

University of Southampton National Cipher Challenge Solutions

Message 8 Plaintext:

Cover Note:

By Hand

My Dear Mr. Babbage,

Real progress with our campaign I believe. The enclosed message was enclosed in a diplomatic communique and seems to betray the location of the stolen diagrams, though my friend has reason to believe that the message itself is not of French origin. If the treacherous French government are involved in this affair then I fear we must be even more careful. We should use the French cipher ourselves. If we use a keyword longer than the three letters they customarily seem to use then our letters should be safe.

Yours respectfully, L



Attachment:

Todgers's Boarding House

Billingsgate

London

Sir,

It is with pleasure that I accept your offer to discuss the value of the material concerning the English encryption engine on behalf of my Master, CD. As you can see I have moved from Southampton to an address in London and suggest you should meet me there at noon a week on Wednesday. Please come alone, as I fear the material is, shall we say, inflammable. It would be most unfortunate if, as a result of an attack of nerves, I were to knock over a lantern, or perhaps drop a lighted cigar in the vicinity of the stock of chemicals I have stored here. (Chemistry is such a pleasant diversion for the curious mind, and with so many fascinating and rather pleasing applications in the modern world, I'm sure you will agree.)

Of course the pleasure in such a transaction is necessarily mutual, and I hope that, all unpleasantness avoided, I will be able to satisfy your curiosity concerning Prof. Babbage's device, and you will be able to satisfy my master's need for currency. As a gentleman I am sure he felt unable to discuss terms with you, but as his faithful servant I must of course endeavour to arrive at an agreement favourable to him. I trust we understand one another and that our meeting will indeed be a pleasure for us both.

Please reply in the usual fashion

Yours, E.S.



Sponsored by:

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

University of Southampton National Cipher Challenge

Solutions

Cipher:

- Covering note: keyphrase substitution with keyphrase Charles Dickens
- Attachment: English text in a period 3 Vigenere blocked to reveal that it had period 3. We also added a lot of repetition to the text (note the peculiar use of the word “pleasure” and its derivatives throughout the text. The keyword was IBM.

Todgers's Boarding House appears in Martin Chuzzlewitt by Charles Dickens and was near The Monument. (This striking landmark commemorates The Great Fire Of London, a tragedy with the unexpected benefit of chasing out the plague.)

This extract gives you an idea of what a pleasant establishment it was!

“..M. Todgers's Commercial Boarding-House was a house of that sort which is likely to be dark at any time; but that morning it was especially dark. There was an odd smell in the passage, as if the concentrated essence of all the dinners that had been cooked in the kitchen since the house was built, lingered at the top of the kitchen stairs to that hour, and like the Black Friar in Don Juan, 'wouldn't be driven away.'...”

You can visit the monument today. More information is at

http://www.cityoflondon.gov.uk/leisure_heritage/architectural_heritage/monument.htm

In addition to their great literary value, the novels of Dickens give a graphic picture of English life during the middle of the 19th century. An excellent place to start finding out about Dickens is:

<http://www.lang.nagoya-u.ac.jp/~matsuoka/Dickens.html>

The attachment (in English, like the covering note!) is enciphered using a period 3 Vigenere cipher; the ciphertext is grouped in blocks of 3 to help the deciphering process. The keyword IBM is the name of one of our sponsors, whose computers embody many of the ideas about calculating machines first developed by Charles Babbage. Click on their logo on our home page to find out more about IBM.



Sponsored by:

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