University of Southampton National Cipher Challenge Solutions

Solution: Message 13

Plaintext:

Dear Friends,
it is with some shame that I now realise how foolish I have been. The significance of the strange laboratory at Todgers should have been obvious our presumption that the recovery of our plans terminated that most unpleasant incident will I fear haunt us in the days and weeks ahead. But allow me to explain. At a recent meeting of the Royal Society a colleague returning from France outlined to me the work of M. Daguerre on the fixing of images upon glass plates. His process, similar in spirit to that employed by our own Mr. Talbot is, with imminent support from his own government, close to commercial success. The description of the process, inasmuch as it is known outside a close circle, involves the very compounds discovered in the boarding house. Given the French interest in our designs and their expertise in the photographic arts it would be too much to assume this a coincidence. I fear that already the copied designs are in foreign hands. On a more optimistic note I have made a most remarkable mathematical discovery. It will allow us to develop a new cipher which does not require the secret distribution of encryption keys rather the converse one may publish the encryption key freely keeping secret only the key to deciphering. I call this new method the remarkably secure artifice cipher. Messages are first encoded as numbers using some agreed mechanism; these encoded messages are then enciphered by exponentiating them to the seventh power modulo the product of two prime numbers using the remarkable results of Fermat one may decipher the messages by another exponentiation. However, without knowledge of the two primes, the exponent is extremely difficult to determine given the difficulty of factorising the large integer. One may publish the product secure in the knowledge that the primes themselves are concealed, though it must be said that, given the resources, the problem of factorisation itself may yield to the powers of the analytic engine were it ever to be built. By way of illustration of the security of this method you may wish to see if you can find the two prime factors of 316x6924169361x1.
We have now used this Playfair cipher twice and I was minded to suggest xthat we should perhaps change to another method but all this reflection on numerical factors brings to mind a further natural variation of our current cipher. Perhaps you might respond using it.
Yours as ever,

Br

Cipher:

- A Playfair cipher based on a 6x6 grid encoding the alphabet a-z together with the numerals 0-9. There is no keyword, but the grid reads

```
01234N
OPQRST
UVWXYZ
ABCDEF
GHIJKL
M56789
```

Sponsored by:

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

University of Southampton National Cipher Challenge Solutions

Notes:

- Daguerre's process for fixing photographic images on glass plates was sponsored by the French government and became one of the first successful photographic systems in the world. In the UK the Fox Talbot process was developed around the same time. You can find out more about the history of photography at

- http://www.rleggat.com/photohistory/

- The really secure artifice cipher described here is a version of the discrete logarithm cipher devised by Rivest, Shamir and Adelman to overcome the classical problem of distributing encryption keys securely. In fact the method had been previously discovered independently by the cryptographers at the UK intelligence agency GCHQ. They have a web site at www.gchq.gov.uk. The key fact underlying RSA encryption is that it is easier to compute a^x mod n than it is to solve $a^x=b$ mod n, given that you know a,b and n. To make the code usable it is necessary to have a method of solving the equation given some extra, secret knowledge. In this case the knowledge is the prime factorization of n, which is chosen to be the product of two primes. The final ingredient is a theorem due to Fermat, famous for his conjecture, Fermat's last theorem, which was finally proved by Andrew Wiles. You can find a good account of this material in a presentation by Bruce Murray of Philips Electronics:

- http://www.maths.soton.ac.uk/staff/Niblo/MA107/Murray

University of Southampton

Sponsored by:

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