One Time Pad Lab 3

Lab 2c - 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.