University of Southampton National Cipher Challenge Solutions

Message 7 Plaintext:

Cover Note:

My dear friends,
I enclose an ancient text that I have been studying that you may well find of interest. If you are unable to translate it you will find that Mr Holmes of Baker Street will be able to help you out.

Yours as ever, B.

Attachment:

I am pleased to say that the Vigenere cipher is not as secure as our French friends seem to believe. I have spent some time studying the method and I am sure that I have devised a way to prise open this French enigma. The key, if you will excuse the intolerable pun, lies in identifying the period of repetition of the cipher, which one can deduce by analysis of repetition patterns in the enciphered text. The length of the keyword may be revealed as a common factor of the periods of such repetitions. Of course all my research will avail us nothing without more information, so I must beg your assistance again, my dear Countess, in obtaining more intelligence from your extensive circle of contacts.

The cover note, from the Babbage to his friends, is enciphered with a key phrase cipher using the phrase “Lord Melbourne”, which refers to William Lamb, the 2nd Viscount Melbourne (1779-1848). A Whig, he was Prime Minister briefly in 1834, and again from 1835 to 1841. His wife, Lady Caroline Lamb, had a scandalous affair with the poet Lord Byron (whom she memorably referred to as "mad, bad and dangerous to know"). Melbourne and his wife separated in 1825. His friendship with Mrs. Norton led to a civil court case satirized by Charles Dickens in The Pickwick Papers. When the young Victoria took the throne in 1837, Melbourne carefully guided her through the politically difficult early years of her reign. One of the successes of his government was the introduction of the penny post.

http://65.107.211.206/history/pms/melbourne.html

http://dspace.dial.pipex.com/town/terrace/adw03/peel/mel.htm

http://www.englishhistory.net/byron.html

Sponsored by:

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

University of Southampton National Cipher Challenge Solutions

The attachment describes Babbage’s work in attempting to crack the Vigenére cipher, widely believed at the time to be invulnerable. This cipher is discussed extensively in Chapter 2 of Simon Singh's The Code Book. In truth Charles Babbage discovered how to break this cipher, probably around 1854; however, he did not publish his method, possibly to encourage our then enemy Russia to continue to use it insecurely during the Crimean War (1854-56). The cipher was again broken in 1863 by Friedrich Kasiski, a Prussian, who published his discovery and got the credit for it, while Babbage's contribution remained largely ignored, as in the following otherwise informative source:.

http://www.trincoll.edu/depts/cpsc/cryptography/vigenere.html

The remark about Holmes is an anachronism, but refers forward to “The Adventure of the Dancing Men” in which Holmes and Watson encounter a cipher based on pictograms. This inspired our (not entirely successful) experiment with the hieroglyphs provided by the WebDings font.

University
of Southampton

Sponsored by:

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