University of Southampton National Cipher Challenge Solutions

Solution: Message 10

Plaintext:

I believe this cipher would be of greater utility if we included numbers. It occurs to me that we should extend the alphabet to include the numerals, and this would lend itself most conveniently to a six by six grid that would also avoid the need to arbitrarily concatenate two letters in one cell. An altogether more satisfactory solution I am sure you will agree.

With regard to our turning machine bad news I am afraid. My friend close to the French embassy has been making enquiries about CD and Espion. Information is hard to obtain but it seems that the French are constructing an automatic enciphering machine that bears some marked resemblance to our designs. It is an electromechanical device and, like ours, has two rotating wheels that move forward each time a letter is punched into the machine. From what I gather these wheels can be interchanged a marked improvement on our own more fixed design. I have not been able to obtain further details of the internal construction but I will make further enquiries. The most alarming detail which has so far come to my attention is the fact that operating the machine can both encipher and decipher a text using the same settings. This suggests strongly that, like our design, the French machine embodies the principle of the electrical reflector though I am unable to understand how they could have obtained this idea given that we retrieved the only copy of the design drawings from that fiend Espion. It all appears to be a bit of an enigma.

The news from Afghanistan, and the progress of General Keane at the head of the army of the Indus has set me to consider how we might make our machine portable for use by the military. Messages could be passed along a veritable web of electric telegraph lines but it would greatly help if small letters illuminated by the power of electricity could replace the large letter indicator mechanism. Today this seems but an idle dream.

Cipher:

- A Playfair cipher based on the keyword Sherlock. There was a clue given in the plaintext introduction, since Holmes met with Moriarty at the famous Riechenbach Falls. The actual text was padded with the character x to split up any repeated characters, so, for example the word embassy becomes embasxsy. Finally, since the resulting text has an odd number of characters we appended the letter a. The solution checker was able to deal with submissions that variously did or did not include these additions. Usually the characters I/J are treated as one character in the Playfair grid, but to trip you up we elided Y and Z. We arranged the grid so that I and J were almost together so that assuming they were would not prevent you from beginning to tackle the challenge.

Sponsored by:

EPSRC, IBM,
EducationGuardian.co.uk,
London Mathematical Society,
http://www.cryptomathic.com/