University of Southampton National Cipher Challenge Solutions

Solution: Message 16

Plaintext:

My dear brothers,
Ingenuity, duplicity, secrecy, if I may paraphrase our own dear song of liberation.
As you can see the English cipher machine, obtained at such great expense, is now ours to command. I must congratulate all those involved in contributing to this masterful coup de main.
The new cipher is, beyond doubt, the most ingenious and the most secure in the world today and messages enciphered using its rotary mechanism will frustrate the efforts of the most ardent cryptanalysts for years to come. In the meantime our own efforts must go to the frustration of those who would develop rival machines. Given the history of M. Babbage, a man for whom the word dilettante was invented, a campaign of gentle sabotage may be sufficient to prevent his own machine from reaching completion.
It is with some sadness that I bring this letter to a close. I have enjoyed the battle of wits in which we have been engaged, and feel a little sorrow that with the completion of the Turning Machine the battle must draw to a close. Yet who knows, perhaps another time we will engage once more in a war of the mind, another Cryptographic Challenge, with those ingenious and dedicated English mathematicians.
Vive la France!

Cipher:

- Of course our Turning Machine is a variant of the infamous Enigma machine cracked by the Bletchley code breakers. If we had not given you any of the settings of the machine you would have had 36! 36! 36!/18! (or about 8x10^108) possibilities to try. Don't even think about it . Once you cracked the RSA encypted rotor settings you were left with only 500,000 settings to play with and a factor of four in deciding which way the rotors turned. In fact the RSA was critically weakened by the fact that the numbers we enciphered (in the range 0-35) and the exponent 7, were too small for the modulus we chose. Since 35^7 is less than the modulus the encryption did not alter the order of the numbers and merely sorting them in increasing order would have cracked the RSA cipher.

Sponsored by:

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