

Simon Singh, *The Code Book*, page 45.

Key: 1

For centuries, the simple monoalphabetic substitution cipher had been sufficient to ensure secrecy. The subsequent development of frequency analysis, first in the Arab world and then in Europe, destroyed its security. The tragic execution of Mary Queen of Scots was a dramatic illustration of the weaknesses of monoalphabetic substitution, and in the battle between cryptographers and cryptanalysts it was clear that the cryptanalysts had gained the upper hand.