LAB – 3 B00122875 Vimal Jaswal

One Time Pad Lab 3

Numbers station

As a little exercise we will decipher a recording of an actual numbers station. The broadcast starts with a repeated call sign melody and the receiver's call sign "39715", followed by six tones and the actual message. Try using the given one-time pad key underneath with the help of the "AT-ONE-SIR" straddling checkerboard. (You have to research how straddling checkerboard works)

This little exercise shows exactly how secret agents can receive messages in an absolutely secure manner, with only one-time pads, a small short-wave receiver and pencil and paper.

The one-time pad key to decipher this message:

```
66153 77185 10800 54937 48159 83271 12892 07132 34987 53954 23074
```

Important Note: Although we use a recording from an actual numbers station (Lincolnshire Poacher, E3 Voice), the one-time pad key is fictitious and reverse-calculated (key = plaintext - ciphertext) so that a readable but fictitious message is obtained when using this key. In reality, we don't know which key was used, whether we must add or subtract and there is no way to decipher the original message. In fact, since a one-time pad key is truly random, one can calculate any plaintext from a given ciphertext, as long as you use the 'right' wrong key. That's exactly why one-time pad is unbreakable.

Solution:

key = plaintext – ciphertext

plaintext = key +ciphertext

The digit of ones' place is considered while addition of ciphertext and one-time pad key.

66153 77185 10800 54937 48159 83271 12892 07132 34987 53954 23074 OTP Key

+

66475 19274 92028 78494 24146 68542 17507 39398 32348 59378 70636 ciphertext (audio)

=

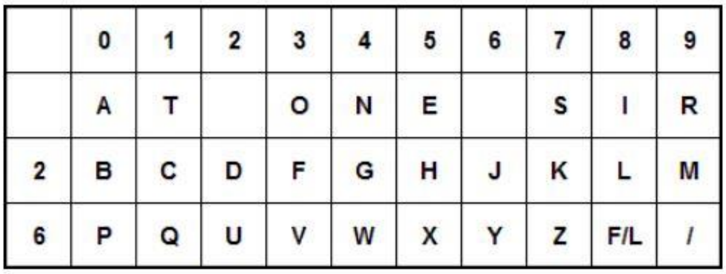
22528 86359 02828 22321 62295 41713 29399 36420 66225 02222 93600 plaincode

Straddling Checkerboards:

straddling checkerboards is a system to encode plain text into digits. This encoding is not a type of encryption and offers no cryptographic security. The encoding only prepares the plaintext for the actual encryption process. Therefore, the result of encoding a plain code, the message is still in its plain readable form.

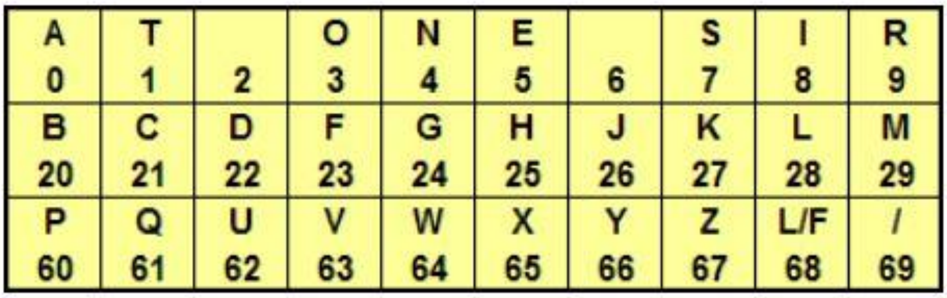
These checkerboards are easily designed from scratch or customized to fit the requirements of its users. This can range from simple text-only encoding to the use of special characters, words or codes for specific purposes or languages. Anything is possible, as long as both sender and receiver agree upon a common system. The straddling checkerboard encodes the most frequently used letters into one-digit values. All other letters are encoded into two-digit values. This reduces the size of the message.

A checkerboard also breaks up individual letters into seperate parts. This is called fractionation. Moreover, it does this irregularly (some are single and some double-digit values). When the checkerboard encoding is followed by an encryption algorithm that transposes the plaincode digits, then the irregular fractionation will cause the characters to be torn apart in a most irregular fashion and produce a far more complex encryption. Often, such encryption methods also use a checkerboard that has the order of its letters or digits scrambled to increase the total strength of the encryption.



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

Another version of the above checkerboard is shown below.



A 0	T 1	2	O 3	N 4	E 5	6	S 7	I 8	R 9
B 20	C 21	D 22	F 23	G 24	H 25	J 26	K 27	L 28	M 29
P 60	Q 61	U 62	V 63	W 64	X 65	Y 66	Z 67	L/F 68	/ 69

The digits 2 and 6 are used in combination with other numbers as per checkerboard. Using this standard checkerboard the plaintext decoded can be written as following:

Plain code→Plaintext

22 5 28 8 63 5 9 0 28 28 22 3 21 62 29 5 4 1 7 1 3 29 3 9 9 3 64 20 66 22 5 0 22 22 9 3 60 0

D E Liver A L L D O C U MENTSTO MORRO W B Y D EAD DRO P A