THE PLAYFAIR ENCRYPTION

Author: Pascal Schöttle

December 2010

The Playfair Encryption

The Playfair encryption is a relatively simple *monoalphabetic* and *digraph* substitution, which means there is only one ciphertext alphabet but it encrypts pairs of letters. The cipher was invented by *Sir Charles Wheatstone*.

This kind of encryption was promoted by *Lord Lyon Playfair* and was used by the British forces in the Crimean War and in World War I, among others.

Your challenge is to decrypt the ciphertext on the following pages.

Hints: The plaintext is English and the used key is relatively short. The wanted solution is the (fictitious) author of the plaintext and must be typed in with capital letters.

Ciphertext (I)

TNYOLCOIUHNFBMQIPCPNEANV
AFSHPCRYQYNTPBOHZUMVXKAIOA
BITRCZAEWBDHMCUCNF
IOCGBDBPLCOCHKNY

TNOGFEVSAPIOTPTQULLE
NSTBNIPQTPLUABNSCBRKCZLE
QYCZBPNMAIQVBQLCYTPQBITHCZLE
GNOGFCPBNKCPGQKN

AQEQYBCMTINPCDOAHTIOSVEUIBAI
UADBKUCUDFTPYNNPLCLRVFCXIBAC
OISHSVBITNHVKDSXCOKOTQBDBQKV
BGTNYOLCZKZHOARBNTNCABDSAEVBTOKT

Ciphertext (II)

HREONTSVRKPQFPCUVFPADGQBGEINDR
ZTQCTPAPBCXHQEBYGELBEFCZCBNT
PBTCEGZHGIPHIQCBLMCHOBNTUQBVEAQDUC
NKBZVFLBUAOEBHNKLEEDCUDGVHNKALGPWNXN

HTIOYXFCDSBFBUUAUCEFZHVSFA
NKBZEHAIDRIZBOFCCSEGZHNDFA
IBCMVIRKOIZUOTBKBUTIFA
GELAONTPYNEFSBDQAIITSPGELA

AQQTPANUBUYRAPCBPQFPCZELBNNQBD
AUVSDWCOLOCMBYCMACDCQTGETMDBPB
GOCDNYPNSMYBCOELIBBUOGNBGNHVMFTOGEAC
TPFCOKUCBDEQTHVBMNCONKBUST