University of Southampton National Cipher Challenge Solutions

Solution: Message 14

Plaintext:
Top Secret!

Dear L and B,
This new RSA cipher is most ingenious. To understand the security of the RSA I have spent many hours labouring at the factorisation of the number which B challenged us to factor. It is a devil of a job and I have failed miserably which augers well for the security of RSA. Deciphering a message without the prime factorisation of the public key will be a Herculean task.

Of more immediate import, I believe I have found at last a method by which the strength of the Turning Machine may be turned upon our enemies. While the machine is capable of great secrecy in communications, its reliable operation is dependant upon certain elementary precautions which were not documented in the designs, and these may well have escaped the attention of its copiers. From L's very latest intelligence it seems that the French machine incorporates both the wheels and the reflector from our design. While this provides the advantage that the Turning machine can both encrypt and decrypt a message from the same settings I now realise that it also incorporates a small weakness in the resulting cipher. By virtue of its design the reflector ensures that no letter is ever encrypted as itself. As we recently noted the ability to match a known fragment of plaintext to the correct position in its ciphertext gives us much information about the cipher used. Whilst the Turning machine is far more sophisticated than the Playfair cipher if we could find a fragment of plaintext corresponding to a given ciphertext we might use this weakness to identify exactly which part of the enciphered message matches the fragment. In this happy situation it may be possible, using the ideas of the Countess, to write instructions for the Analytic Engine to emulate the Turning machine. Asking it to encipher the fragement in all the possible ways and matching these with the known encryption we may be able to identify which of the many possible wirings for the rotors and reflectors the French have used. With this knowledge it should be possible to decrypt the rest of the cipher text. I now believe that finding an effective decipherment process is where we should devote our efforts. It would provide a major benefit to Her Majesty's Government if the French were to rely on the security of a broken cipher for their deepest secrets.

Yours etc W.

P.S I have enjoyed studying the fascinating case of Mr Beale's lost treasure. Mr. Beale's ingenious use of the Declaration of Independence demonstrates that a simple idea for a cipher can render a very strong encryption. I have my own idea for a variation on this method which would pose a monumental task for those inclined to decipher it. Of course it would be a monumental disaster should the key be too easily discovered.

Sponsored by:

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

University of Southampton National Cipher Challenge Solutions

Cipher:

- One of the joys of extending our alphabet to the thirty six alpha-numeric characters is that 36 has so many more factorisations than 26. On this occasion we used the factorisation 36=9.4 to yield a Playfair rectangle based on the key "The Beale Papers". Could it been made any more explicit that the in the clue from the Countess? "Perhaps we should turn to "The Beal Papers" for inspiration?

Notes:

- The story of the Beale treasure and the enciphered documents describing its location is told in Simon Singh's "The Code Book". The cracking of the first Beale cipher is described there, as is the devilish book cipher used to encode it. This cipher can defeat all but the most determined cryptanalyst, since the key to deciphering it lies in making a lucky, or informed, guess at the source document used to construct the cipher.

- The weakness in the Cryptographic Engine is strangely similar to a weakness in the Enigma machine, which could be exploited by Alan Turing and his fellow cryptanalysts in their cracking of the cipher. They, together with the GPO engineer Tommy Flowers designed and built programmable computers to run a search for the Enigma settings. You can find out more about their exploits by visiting the home of our sponsors at Bletchley Park:
  http://www.bletchleypark.org.uk/

- The Bletchley machines are now credited as the world's first ever electronic computers, but the honour for designing the first ever fully programmable computers goes to Babbage and Lovelace. Babbage's contribution was the mechanical design of the Analytic Engine, and Lovelace worked on the language used to programme it. The modern programming language ADA is named in honour of her, and the Science Museum has a permanent exhibition dedicated to the work of these pioneers. You can read more about it at:
  http://www.sciencemuseum.org.uk/collections/exhiblets/babbage/babbwork.asp

University of Southampton

Sponsored by:

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