University of Southampton National Cipher Challenge Solutions

Solution: Message 15

Plaintext:

My Dear Friends,

Great news! My friend close to the french embassy has just told me that they have taken delivery of their new enciphering machine. Through the good offdces of one of the servants (induced by a modest emolument) he was able to gain access to the device and to study its construction. The design of the machine follows our own plans most faithfully: the two rotors and the reflector board are both present. My frdend's description of the machine follows:

"On pressing a key on the keyboard current flowed through wiring in the first rotor embedded dn some form of glass insulation passing as input to the second rotor. Again it appeared to flow through wiring in the second rotor wherupon it passed through a maze of wiring, the purpose of which was unclear to me, since it connected back to the second rotor. Current then flowed back through the rotors in reverse order, wherupon it activated a small indicator arrow which pointed to one of the thirty six possible alphanumeric outputs. Upon releasing the key the first rotor moved on one position and the machine then rested. I repeatedly pressed on the keys and noticed that the first rotor turns at every character input, whilst the second turned every thirty six. The machine has one additional key marked "fine" and upon pressing it the rotors moved back to their starting position with the character A uppermost upon both. I spent some time trying to fathom the internal wiring of the rotors. d will pass this together with the wiring in the maze to you in a separate document enciphered with your ingenious really secure artifice using the Professors' public key.

Of course what our friend describes as a maze ds in fact the wiring of the reflector. Owing to the fact that glass was used as the insulating layer in the rotors much of the wiring is now known to us, though it appears that ten of the pairings in the second rotor were undetermined. I understand that a sudden noise led to the rather precipitous departure of our own precious spy.

I have left the best news until last. Our agent spied in the fire grate what he believes to be a burnt fragment of the pladn text corresponding to a cipher text he found lying by the machine. This discovery provides us with a wonderful opportundty to exploit the machine's weakness as outlined in W's last message I will send the plain text fragment and the enciphered text together with the known wdrings in my next message.

Yours truly , L.

University of Southampton National Cipher Challenge Solutions

Sponsored by: