603273618132713203513031811050127
260711081127030810312011070310032003100307181118
05313105110127

# Example: Stage 1 – Book Cipher (1)

Given the book text from the previous slide, you know that 01 is TWO, 02 is ALPHA, and finally, 36 is SIX. Except for the numbers which have an obvious substitution, the words represent the first letter as in the NATO phonetic alphabet, i.e. XRAY = X. In detail the book text stands for:

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

and is substituted to

```
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
```

# Example: Stage 1 – Book Cipher (2)

The final number can be seen as
18-31-08-20-10-27-05-36-03-27-36-18-13-27-13-20-35-13-03-18-11-05-01-27
26-07-11-08-11-27-03-08-10-31-20-11-07-03-10-03-20-03-10-03-07-18-11-18
05-31-31-05-11-01-27.
With the substitution on the previous page 18 is 5, 31 is 7, 08 is 3, 20 is I and so on. In the end the final number is converted to
573IEJ169J65HJHI8H95412J0F434J93E7I4F9E9I9E9F545177142J

# Example: Stage 2 – Caesar Cipher

Since the key of this stage is 2203, the letters of the output of the first stage (573IEJ169J65HJHI8H95412J0F434J93E7I4F9E9I9E9F545177142J) are shifted by an offset of 22 to the right. The digits are shifted three positions to the left.
The output of this stage is the HEX number:
240EAF836F32DFDE5D62189F7B101F60A4E1B6A6E6A6B212844819F

# Example: Stage 3 – RSA Cipher (1)

This HEX number is now converted into the decimal system.
This results in: 237330237825208780597560937716131711118972545543347912460760023455

The given key RSA (320232) means that the 32 most significant digits (from the left to the right) are the RSA modulus (n), the next two digits (to the right) represent e and the 32 digits to the right are the ciphertext, so:
n = 23733023782520878059756093771613
e = 17
c = 11118972545543347912460760023455

# Example: Stage 3 – RSA Cipher (2)

Hence, the plaintext is m = 065083049048069048053068048051. If you split this numbers into groups of three digits, each group represents the decimal equivalent of a character in ASCII code: 065-083-049-048-069-048-053-068-048-051 is AS10E05D03. This means choose starting position A (as indicated on the map), go 10 meters south, then 5 meters eastwards and dig 3 meters deep to find the treasure.