# STRADDLING CHECKERBOARD

In cryptography, a straddling checkerboard is a device for converting an alphabetic plaintext into digits whilst simultaneously achieving fractionation (a simple form of information diffusion) and homophony (a simple method for suppressing peaks of the frequency distribution).

A straddling checkerboard is set up something like this:

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

The first row is set up with the eight highest frequency letters, leaving two blank spots. It has no row label. The second and third rows are labelled with whichever two digits didn't get a letter in the top row, and then filled out with the rest of the alphabet. (This can be scrambled by a key word, or simply done in order - relying on another stage of the cipher for security). Since there are 30 slots in our grid, and we missed two letters in the first row, there will end up being two spare in the other rows. It doesn't matter where spares go, as long as sender and receiver use the same system.

To encipher, a letter on the top row is simply replaced by the number labelling its column. Letters on the other rows are replaced by their row number, then column number. Like so:

```
A  T  T  A  C  K  A  T  D  A  W  N
3  1  1  3 21 27  3  1 22  3 65  5
```

The resulting message, `3113212731223655`, may be sent directly (if the table was set up with a key word), but usually is first input into a second cipher stage, such as transposition or substitution. As a simple example, we will add a secret key number (say, 0452) by non-carrying addition:

```
  3 1 1 3 2 1 2 7 3 1 2 2 3 6 5 5
+ 0 4 5 2 0 4 5 2 0 4 5 2 0 4 5 2
= 3 5 6 5 2 5 7 9 3 5 7 4 3 0 0 7
```

then use the same straddling checkerboard to turn it back into letters:

```
3  5 65 25 7  9  3  5  7  4  3  0  0  7
A  N  W  H  R  S  A  N  R  O  A  E  E  R
```

Deciphering is simply the reverse of this process. Although the size of groups can vary, deciphering is unambiguous because whenever the next element to be deciphered starts with a 2 or a 6, it is a pair; otherwise, it is a singleton.

[Excerpt from “Straddling checkerboard” from Wikipedia]