Unlocked: The hidden love note on the grave of America's first crypto power-couple

BAAAB AABBB AAAAA BAAAA AABAA ABBAB ABBAA BAAAA AABAA AAABB AAABB ABAAA BAABA

Iain Thomson in San Francisco
Sat 20 Jan 2018 // 08:58 UTC

SHMOOCON Among the 400,000 graves at the Arlington National Cemetery – a solemn US military graveyard in Virginia – lies the final resting place of cryptography pioneers William and Elizebeth Friedman.

And hidden in code on their tombstone is a touching tribute from a wife to her husband. A code that's only now just been cracked, decades after it was engraved in the cool stone.

William, born 1891, and Elizebeth, born a year later, married in 1917.

Among many cryptological feats, the couple trained America's first cadre of code-breakers after developing an interest in cryptography while examining the so-called Baconian cipher – developed by the British Elizabethan cryptographer Sir Francis Bacon.

William invented the term cryptanalysis, and pretty much broke the key Japanese World War II cipher Purple – so named because transcripts were kept in purple folders.

Meanwhile, Elizebeth was America's first woman cryptanalyst, and encouraged her husband to pursue cryptography. She also worked with the US government to break the communication codes of rum runners during the prohibition era, and helped crack Germany's Enigma machine ciphers during World War II.

In 1969, at the age of 78, William died, and was buried at Arlington. His wife designed his gravestone, consisting of a pair of crossed flags – the symbol of William's military signals unit – and one of his favorite phrases, "Knowledge is power," a quote attributed to Sir Francis.

The same phrase appeared in code in the graduation photograph of the 1918 code-breakers class the Friedmans taught, in which some of the students faced sideways and others look

straight at the camera. The direction of their faces spelled out a phrase using the <u>Baconian cipher</u>.

Smart ... Part of the crypto-class graduation photo in 1918

Sir Francis came up with a code whereby every letter in the alphabet could be represented by a group of five 'a' or 'b' letters. For example, N is 'abbaa', and O is 'abbab'. In the class photo, by converting the direction of each person's face – ahead or to the side – as an 'a' or 'b', and running it through the cipher, the class lineup spelled out.. KNOWLEDGE IS POWER.

Shortly after moving to Washington DC, cryptographer Elonka Dunin paid a visit to the Friedmans' grave. Elizebeth was buried alongside her husband after her death in 1980, and her name was added to the tombstone. Dunin noticed [PDF] something odd. The phrase "Knowledge is Power" chiseled into the stone using a mix of serif and sans-serif letter designs.

If you assume the serif letters represent a 'b', and the san-serif characters are each an 'a', the phrase can be converted into 'babaa aabab aabab', if you discount the final letter r.

Running that sequence through the Baconian cipher spells out WFF, William's initials. Dunin <u>told this year's Shmoocon computer security conference</u> in Washington DC on Friday that she believes this is a hidden note to William from his wife when she designed his gravestone.
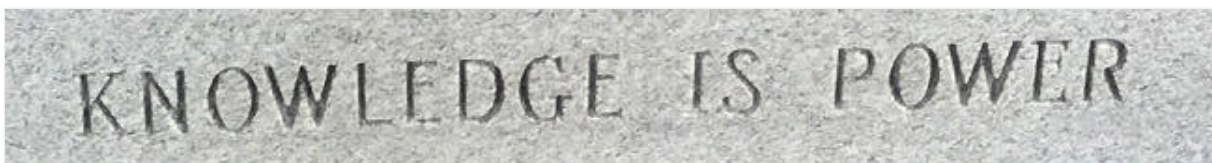
Encoded ... 'Knowledge is power' written on the couple's tombstone

The pair had a reputation for this sort of thing. They wrote a book together in 1957 called The Shakespearean Ciphers Examined, which thoroughly debunked the theory that Sir Francis wrote many of the Bard's plays and left coded clues in his manuscripts.

On page 257 of the book, in the bottom paragraph, the authors bolded up certain letters and left other untouched. When translated using the Bacon's cipher, the message read: "I did not write the plays, F Bacon."
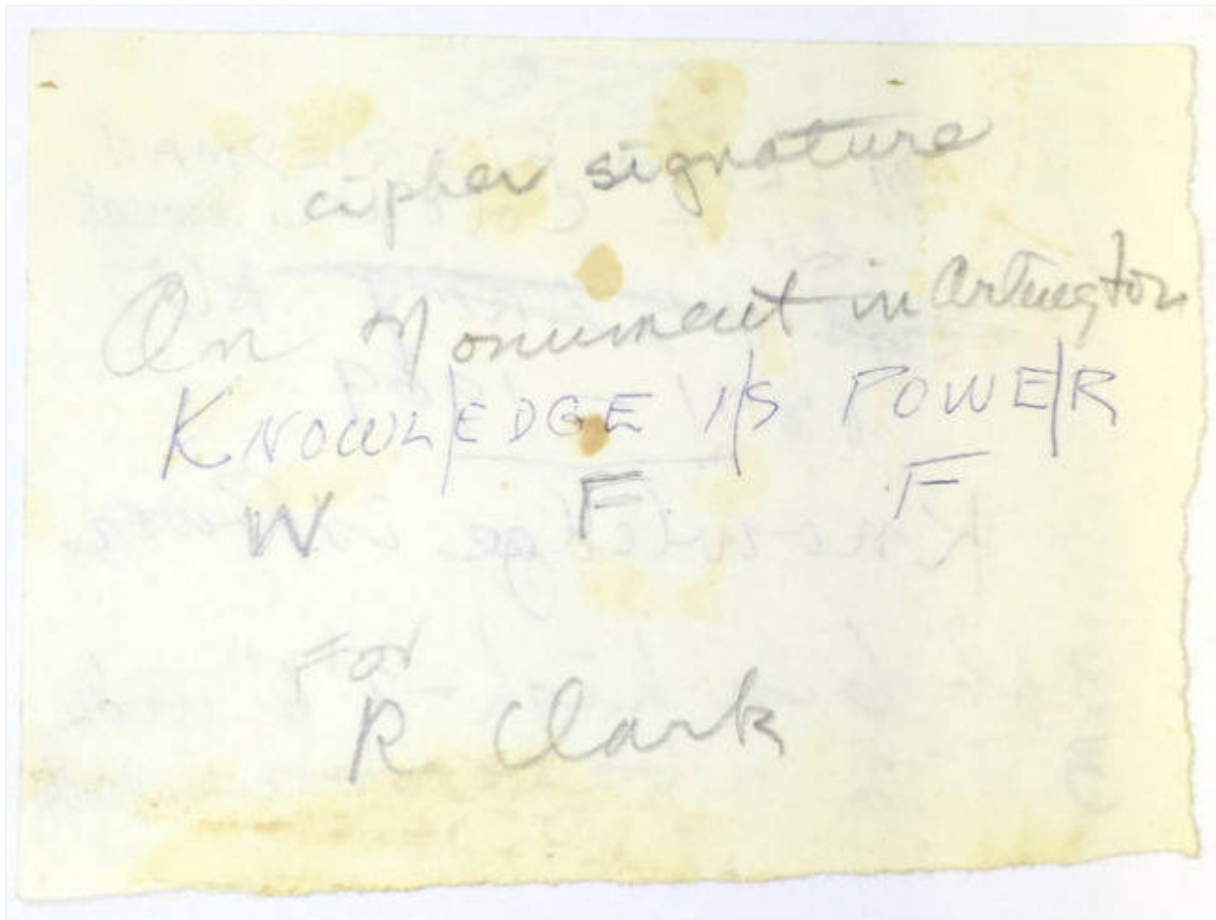
Confirmation ... A note planning the grave's design

The final confirmation of Dunin's theory about the tombstone came after an examination of the Friedman papers in the Marshall Library, where a note by Elizebeth was found indicating how the WFF message was generated – by breaking up "Knowledge is Power" into three letters using Sir Francis' algorithm.

All like all mortals, cryptographers die – but their hidden notes live on unbroken for decades, if not forever. ®