

THE PECULIAR STORY OF THE HISTORY OF CRYPTOGRAPHY

SHAKESPEARE, BACON & THE NSA

Brendan O'Leary

Head of Community, ProjectDiscovery

FRANCIS BACON

**KNOWLEDGE
ITSELF IS
POWER**

Sacred Meditations,
1597

Elizebeth Smith

Yes that's how Elizebeth is spelled



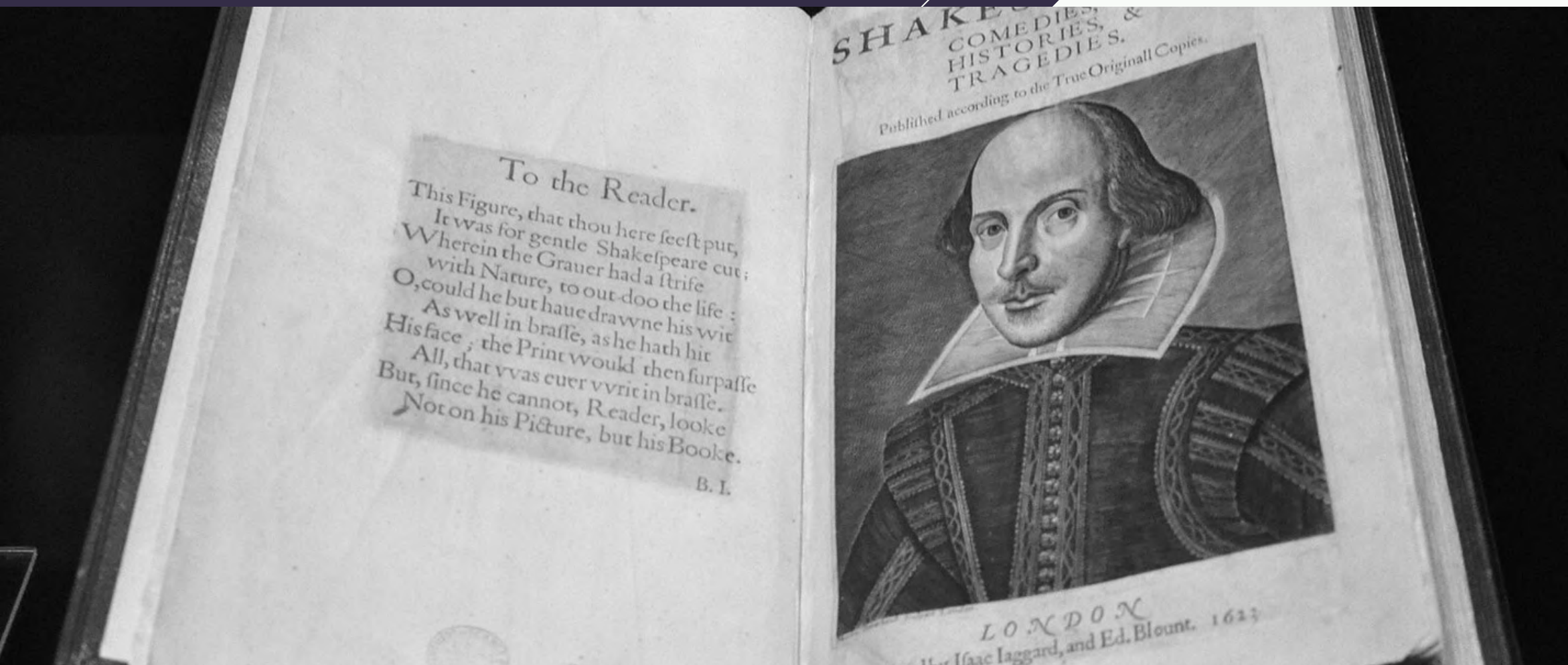
Brendan O'Leary

*Yes that's how Brendan
is spelled*



PROJECTDISCOVERY
Head of Community

FIRST FOLIO



The collected works of
William Shakespeare



Riverbank Laboratories

Elizebeth Smith and George Fayban

BACON'S CIPHER

| Letter | Code | Binary | Letter | Code | Binary |
|--------|-------|--------|--------|-------|--------|
| A | aaaaa | 00000 | N | abbaa | 01100 |
| B | aaaab | 00001 | O | abbab | 01101 |
| C | aaaba | 00010 | P | abbba | 01110 |
| D | aaabb | 00011 | Q | abbbb | 01111 |
| E | aabaa | 00100 | R | baaaa | 10000 |
| F | aabab | 00101 | S | baaab | 10001 |
| G | aabba | 00110 | T | baaba | 10010 |
| H | aabbb | 00111 | U, V | baabb | 10011 |
| I, J | abaaa | 01000 | W | babaa | 10100 |
| K | abaab | 01001 | X | babab | 10101 |
| L | ababa | 01010 | Y | babba | 10110 |
| M | ababb | 01011 | Z | babbb | 10111 |

Queene Elizabeth is my true mother
and I am the lawfull heire to the
throne. Finde the cypher storie my
bookes containe. It tells great secrets,
every one of which, if imparted openly,
would forfeit my life. – F. Bacon.

Francis of Verulam is author of all the
plays heretofore published by
Marlowe, Greene, Peele, Shakespeare,
and of two and twenty now put out for
the first time. Some are alter'd to
continue this history.

AHA! SHERLOCK IS OUTDONE!

The Great Shakespeare Mystery Is No Longer a Mystery; It Has Been Solved Right Here in Chicago, and the Spirit of Lord Bacon Says: "I Am Content with My 1916 Glory."

COL. GEORGE FABYAN

AMONG experts in free advertising there is much speculation as to who will get the most publicity following the suit brought by Col. Selig against Col. Fabyan. Some authorities in press work believe it the greatest publicity "stunt" ever attempted. There is a general belief that Col. Selig will benefit the most, because motion pictures are a more popular diversion than perusing volumes of

JUDGE RICHARD S. TUTHILL

Baconian cipher. And, in view of the fact that Col. Selig proposes to present Shakespearean plays on the screen much merit was seen in the suit against Fabyan. Col. Selig and Fabyan are not the enemies one might expect in such an extreme litigation. In fact, they are great cronies. Out in Geneva Col. Fabyan is master of a beautiful estate known as Riverbank. It is a miniature Japan. This is in honor of Mrs. Fab-

WILLIAM SHAKESPEARE LORD BACON

yan, who is a Japanese. There are wonderful formal gardens and Japanese landscape work, rendering a miniature Japan effect to give Mrs. Fabyan the atmosphere of her beloved native land. One of Col. Selig's most valued scenario writers for his motion picture plant is Onoto Watanna, a Japanese girl of much talent. In preparing her scenarios she has been a guest of Mrs.

COL. WILLIAM N. SELIG

Fabyan, and Col. Selig, too, has been wont to grace the table of his friend, Col. Fabyan. It is said that Col. Selig was the guest of Col. Fabyan on the day before the famous Shakespeare-Bacon suit was filed. Estimates on the amount of publicity are varied. Some experts say Col. Selig will get as much as 10,000,000 columns of free advertising.

J. Gotthelf

—
Die schwarze
Spinne

WILLIAM
SHAKESPEARE

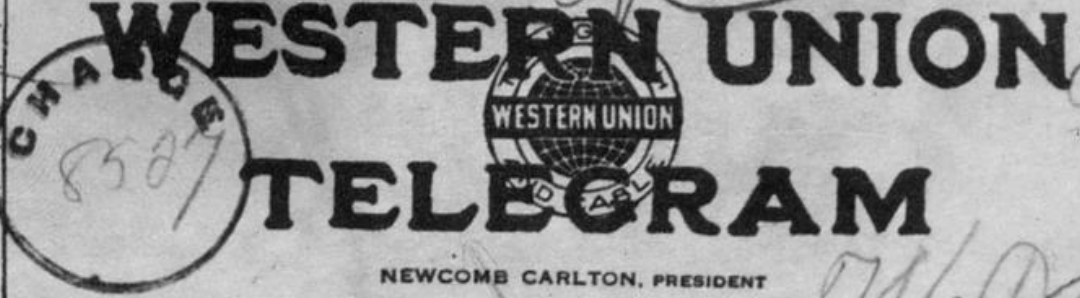
HAMLET

Martin
Luther

Worte



| |
|---|
| CLASS OF SERVICE DESIRED |
| Fast Day Message |
| Day Letter |
| Night Message |
| Night Letter |
| Patrons should mark an X opposite the class of service desired: OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE. |



| |
|---------------|
| Receiving No. |
| Check |
| Time Filed |

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

GERMAN LEGATION
MEXICO CITY

| | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 130 | 13042 | 13401 | 8501 | 115 | 3528 | 416 | 17214 | 6491 | 11310 |
| 18147 | 18222 | 21560 | 10247 | 11518 | 23677 | 13605 | 3494 | 14936 | |
| 98092 | 5905 | 11311 | 10392 | 10371 | 0302 | 21290 | 5161 | 39695 | |
| 23571 | 17504 | 11269 | 18276 | 18101 | 0317 | 0228 | 17694 | 4473 | |
| 22284 | 22200 | 19452 | 21589 | 67893 | 5569 | 13918 | 8958 | 12137 | |
| 1333 | 4725 | 4458 | 5905 | 17166 | 13851 | 4458 | 17149 | 14471 | 6706 |
| 13850 | 12224 | 6929 | 14991 | 7382 | 15857 | 67893 | 14218 | 36477 | |
| 5870 | 17553 | 67893 | 5870 | 5454 | 16102 | 15217 | 22801 | 17138 | |
| 21001 | 17388 | 7446 | 23638 | 18222 | 6719 | 14331 | 15021 | 23845 | |
| 3156 | 23552 | 22096 | 21604 | 4797 | 9497 | 22464 | 20855 | 4377 | |
| 23610 | 18140 | 22260 | 5905 | 13347 | 20420 | 39689 | 13732 | 20667 | |
| 6929 | 5275 | 18507 | 52262 | 1340 | 22049 | 13339 | 11265 | 22295 | |
| 10439 | 14814 | 4178 | 6992 | 8784 | 7632 | 7357 | 6926 | 52262 | 11267 |
| 21100 | 21272 | 9346 | 9559 | 22464 | 15874 | 18502 | 18500 | 15857 | |
| 2188 | 5376 | 7381 | 98092 | 16127 | 13486 | 9350 | 9220 | 76036 | 14219 |
| 5144 | 2831 | 17920 | 11347 | 17142 | 11264 | 7667 | 7762 | 15099 | 9110 |
| 10482 | 97556 | 3569 | 3670 | | | | | | |

BERNSTORFF.

7600
via Galveston
JAN 19 1917

862.20212/52A

4458 gemeinsam
17149 Friedensschluss.
14471
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 Einverständnis
7382
158(5)7
67893 Mexic
14218 in
36477 Texas
5870
17553
67893 Mexic
5870
5454 AR
16102 IZ
15217 ON
22601 A

TELEGRAM RECEIVED.
FROM 2nd from London # 5747.
By Wm A. Eckhoff
Date Oct 27 1917

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite ~~the~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMAN.

RECEIVED
Director 1-8-88
State Dept.

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

By Mark A. Eckhoff
Date Oct. 27, 1917

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the



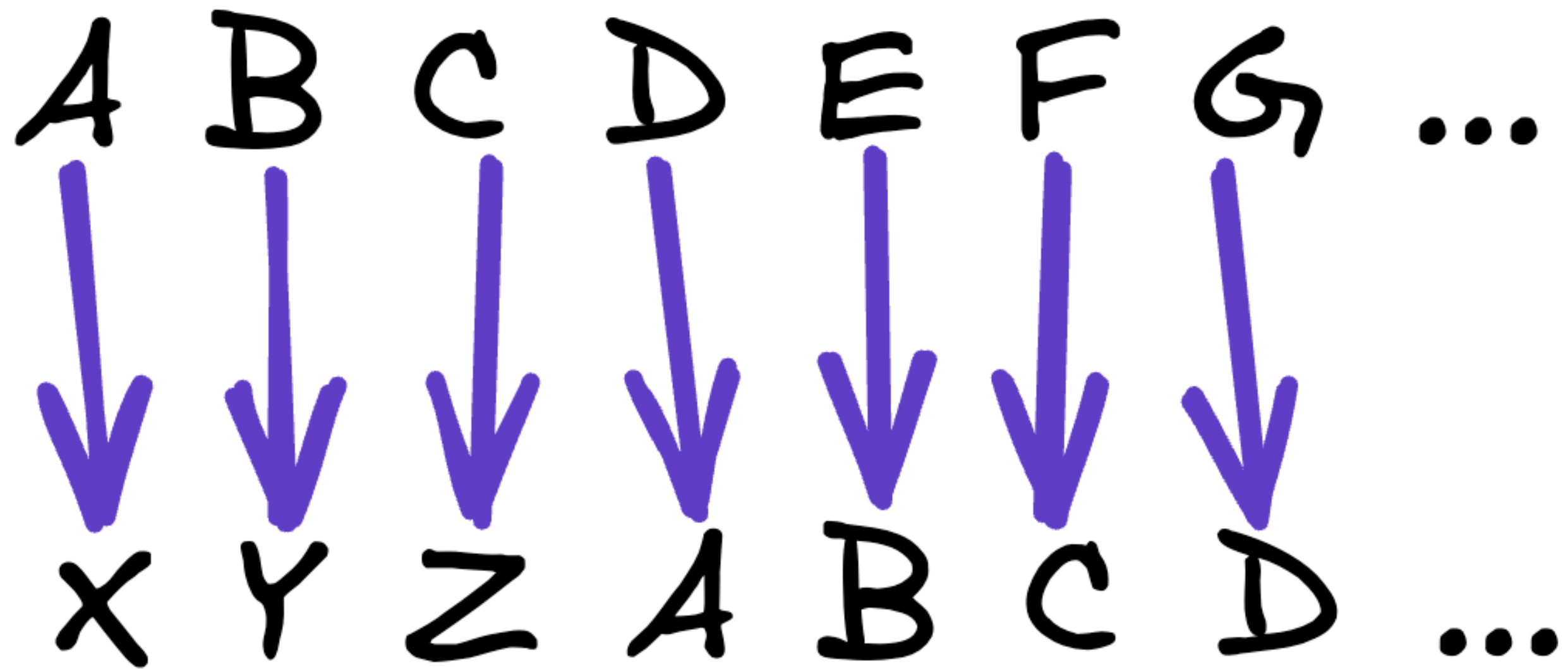
METHODS FOR THE
SOLUTION OF
CIPHERS

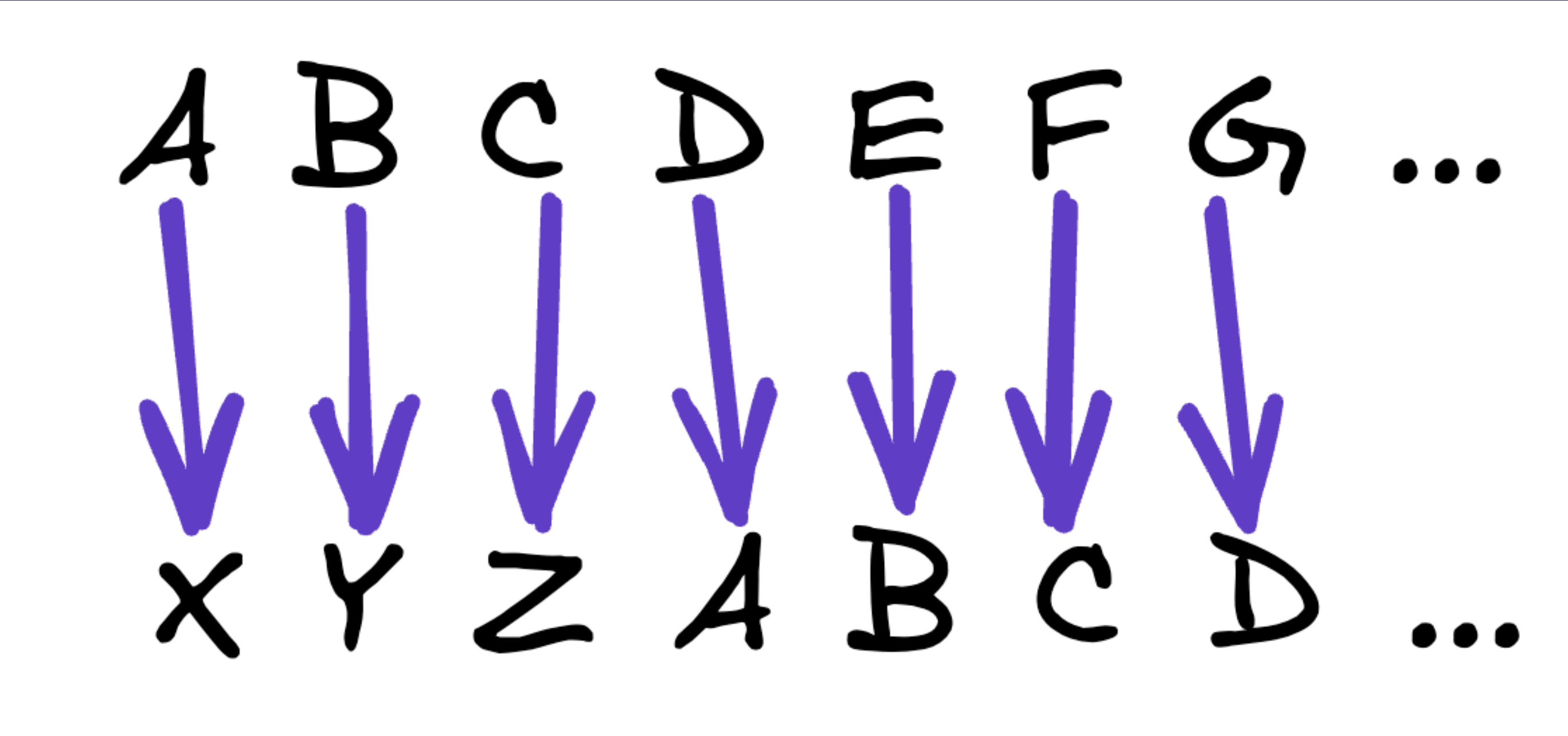
PUBLICATIONS, 15-22 INCL.

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
Riverbank--Geneva, Ill.

Gift of
Riverbank Laboratory

Note -
All these papers were written by me
except No. 19 (Transposition Ciphers) which
was written in collaboration with
Capt. Lenox R. John, and No. 21, which
was written in collaboration with
Elizabeth Smith Friedman, my wife.
W. F. F.





403,291,461,126,605,635,584,000,000



*as an, rosolut class
Crafted in the village
Åhus, Sweden.
Absolut Since 1879*

IMPORTED
40% ALC./VOL. (80 PROOF)
1L

LIME FLAVORED VODKA
PRODUCED AND BOTTLED IN ÅHUS, SW

Prohibition

1920 – 1933

"The pretty cryptanalyst"



The Second World War



The Second World War

The Second World War





WILLIAM F. FRIEDMAN AUDITORIUM

May 21, 1975



Friedman Conference Center

Fort Meade, MD
2018



LESSONS

Interdisciplinary Problem Solving

Bringing unique perspectives to bear on your problems

Stop being Complacent with Compliance

Speak up when you're defending against the wrong things

Nothing is Impenetrable

Always be trying to "decode" your own security systems & practices

Think like an Attacker

The best defense can often be a good offense - or at least thinking like one

Interdisciplinary Thinking

COMPLEXITY

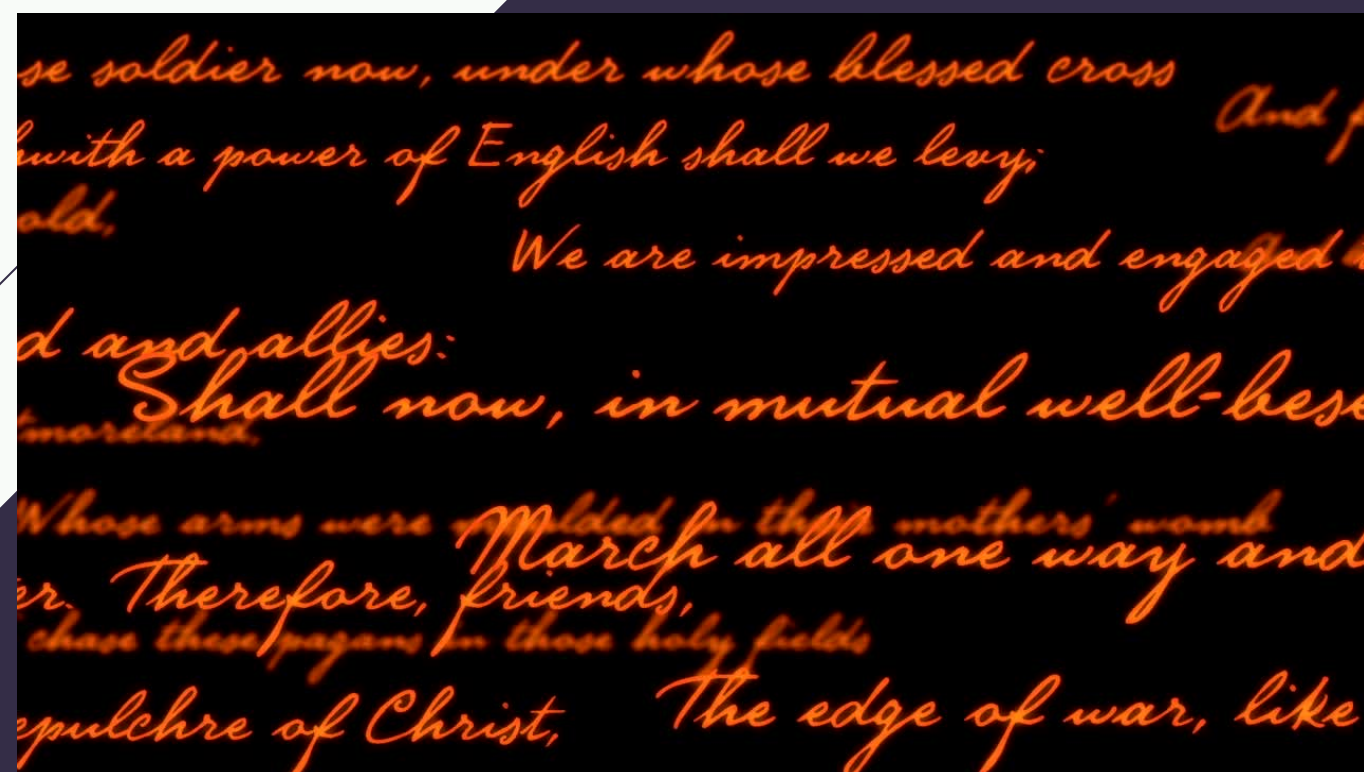
Effectively address the multifaceted challenges modern threats present

COMPREHENSIVE

An entire picture of your attack surface, attack vectors, and exposures

COLLABORATION

Bringing to bear on the problem more than just the "old guard" in security



Think like an Attacker



ATTACK SURFACE

The first thing any good attacker will do is evaluate the entire attack surface

PRIORITIZATION

Attackers don't want to waste time chasing non-valuable assets and vectors

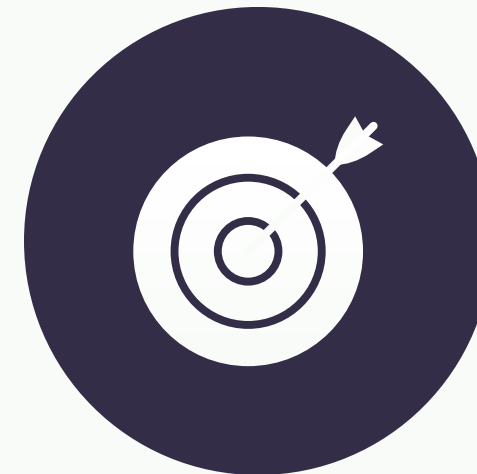
LEVERAGE EXPLOITS

Reusing or leveraging existing exploits allows an attacker to move faster

Nothing is impenetrable



Red, Purple
Teaming



Continuous
Penetration
Testing



Bug Bounty
Programs

Stop being Complacent with Compliance



COMPLIANCE

Compliance is the low bar - not the final one. It is rarely enough

WHAT ARE YOU PROTECTING AGAINST?

Do you want to protect against an auditor or an attacker?

"SECURITY IS EVERYONE'S JOB"

Sure - that may be true, but it is *our* job for sure - so speak up!

v2apz3a

: DU VX EE GF NP GO 34 99 QS BD
AV MS 27 BE BL FC DW AA HH VE

: YY FE DU UR TX OC UN OX 3K O
F2 05 80 M1 E4 15 15 GO OE O
AR 2F G2 J2 GO 00 NO 00 00 0
YY FB DU UR TX OC UN OX 3K O



WILLIAM F. FRIEDMAN
LIEUTENANT COLONEL

UNITED STATES ARMY

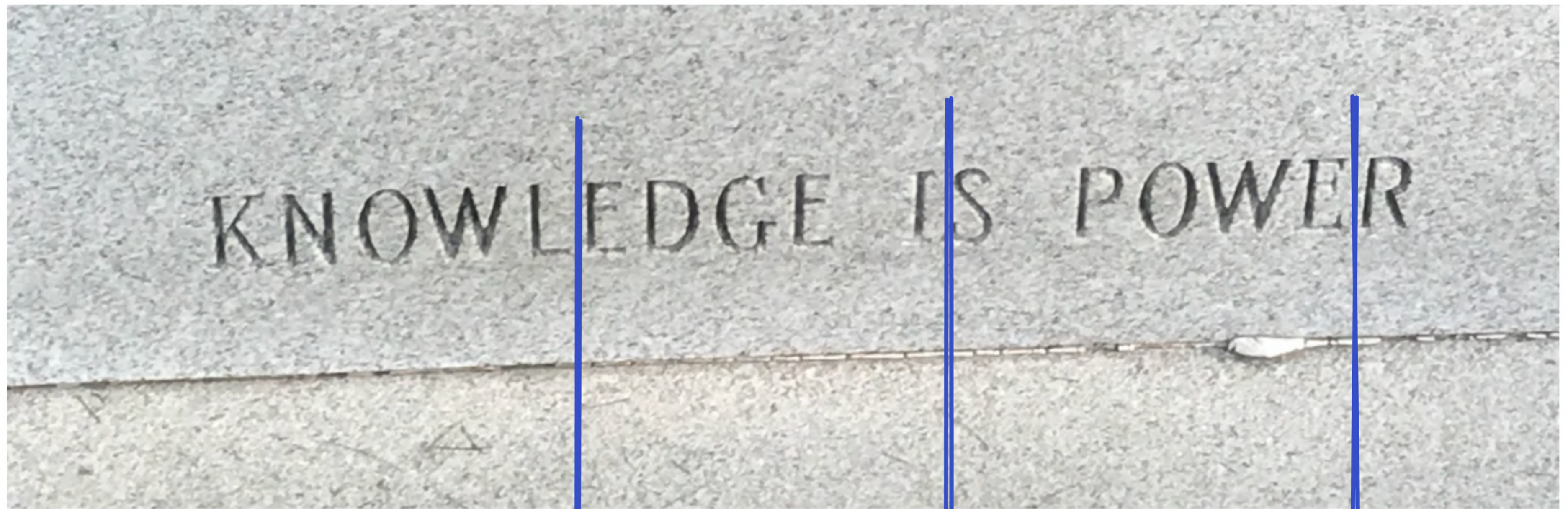
1891 ... 1969

BELOVED WIFE

ELIZABETH SMITH FRIEDMAN

1892 ... 1980

KNOWLEDGE IS POWER



W

F

F



Thank You

Shakespeare, Bacon
and the NSA



nux.gg/bacon
nux.gg/discord

Twitter: @olearycrew
Bluesky: @brendan.fyi





Lard_Baron · 13 yr. ago · edited 11 yr. ago 🏆 3 💡 🧠 🙌 7 & 15 More

When I was young my father said to me:

"Knowledge is Power...Francis Bacon"

I understood it as "Knowledge is power, France is Bacon".

For more than a decade I wondered over the meaning of the second part and what was the surreal linkage between the two? If I said the quote to someone, "Knowledge is power, France is Bacon" they nodded knowingly. Or someone might say, "Knowledge is power" and I'd finish the quote "France is Bacon" and they wouldn't look at me like I'd said something very odd but thoughtfully agree. I did ask a teacher what did "Knowledge is power, France is bacon" mean and got a full 10 minute explanation of the Knowledge is power bit but nothing on "France is bacon". When I prompted further explanation by saying "France is Bacon?" in a questioning tone I just got a "yes". at 12 I didn't have the confidence to press it further. I just accepted it as something I'd never understand.

It wasn't until years later I saw it written down that the penny dropped.

↑ 3.9k ↓ Share ...

France is Bacon



nux.gg/bacon

nux.gg/discord

Twitter: @olearycrew

Bluesky: @brendan.fyi



=

