This is based on Chapter 3 of Lewand and Chapter 2 of Trappe and Washington.
**PLAYFAIR**

The Playfair cipher was used during WWI.  

**Sample codeword:**  PLAYFAIR

<table>
<thead>
<tr>
<th>MATRIX</th>
<th>RULE 1</th>
<th>RULE 2</th>
<th>RULE 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>p l a y f</td>
<td>p₁ c₁</td>
<td>p₁c₁p₂c₂</td>
<td>p₁</td>
</tr>
<tr>
<td>i r b c d</td>
<td>c₂ p₂</td>
<td>c₁</td>
<td>c₁</td>
</tr>
<tr>
<td>e g h k m</td>
<td></td>
<td></td>
<td>p₂</td>
</tr>
<tr>
<td>n o q s t</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>u v w x z</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** no j in the matrix.

**Preparing the message**

john meet at school house  ⇒

io hn me et at sc ho ol ho us ex
PLAYFAIR, CONTINUED

<table>
<thead>
<tr>
<th>MATRIX</th>
<th>RULE 1</th>
<th>RULE 2</th>
<th>RULE 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>p</td>
<td>l</td>
<td>a</td>
<td>y f</td>
</tr>
<tr>
<td>i</td>
<td>r</td>
<td>b</td>
<td>c d</td>
</tr>
<tr>
<td>e</td>
<td>g</td>
<td>h</td>
<td>k m</td>
</tr>
<tr>
<td>n</td>
<td>o</td>
<td>q</td>
<td>s t</td>
</tr>
<tr>
<td>u</td>
<td>v w</td>
<td>x z</td>
<td></td>
</tr>
</tbody>
</table>

The message:

io hn me et at sc ho ol ho us ex

io $\Rightarrow$ RN by Rule 1.  hn $\Rightarrow$ EQ by Rule 1.  me $\Rightarrow$ EG by Rule 2.
et $\Rightarrow$ MN by Rule 1.  at $\Rightarrow$ FQ by Rule 1.  sc $\Rightarrow$ XK by Rule 3.
ho $\Rightarrow$ GQ by Rule 1.  ol $\Rightarrow$ VR by Rule 3.  ho $\Rightarrow$ GQ by Rule 1.
us $\Rightarrow$ XN by Rule 1.  ex $\Rightarrow$ KU by Rule 1.

The Result:
RNEQEGMNFQXKGGQVRGQXN
The Playfair scheme is susceptible to frequency analysis.

Single-letter frequency analysis no longer works.

But digraph frequency analysis still does.

Recall the most common digraphs in English: th, er, on, an, re, he, ...

Note that er and re are both in the top 5!

So, if we see, for example, IG and GI frequently in the text, odds are good that i, g, r, e are on the corners of a rectangle in the matrix.

Each character has only 5 possible substitutions. (What are they?)

The end of the matrix is fairly predictable.
**ADFGX CIPHER**

- **Why ADFGX?** Because their symbols in Morse code were not easily confused.

- **Another 5x5 matrix, with** j **treated as i.**

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>F</th>
<th>G</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>p</td>
<td>g</td>
<td>c</td>
<td>e</td>
<td>n</td>
</tr>
<tr>
<td>D</td>
<td>b</td>
<td>q</td>
<td>o</td>
<td>z</td>
<td>r</td>
</tr>
<tr>
<td>F</td>
<td>s</td>
<td>l</td>
<td>a</td>
<td>f</td>
<td>t</td>
</tr>
<tr>
<td>G</td>
<td>m</td>
<td>d</td>
<td>v</td>
<td>i</td>
<td>w</td>
</tr>
<tr>
<td>X</td>
<td>k</td>
<td>u</td>
<td>y</td>
<td>x</td>
<td>h</td>
</tr>
</tbody>
</table>

- No keyword; fill in the matrix randomly.

- Replace each plaintext letter by its Row/Column label, e.g. **Kaiser Wilhelm** ⇒ **XA FF GG FA AG DX GX GG FD XX AG FD GA.**

- **So, what have we really achieved at this point?**
So far, this is just a substitution cipher.

1. Choose a keyword, e.g. Rhein.

2. Label the columns of a matrix.

3. Write the message into the matrix.

4. Sort columns alphabetically.
5. Read off vertically.

$\begin{array}{cccccc}
E & H & I & N & R \\
F & A & F & G & X \\
A & F & A & G & G \\
G & X & X & G & D \\
D & F & X & X & G \\
F & G & D & G & A \\
A & & & & & \\
\end{array}$

$\Rightarrow$ FAGDFAFXFVFGFAXXDGGGXXGXXGDGAA

Discussion of cryptanalysis on pp. 32–33 of Trappe and Washington.
**BLOCK CIPHERS**

\[ p_1 p_2 \cdots p_n \quad \text{key} \quad \Rightarrow \quad c_1 c_2 \cdots c_n \]

- **DES** 64 bits
- **AES** 128 bits
- **RSA** 100s of bits
- **Playfair** 2 letters

**Claude Shannon:** Principles for a good cipher

**DIFFUSION**

Changing one character in the plaintext changes many characters in the ciphertext.

**CONFUSION**

Each part of the ciphertext should depend on several parts of the key
We consider the digraph version of this cipher.

key: a $2 \times 2$ matrix of elements from $\mathbb{Z}_{26}$ \( \exists \)

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ad - bc)$$ is relatively prime to 26.

Encryption:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \pmod{26}.$$

That is:

$$c_1 = (a \cdot p_1 + b \cdot p_2) \pmod{26} \quad \text{Good diffusion}$$

$$c_2 = (c \cdot p_1 + d \cdot p_2) \pmod{26} \quad \text{Poor confusion}$$

Decryption:

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \pmod{26}.$$
To go from ciphertext to plaintext, we need to find $A^{-1}$

Let $d = \det(A)$.

From linear algebra:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = d^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

But remember, $d^{-1}$ can be the multiplicative inverse mod 26.
HILL CIPHER, III

\[ A = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \]

\[ \text{det } A = 9 \cdot 7 - 4 \cdot 5 = 43 \equiv 17 \pmod{26} \]

\[ 17^{-1} \pmod{26} = 23 \]

\[ A^{-1} = 23 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \equiv \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \pmod{26} \]

\[ \text{“fo” } \rightarrow 5 \ 14 \]

\[ \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 5 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 23 \\ 19 \end{pmatrix} \]

\[ 23 \ 19 \rightarrow \text{“xt”} \]

See pages 80 and 81 of Trappe & Washington