

Q.6) DTU/2K16/MC/013

How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Now take into account the fact that some playfair keys produce the same encryption results. How many effectively unique keys does the playfair cycle have?

Ans 6) When we consider the playfair key consists of the alphabet (reduced to 25 letters) spread on a 5×5 square, that's

$25!$ keys.

The rule of Playfair are such that any rotation of the lines in the square, and any rotation of its columns, lead to an equivalent key, in other words, the square reduces to a form.

So, the distinct key classes considering those keys which lead to similar encryption are $25!/5^2$ ciphers