# Famous cryptographers' tombstone cryptogram decrypted

22 JAN 2018 17


Previous: California to make it harder for your license pl... Next: Uber hit with criticism of "useless" two-factor aut...

by Paul Ducklin

*This article was inspired by Elonka Dunin's Schmoocon 2018 presentation about this fascinating topic. Dunin's original paper, **Cipher on the William and Elizebeth Friedman tombstone at Arlington National Cemetery is solved**, was published in April 2017.*

*Hat tip to Iain Thomson at The Register for writing up Dunin's talk at Schmoocon.*

William and Elizebeth Friedman were a husband-and-wife team who were amongst the very first US government cryptographers.

Their careers started just before the US entered World War One in 1917, and continued through and beyond World War Two.

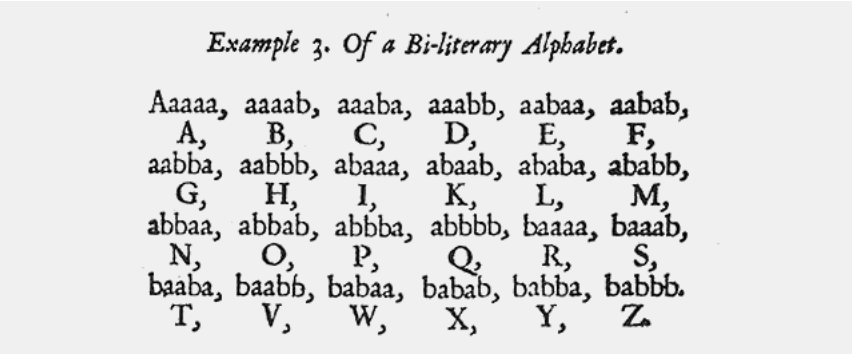
William died in 1969; Elizebeth (apparently, her mother liked the name *Elizabeth* but but not *Eliza*, and chose the unusual spelling to prevent unwanted abbreviations) in 1980:


William was an army Colonel, so their joint tombstone is in the Arlington National Cemetery, just across the river from Washington DC, the capital of the United States.

Of course, the tombstone didn't always look like the picture above – it was commissioned by Elizebeth herself after she was widowed, so her name was added only after her own death more than a decade later.

The phrase at the bottom, KNOWLEDGE IS POWER, was a favourite sayings of William's, so much so that he encoded it into the graduation photograph of the army cryptography course that he and Elizebeth taught in 1918:

The code used here is what's known as a Bacon cipher, essentially a 5-bit binary encoding of the letters of the alphabet:



*Example 3. Of a Bi-literary Alphabet.*

| | | | | | |
|---|---|---|---|---|---|
| Aaaaa, | aaaab, | aaaba, | aaabb, | aabaa, | aabab, |
| A, | B, | C, | D, | E, | F, |
| aabba, | aabbb, | abaaa, | abaab, | ababa, | ababb, |
| G, | H, | I, | K, | L, | M, |
| abbaa, | abbab, | abbba, | abbbb, | baaaa, | baaab, |
| N, | O, | P, | Q, | R, | S, |
| baaba, | baabb, | babaa, | babab, | babba, | babbb. |
| T, | V, | W, | X, | Y, | Z. |

Bacon used A and B, but you can replace them with 0 and 1 and treat the codes as binary numbers.

Bacon's idea was to hide the As and Bs (or zeros and ones) in regular printed text by using different faces, weights, styles or sizes for successive characters, or by other minor differences in a picture or diagram.

In the graduation photo above, the As and Bs were encoded by whether the person was looking directly at the camera, or to one side.

Below, I've done it by mixing mixed two typacefaces, *American Typewriter* (the one with the serifs, or flourishes, on each letter) and *Arial Black* (with clean edges and uniform stroke widths):

```
PAUL DUCKLIN SOPHOS NAKED SECURITY
```

Marked up with colours, the differences are easier to see:

```
PAUL DUCKLIN SOPHOS NAKED SECURITY
```

Spaced cleanly into fives, as required in the Bacon cipher, with black for Bacon's Bs and red for the As, we can easily decode it:

```
PAULD UCKLI NSOPH OSNAK EDSEC URITY

baaab abbab abbba aabbb abbab baaab

 S     O     P     H     O     S
```

## Bacon redux

Guess what?

The Friedmans originally met and married when they were working together on a project to investigate the many historical claims that Shakespeare's plays were written anonymously by some other author.

Sir Francis Bacon is one of the authors often proposed as "the real Shakespeare", allegedly on the basis of messages left behind – in the Bacon cipher, of course – in contemporary texts.

But the Friedmans published a definitive book in 1957, entitled *The Shakespearean Ciphers Examined: An analysis of cryptographic systems used as evidence that some author other than William Shakespeare wrote the plays commonly attributed to him*.

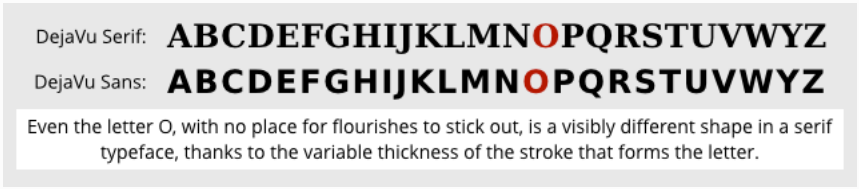
The book pretty much settled the matter: the Baconian theory of Shakespearean authorship was debunked for ever.

Fast forward to the twenty-first century.

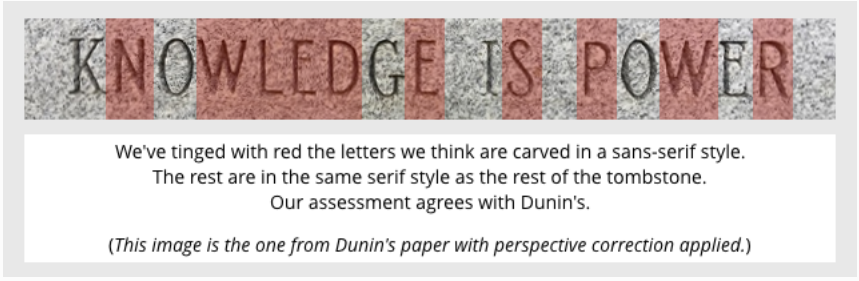
Elonka Dunin, a renowned video game creator and cryptographic historian, visited Arlington Cemetery to pay her respects at the Friedmans' grave, and her attention was quite understandably drawn to the words at the bottom of the tombstone:


If you were Elizebeth, you'd have squeezed a cryptogram in there, wouldn't you?

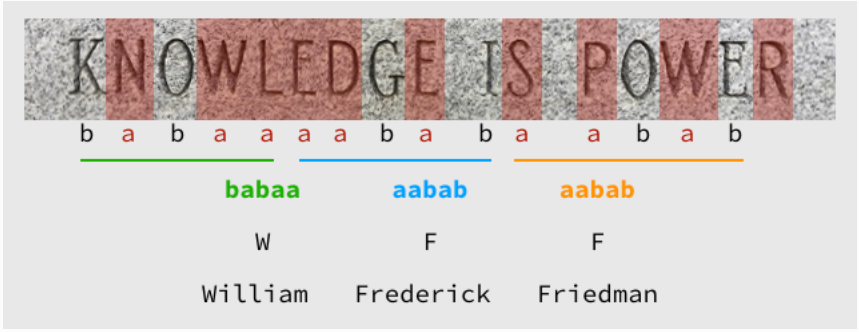
Look closely and you will see that some of the letters do not have serifs – the little flourishes that are obvious on the lines in letters such as K and G above – even though all the other writing on the tombstone is carved in a serif face.



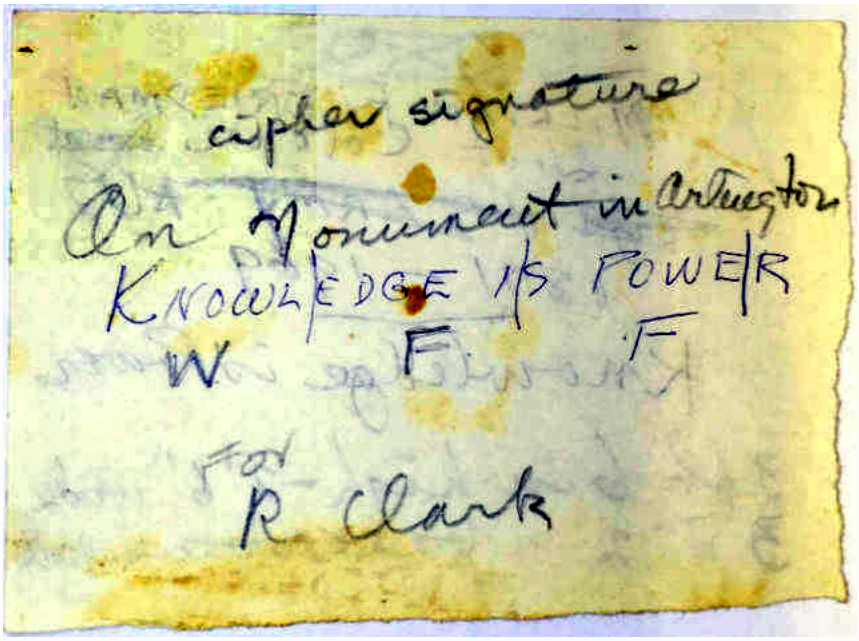

With a bit of care (the letter O doesn't have any lines to embellish, but is typically thinner at top and bottom in a serif face), you can make out a pattern on the tombstone:




The characters differences are subtle, at least in the low-resolution image here, but we agree with Dunin's assessment of how this comes out:

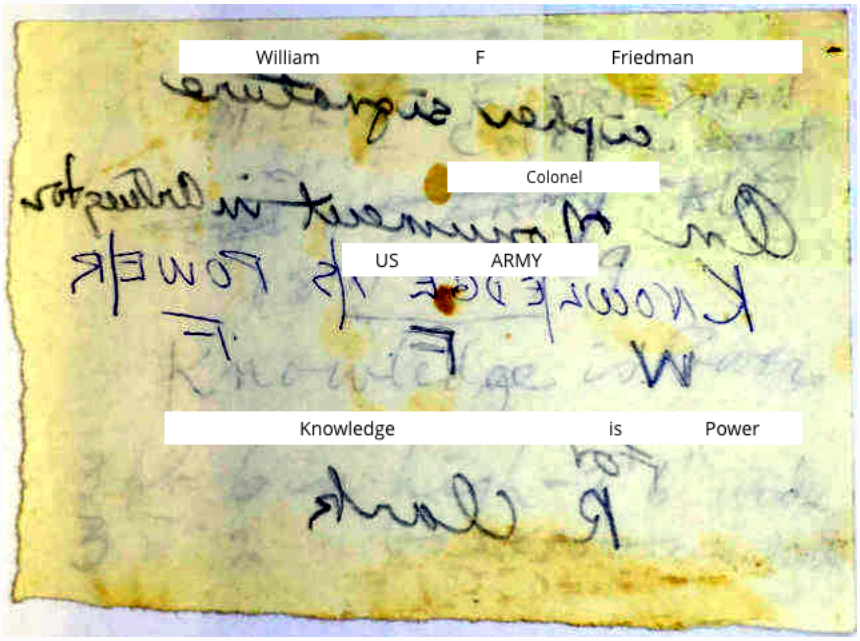



Dunin found additional evidence that Elizebeth planned this all along, and thus that there is no wishful thinking here, thanks to an image found in the Elizebeth Smith Friedman collection:




To make the image above a bit easier to read, we fiddled with the levels in the image, which is why it looks somewhat unnatural; however, that brought out some additional details.

Although the words KNOWLEDGE IS POWER have apparently been added in later in a different hand with what looks like a ballpoint pen, you can see that this paper note definitely relates to the tombstone design if you flip it over and read the other side:




Knowledge is power, indeed.

What a splendid memento!

**PS.** Can you make out any more of the text on the other side of the note? You can use the colour-tweaked version we have here, or try your own enhancements of the original from Dunin's paper. (We used GIMP's *Levels* operator and did a *Flip horizontally*.) What about the numbers at the bottom? We think we can see *3 ft 6 in high* and *3 [??] 2 [???]* (presumably the width), but there's more data there for the finding. Let us know what you think you've got!

> Follow @NakedSecurity on Twitter for the latest computer security news.

> Follow @NakedSecurity on Instagram for exclusive pics, gifs, vids and LOLs!

## Free tools



Previous: California to make it harder for your license pl...

Next: Uber hit with criticism of "useless" two-factor aut...

## 17 comments on "Famous cryptographers' tombstone cryptogram de..."

Habeas Corpus January 22, 2018 at 3:04 pm

Inspiring article, thank you.

1 0 Rate This

Reply

Cetin A. January 23, 2018 at 4:46 am

That's the most romantic real life story I've read in a while.

9 0 Rate This

Reply

Farid Tahery January 23, 2018 at 4:46 am

Is there a reason for leaving out letters J and U from alphabet?

3 0 Rate This

Reply

Paul Ducklin January 23, 2018 at 8:28 am

I think the reason is that those letters are actually quite new in Roman alphabets, and in Bacon's time I/J and U/V were basically interchangable – visual variants of one another rather than distinct sounds.

10 0 Rate This

Reply

Farid Tahery January 24, 2018 at 1:05 am

Thanks for the info.

1 0 Rate This

Reply

Farid Tahery January 24, 2018 at 1:12 am

It also explains why in some European languages the letter V is used where you expect to see a U, for example many Swedish names such as Lindqvist.

4 0 Rate This

Reply

Laurence Marks January 24, 2018 at 3:39 am

In high school Latin, we learned about Iulius Caesar. And about two decades the US TV network had a series called I, Clavdivs (Claudius).

3 0 Rate This

Reply

Fox January 23, 2018 at 4:55 am

Fascinating stuff! Thank you for taking the time to write this up.

8 2 Rate This

Reply

Steve January 23, 2018 at 5:26 am

Great story!

9 1 Rate This

Reply

Andrew Ludgate January 23, 2018 at 7:11 pm

thanKs for this WonDErFuL UpdAtE On A neAT clpHEr PrOBLeM, Paul!

3 1 Rate This

Reply

Bryan January 25, 2018 at 2:45 am

Agreed. Twice.

*Of course proper credit should also go to the good doctor Friedman.*

1 1 Rate This

Reply

Chris d7 January 24, 2018 at 7:01 am

Seeing more:

BEFORE the word "Colonel", I *think* I see "Liut" (as in, missing an "e"..?)

AFTER "3 ft 6 in high", I *think* I see:

— 1 ' 6 " wide

... though the "1" might be a "2"..???

As for the "3 .. 2 .." below, I believe the gaps are either occupied by "dittos" or it reads:

3 ' 2 "

Finally, what's not specifically labelled on the image, but which I presume is "obvious enough" from the final tombstone, I can "clearly" see the YEARS "1891 – 1969" on the reverse of:

WL|EDGE I|S P

... It's where the over-label is for "US ARMY", and after "ARMY", you can see the last "9".

1891:

The first "1" is below the reverse P, the "8" is before/next to the reverse S,

the "9" is behind the I, and the last "1" is clearly visible between the I and reverse E.

The hyphen "–" is high up between the G""E

1969:

Upper half of this is quite clearly visible at WL|ED.

2 2 Rate This

Reply

Anonymous March 13, 2018 at 11:08 am

It seems likely that the "3 ft 6 in high" note relates to the dimensions of the tombstone. The sketch of the tombstone presented in the original paper seems to confirm this. The sketch appears to use each square of the grid paper to indicate one inch. Using this scale the centre of the tombstone is then shown to be 3′ 6″ high and 2′ 6″ wide. Equally, the base of the tombstone is 3′ 2″ wide which fits with the very bottom line. These dimensions appear to match the hard to read portions of the note.

0 0 Rate This

Reply

Clayton Buerkle January 27, 2018 at 4:38 pm

Hello Paul, I'd like to provide a response and update regarding "Bacon Redux". The Friedman's book was quite good for its time but has now been pretty thoroughly answered, even refuted, I'd say by now. In fact, it's an open question whether there was a deliberate misrepresentation of the Baconian evidence or whether one or both of them were just a bit sloppy in their research. In any case, many new potential hidden ciphers have been discovered since then. What we could use is more capable people to take a look at the evidence and contribute to the debate to move it forward. Let the chips fall where they may. In addition, the Baconian authorship theory was never debunked and is now far stronger than it was back in the 1950s. The Wikipedia article you link to is a very poor place for anyone to become informed on this

topic. The main problem with the authorship topic is that the Stratford corporation is quite wealthy and influential and extremely adverse to the authorship topic. And the mainstream scholarship is absolutely and blindly committed to the Stratfordian theory, such that they have never honestly looked at any alternative evidence. You could make a positive contribution toward some movement on this important historical question by affirming the open questioning of this ongoing debate, at least with regards to the cipher evidence.

1 1 Rate This

Reply

John M Howitt March 12, 2018 at 5:35 pm

You really ought to get out into the fresh air a bit more

1 4 Rate This

Reply

Robin March 12, 2018 at 9:50 pm

This is called steganography, not cryptography.

1 0 Rate This

Reply

relavak March 13, 2018 at 5:54 am

So is the real code here that her husband liked bacon?

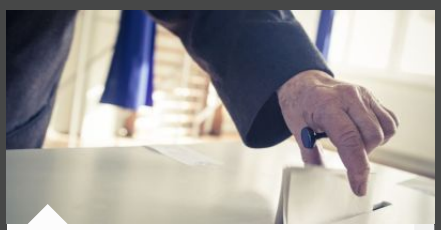
2 0 Rate This

Reply

## Leave a Reply

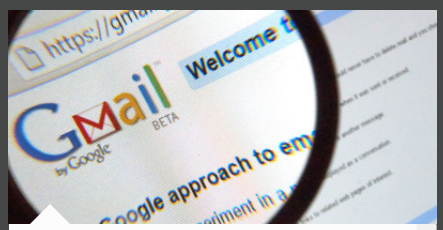
Enter your comment here...

## Recommended reads



SEP 10 BY LISA VAAS 4


JAN 29 BY NAKED SECURITY WRITER 0




JAN 20 BY LISA VAAS 14

‘Only paper ballots by 2020!’ call experts after election tampering

Monday review – the hot 21 stories of the week

School sues sysadmin for wiping its only login to Gmail





:)