One Time Pads (OTP) -- A simplified exercise, by JJS

ENCRYPTING

In this exercise, you will practice encrypting a short message.
Message: 'I am a patriot'

Step 1. Write out your message on a piece of paper: 'I am a patriot'

Step 2. Using the Conversion Table below, translate the plain text into numbers:
(Below is your conversion table, NOT a one-time pad key. This is for converting plain text into a number value.)

```
CONVERSION TABLE NO.1 EN
CODE-1

A-1   B-70 P-80 FIG-90
E-2   C-71 Q-81 (.)-91
I-3   D-72 R-82 (:)-92
N-4   F-73 S-83 (')-93
O-5   G-74 U-84 ( )-94
T-6   H-75 V-85 (+)-95
      J-76 W-86 (-)-96
      K-77 X-87 (=)-97
      L-78 Y-88 REQ-98
      M-79 Z-89 SPC-99
```

I	(space)	a	m	(space)	a	(space)	p	a	t	r	i	o	t
3	99	1	7 9	99	1	99	80	1	6	82	3	5	6

Step 3: Check your work.
You should have the following: 3 99 1 79 99 1 99 80 1 6 82 3 5 6

Step 4: Using the 'Cherry' One Time Pad (OTP) below , line up your converted plain text from Step 3 with the numbers from the first line of your OTP.
NOTE: You will skip the first number group (28106), and begin with the second number group (78366).

Plain Text: - - - - - 39917 99919 98016 82356
One Time Pad: 28106 78366 39313 86843 80570

Cherry

28106-78366-39313-86843-80570
81922-58484-19146-20991-37237
52705-21971-23132-28754-05428
96945-27917-02536-68322-45115
98269-39998-31500-45565-07979

DESTROY AFTER USE

Step 5: Now subtract the numbers, left to right. There are no negatives, so add a 1 to make a two-digit number if you must. For example, 3 minus 7 would become 13 minus 7, equaling 6.

Plain Text: - - - - - 39917 99919 98016 82356
One Time Pad: 28106 78366 39313 86843 80570
28106 61651 60606 12273 02886

NOTE: Whether ENCRYPTING or DECRYPTING, the One Time Pad numbers always go on the bottom.

Now you have encrypted your message and it is ready to send: 28106 61651 60606 12273 02886

Why not use the first set of numbers (in this example, 28106)?
Because this is you KEY ID. It lets the recipient know he is using the correct line when decrypting. This will be important for future exercises.

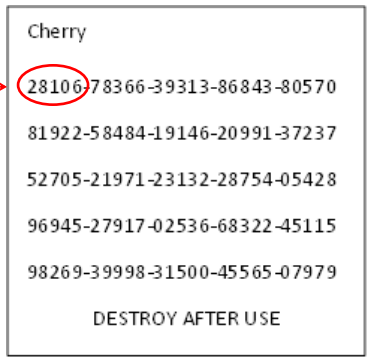
DECRYPTING

In your handling instructions you were told to use the OTP titled 'Cherry', which had been issued to you beforehand.

Here is your encrypted message (cypher text) as you received it: **28106 61651 60606 12273 02886**

Step-1

Identify the line you are supposed to begin decrypting from, by locating the KEY ID



Cypher Text: 28106 61651 60606 12273 02886
One Time Pad: 28106 78366 39313 86843 80570

Step-2

Add the numbers, except for the first group, which is only used as your KEY ID. When adding, drop the first '1' in any two-digit numbers. 9 + 8 = 7 (not 17)

Cypher Text: 28106 61651 60606 12273 02886
One Time Pad: 28106 78366 39313 86843 80570
----- 39917 99919 98016 82356

Step-3

Decode (convert the plain text numbers to text) using the Conversion Table

3 99 1 79 99 1 99 80 1 6 82 3 5 6
i a m a p a t r i o t

As you can see in the Conversion Table, there are no two-digit numbers beginning with 1 through 6, and no single digit numbers higher than 7. So you can't mess up, unless you struggle with 3rd grade math.

