# Meet Me at Midway

## Task

* Category: Van Halen Radiation Belt
* Points: 155
* Solves: 21

Description:

Pacific fleet intercepted some encrypted messages

Attachement:

* encrypted\_msgs.txt
* word\_dictionary.json

## Solution

The challenge name together with the description refers to the battle of Midway, which took place in Second World War in the Pacific. Thus, it is likely we are dealing with a [Japanese naval code](https://en.wikipedia.org/wiki/Japanese_naval_codes). For example, JN-25 is a code book of 5 digit numbers divisible by three. The file word\_dictionary.json contains mappings from these 5 digit numbers to words. Furthermore the messages are encrypted. The encryption function is false addition, that is digit-wise addition without carry.

After sorting the dictionary by the keys we get the following result:

10035 -> THE  
10044 -> IN  
10059 -> CHAPTER  
10062 -> AS  
10065 -> I  
10068 -> SIT  
10071 -> DOWN  
10074 -> TO  
10077 -> WRITE  
10080 -> HERE  
10083 -> AMIDST  
10086 -> SHADOWS  
10089 -> OF  
10092 -> VINELEAVES  
10095 -> UNDER  
10098 -> BLUE  
10101 -> SKY  
10104 -> SOUTHERN  
10107 -> ITALY  
10110 -> IT  
10113 -> COMES  
10116 -> ME  
10119 -> WITH  
10122 -> A  
10125 -> CERTAIN  
[...]

A quick research shows that these words make up the beginning of the novel “The First Men In The Moon” by H. G. Wells. From this we can conclude that the word dictionary is at least partially generated by parsing the text of the novel (omitting duplicates and assuring divisibility by three).

In case a fully random key is used for each word, the cipher becomes a OTP and perfectly secure. So we can probably assume that there is a repeated key used somewhere. Furthermore, the dictionary is not exhaustive. But each decoded word must still be in our given dictionary, we can use this to restrict the key space. For example, if we assume that the same key is used for a single row then there are no possible keys.

Anyways, the solutions is that the opening of the novel is a known plaintext and therefore allows to retrieve the key. The key is repeated for each row. For the remaining part, we noticed that the keys follow a distinct pattern, more precisely there are consecutive primes.

Flag: flag{golf75253november4:GLDsDcqzsvuo\_\_FQjQJSq0XA9uG7OJdhN3TIuPPiqP\_LMcrBxgSJcnklQ5ecMCyU3GgsslDLbkiImKNTV0iMLQU}