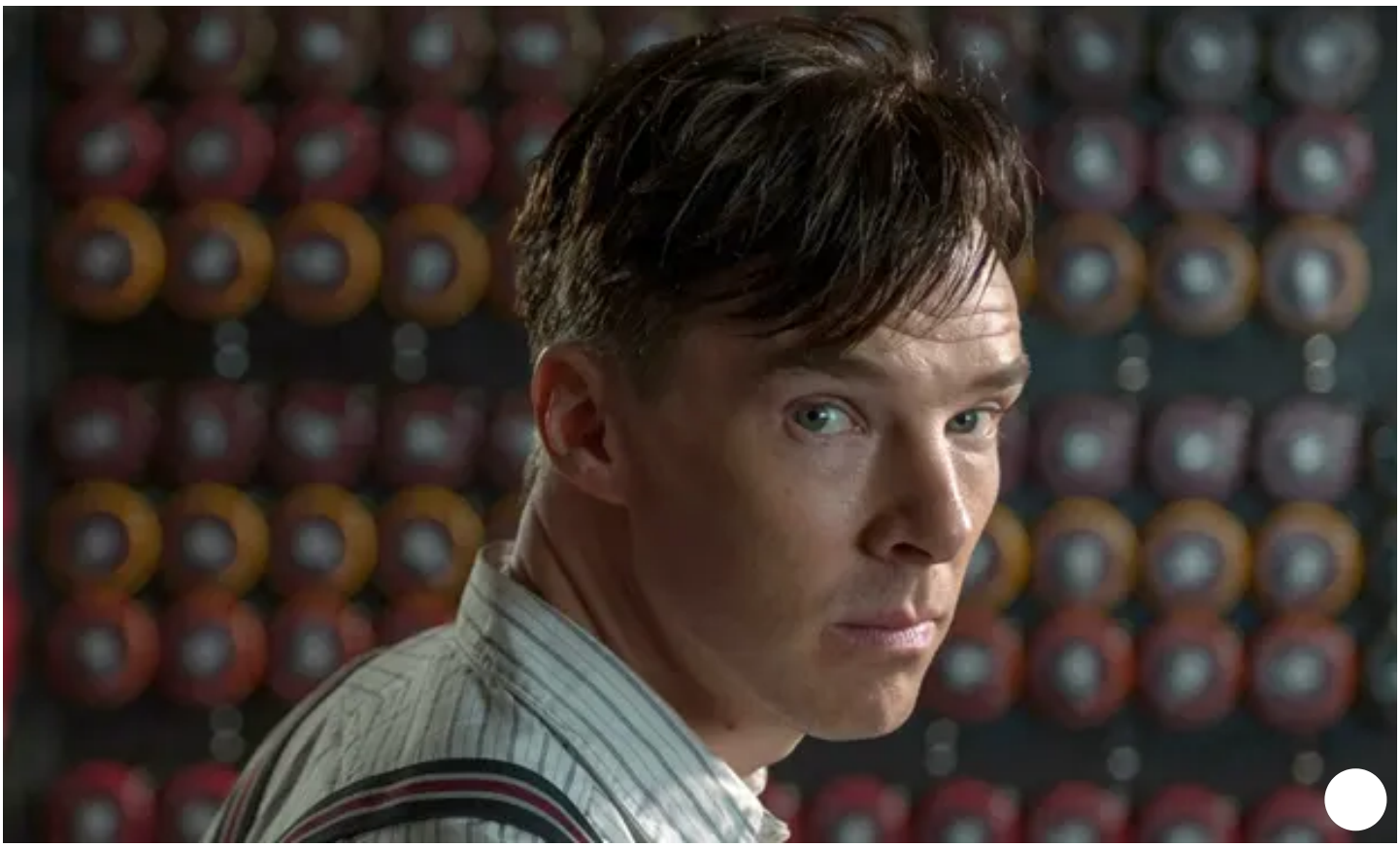
The Guardian



Top 10 codes, keys and ciphers

Kevin Sands, author of The Blackthorn Key, picks his favourite keys, codes and ciphers throughout history, from the Caesar shift to the Enigma machine

Kevin Sands

Thu 10 Sep 2015 08.30 BST

If knowledge is power, then the key to power lies in unlocking secrets. For thousands of years, ciphers have been used to hide those secrets from prying eyes in a cat-and-mouse game of code-makers versus code-breakers. These are some of history's most famous codes.

1. The Caesar shift

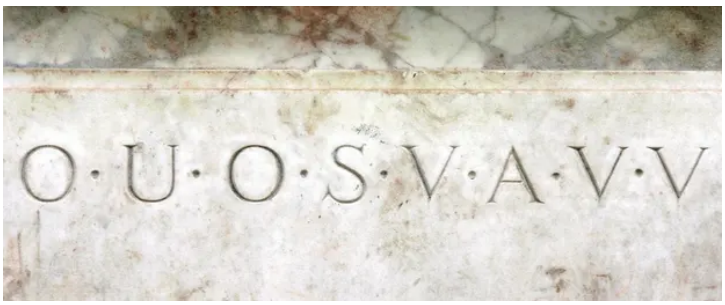
Named after Julius Caesar, who used it to encode his military messages, the Caesar shift is as simple as a cipher gets. All you have to do is substitute each letter in the alphabet by shifting it right or left by a specific number of letters. Today, we can break this code in our sleep, but it took ancient codebreakers 800 years to learn how to crack it - and nearly another 800 years to come up with anything better.

2. Alberti's disk

In 1467, architect Leon Battista Alberti described a curious device. It was a disk made up of two concentric rings: the outer ring engraved with a standard alphabet, and the inner ring, engraved with the same alphabet but written out of order. By rotating the inner ring and matching letters across the disk, a message could be enciphered, one letter at a time, in a fiendishly complex way.

3. The Vigenère square

This 16th-century cipher uses a keyword to generate a series of different Caesar shifts within the same message. Though simple to use, this method of coding resisted all attempts to break it for over 300 years, earning it the nickname "*le chiffre indéchiffrable*": the undecipherable cipher.



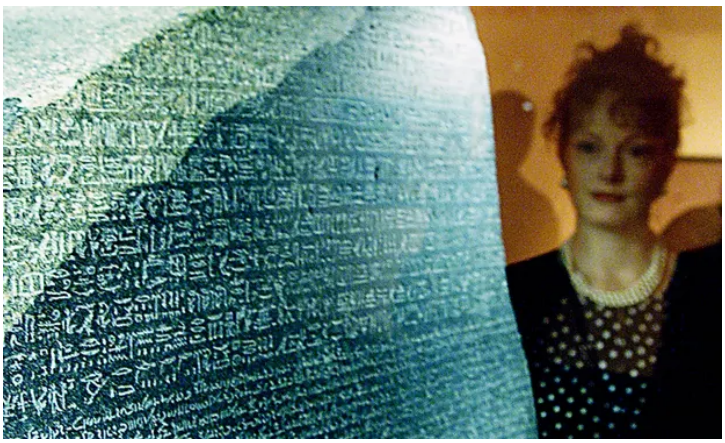
The ancient code etched into the Shepherds' Monument in the grounds of Shugborough Hall. Photograph: PR

4. The Shugborough inscription

On the Shepherds' Monument in Staffordshire's Shugborough Hall, an unknown craftsman carved eight mysterious letters - OUOSVAVV - between two other letters, D and M. Thousands of would-be code-breakers, including Charles Darwin and Charles Dickens, have searched without success for the meaning behind this inscription. More recently, some have claimed this cipher points to the hidden location of the Holy Grail.

5. The Voynich manuscript

This extraordinary codex from the 15th century is filled with bizarre illustrations and written in a unique alphabet that no one has ever identified. To this day, we're not sure if the manuscript contains valuable secrets, the ravings of a madman, or is simply a centuries-old hoax.



Hieroglyphs on display at the British Museum. Photograph: Garry Weaser/PR

6. Hieroglyphs

When no one is left who knows how to read a language, it becomes a secret code of its own. That's exactly what happened with the hieroglyphs of ancient Egypt. These beautiful, iconic characters baffled linguists for centuries, until Napoleon's troops discovered the Rosetta Stone, which allowed scholars to match the hieroglyphs with known Greek words, giving us the key to understanding the language and culture of one of the greatest civilizations in history.

7. The Enigma machine

This infamous Nazi coding device may have looked like a typewriter, but hidden inside was the most complex cryptographic system of rotors and gears yet devised. Allied code-breakers - including British genius Alan Turing and his team at Bletchley Park - worked day and night for

years, building machines called *bombes* to crack the Germans' military messages. Their efforts are estimated to have shortened the war by as much as two years, saving millions of lives.

The Enigma coding machine that was used by the Germans during the second world war. Photograph: Ian Waldie/Getty Images

8. Kryptos

In 1990, the CIA teased its own analysts by installing a sculpture with a complex four-part code on the grounds of its Langley headquarters. To date, only three of the four parts have been solved. If you're looking for a job as a codebreaker, try cracking the last one - as long as you don't mind getting a visit from the Men in Black...

9. RSA encryption

For most of our history, ciphers required both coder and decoder to have the same key to unlock it. But in the 1970s, researchers at the Massachusetts Institute of Technology found a way to encode messages safely without sharing the key beforehand. Called *public-key cryptography*, this type of security protects most electronic communications today. It's not known if it can be cracked, but if you figured out a way, you'd own pretty much everything on the internet!

10. The Pioneer plaques

Our final code is one we sent to others - and I really mean *others*. Attached to the Pioneer 10 and 11 spacecraft, these gold-aluminium plaques depict us, our solar system, and our location in the universe, and are encoded with one of the properties of hydrogen as the key to decipher our message. Travelling through the vastness of space, it's unlikely any alien civilisation will discover these probes. But if they do, we'll have passed on to them our love of knowledge - and the secrets we use to hide it.

Kevin Sands is the author of The Blackthorn Key, about a young apothecary called Christopher Rowe who must crack a code in order to thwart a murder. Find out more about Kevin Sands and his book on his facebook page. Buy The Blackthorn Key at the Guardian bookshop.