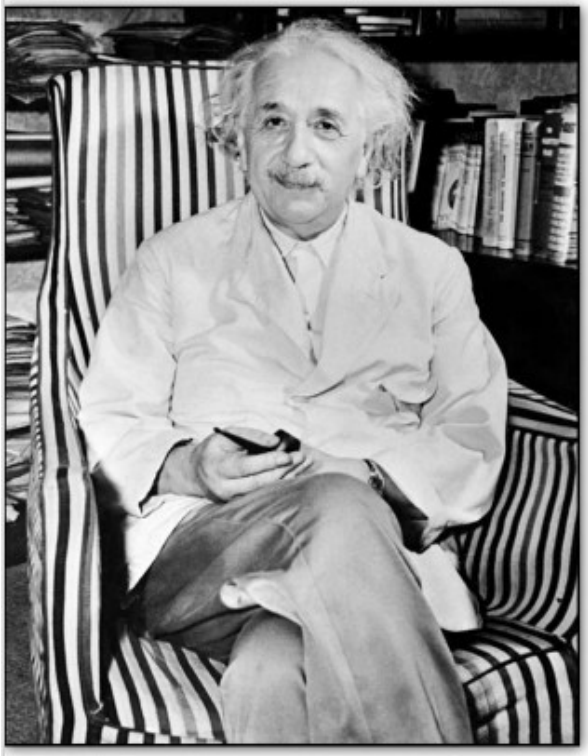
THE CHALLENGE CIPHER

In 1953, Byrne published *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland*. The last chapter was all about the chaocipher. It described the history of his invention and his attempts to offer it to government departments. The chapter included twenty-three pages of plaintext and corresponding ciphertext encrypted with the chaocipher. The book ended with a challenge cipher—the following two lines of text and an offer of five thousand dollars to the first person who could decipher them.

HCYXR XRZWN TXOAI MOWEK PSIXP CPOLZ JJMXS CYLRF
UKMYF DPRCOARREU

DGYQH TQCFJ NGNQA DTLBU MYVDM ULXIW XNVHG OIK



Byrne wanted people to try to crack his code so he could prove it was indecipherable. He sent a copy of his book to Albert Einstein and suggested it "might

There is no record of Albert Einstein responding to Byrne's cipher challenge, but he must have read it because he marked paragraphs in his copy of Byrne's book.

be of scientific interest" to the renowned mathematician. For nearly sixty years many cryptologists puzzled over the nineteen blocks of letters, but none solved the challenge.

The Answer

John Byrne died in 1960 with his device lost and his principle still undiscovered. His son knew how his father's system worked, and he constructed a crude model of the original device from cardboard and wooden tiles. But he also died without disclosing the key to the cipher. Fortunately for code analysts, his widow donated the little model as well as all his papers on the cipher to the National Cryptologic Museum in 2012. The challenge cipher was never cracked, but its secret was revealed.

The chaocipher is a complex substitution cipher. Byrne's device consists of two different alphabet wheels, one for the plaintext and one for the ciphertext. The wheels connect so that as one rotates clockwise the other turns counter-clockwise. Every time a plaintext letter is matched with a ciphertext letter, the two letters are moved to new slots in the wheels and all the other letters shift one space. This process makes the code unique every time it is used.

Byrne was right when he said a ten-year-old could encrypt with his machine. What about his other claim—that the messages would be "absolutely indecipherable" by anyone except the intended recipients? Cryptographers are still working to see if that is true.