PLAYFAIR

History

The Playfair system was invented by Charles Wheatstone, who first described it in 1854.

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 676 possible digraphs rather than the 26 possible monographs. The frequency analysis of digraphs is possible, but considerably more difficult - and it generally requires a much larger ciphertext in order to be useful.

Lord Playfair promoted the use of the cipher, and his name became associated with the system.

The first recorded description of the Playfair cipher was in a document signed by Wheatstone on 26 March 1854. However, the scheme eventually came to be known by the name of Wheatstone's friend Lord Playfair, who popularized it. It was not adopted by the British Foreign Office when it was developed, rejected because of its perceived complexity. When Wheatstone offered to demonstrate that three out of four boys in a nearby school could learn to use it in 15 minutes, the Under Secretary of the Foreign Office responded, "That is very possible, but you could never teach it to attachés."

It was used by British forces in the Boer War and World War I and also by the Australians during World War II.

The first published solution of the Playfair was described in a 19-page pamphlet by Lieutenant Joseph O. Mauborgne, published in 1914.

Usage

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit, other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

To encrypt a message, one would apply the following 4 rules, in order, to each pair of letters in the plaintext:

- If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
- If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
- If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
- If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important - the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter.

To decrypt, use the inverse of these 4 rules (dropping any extra "X"s that don't make sense in the final message when you finish).

Example

Using "playfair example" as the key, the table becomes:

```
P L A Y F
I R E X M
B C D G H
J K N O S
T U V W Z
```

Encrypting the message "Hide the gold in the tree stump":

```
HI DE TH EG OL DI NT HE TR EX ES TU MP
                ^
```

1. The pair HI forms a rectangle, replace it with BM
2. The pair DE is in a column, replace it with ND
3. The pair TH forms a rectangle, replace it with ZB
4. The pair EG forms a rectangle, replace it with XD
5. The pair OL forms a rectangle, replace it with KY
6. The pair DI forms a rectangle, replace it with BE
7. The pair NT forms a rectangle, replace it with JV
8. The pair HE forms a rectangle, replace it with DM
9. The pair TR forms a rectangle, replace it with UI
10. The pair EX (X inserted to split EE) is in a row, replace it with XM
11. The pair ES forms a rectangle, replace it with MN
12. The pair TU is in a row, replace it with UV
13. The pair MP forms a rectangle, replace it with IF

```
BM ND ZB XD KY BE JV DM UI XM MN UV IF
```

Thus the message "Hide the gold in the tree stump" becomes "BMNDZBXDKYBEJVDMUIXMMNUVIF".

[Excerpt from “Playfair cipher” from Wikipedia]