Register for the competition on the form at http://www.cipher.maths.soton.ac.uk/registration

National Cipher Challenge 2009, part 7A

July 1st 1837

My Dear Miss Lovelace, I have been studying your notes on your Father's Engima. As you suggest it seems likely that it has been encrypted using a simple Vigenere cypher, and I hope you will not object if I suggest using my own methods to discover the length of the keyword by analysing the frequency of repeating sequences in the text. I suspect that your father, who was not a truly sophisticated user of cyphers, will have restricted himself to a key of length two or perhaps three and this should render the exercise relatively simple.

Mr. Cocking has organised the auction for our machine to be held at a secret location early next month. He believes that his subterfuge remains undetected and is confident in the ability of our constabulary to arrest the miscreants. However he did obtain the enclosed copy of the most recent missive from Monhier and his cronies to their masters in France, and he has asked if we would decypher the text for him. He would like some assurance that his plan is likely to work before embarking on the final stage.

Having analysed the text myself I am convinced that this message is itself encrypted using a Vigenere cypher though it has been cleverly disguised, as I am sure you will discover for yourself. Given what we have recently heard I am slightly puzzled that Monhier is still using such an elementary device. I had expected him to use the Jefferson cypher – Mr. Cocking was emphatic that he saw a Jefferson cylinder in the possession of the conspirators at their last meeting. Perhaps they reserve this for matters of top secrecy. I hope that we will have the opportunity to test the Turning Engine on at least one of their Jeffersonian communications before this adventure ends.

With much affection, Babbage

National Cipher Challenge 2009, part 7B
June 23rd 1837

My brothers I must keep this message short. Mr. Cocking has arranged the auction for the Turning Engine for July Twelfth and we urgently need additional funds to arrange the purchase. I am told that there are many bidders for the device and, having studied it in some depth over the last few months I can see why. It acts as a giant automated Jefferson cylinder and may be used to automate an attack upon it by generating large numbers of candidate decryptions and using a dictionary of cribs to test them. It may be that the days of the Jefferson wheel are numbered, though I am inclined to trust it for the moment.

Regarding the Jefferson cypher itself the new cylinder arrived from the embassy by courier late last night and I was most impressed by the apparently completely random arrangement of the characters on the wheels, though the fact that each wheel was identical to exactly one other really did seem an unfortunate weakening of the device. Nonetheless, together with the various orderings for the wheels on the axis the number of combinations possible are beyond discernment even by the Turning Engine without some other weakness in the implementation of the cypher and I will use it for all future communications. M