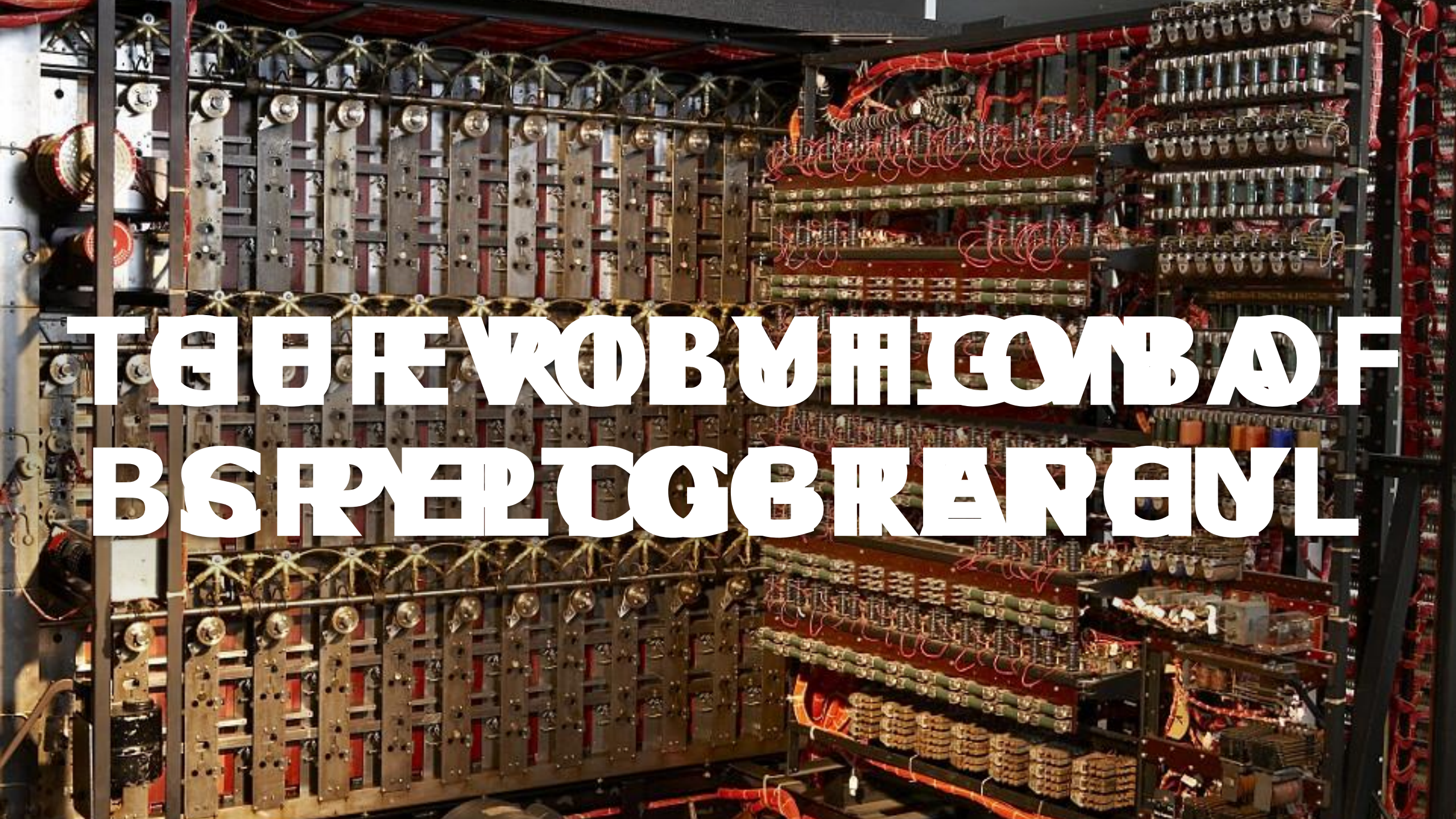

THE ROBUSTICS OF
BSPERTOGRAPHUL

online

Results. Guaranteed.

Jeff Man

Information Security Evangelist

InfoSec Curmudgeon

PCI QSA; Trusted Advisor

Online Business Systems

@MrJeffMan

301-310-4275

jman@obsglobal.com



online

Results. Guaranteed.



Online Business Systems

https://www.obsglobal.com/

online

Results. Guaranteed.

My Background

- 13 years with the Department of Defense
  - Certified Cryptanalyst
  - Designed Cryptosystems and Cryptologic Aids
  - Founding Member of Systems & Network Attack Center
- 14 years as a PCI Qualified Security Assessor (QSA)
  - Lead Assessor/Assessment Team Member
  - Trusted Advisor
- 3 years with a Software Vendor
  - PCI Subject Matter Expert
  - Thought Leader
  - Security Strategist
- 27+ years of commercial professional servic
  - Penetration Testing
  - Vulnerability Assessments
  - Security Architecture



QUALIFIED SECURITY ASSESSOR







Catching Up

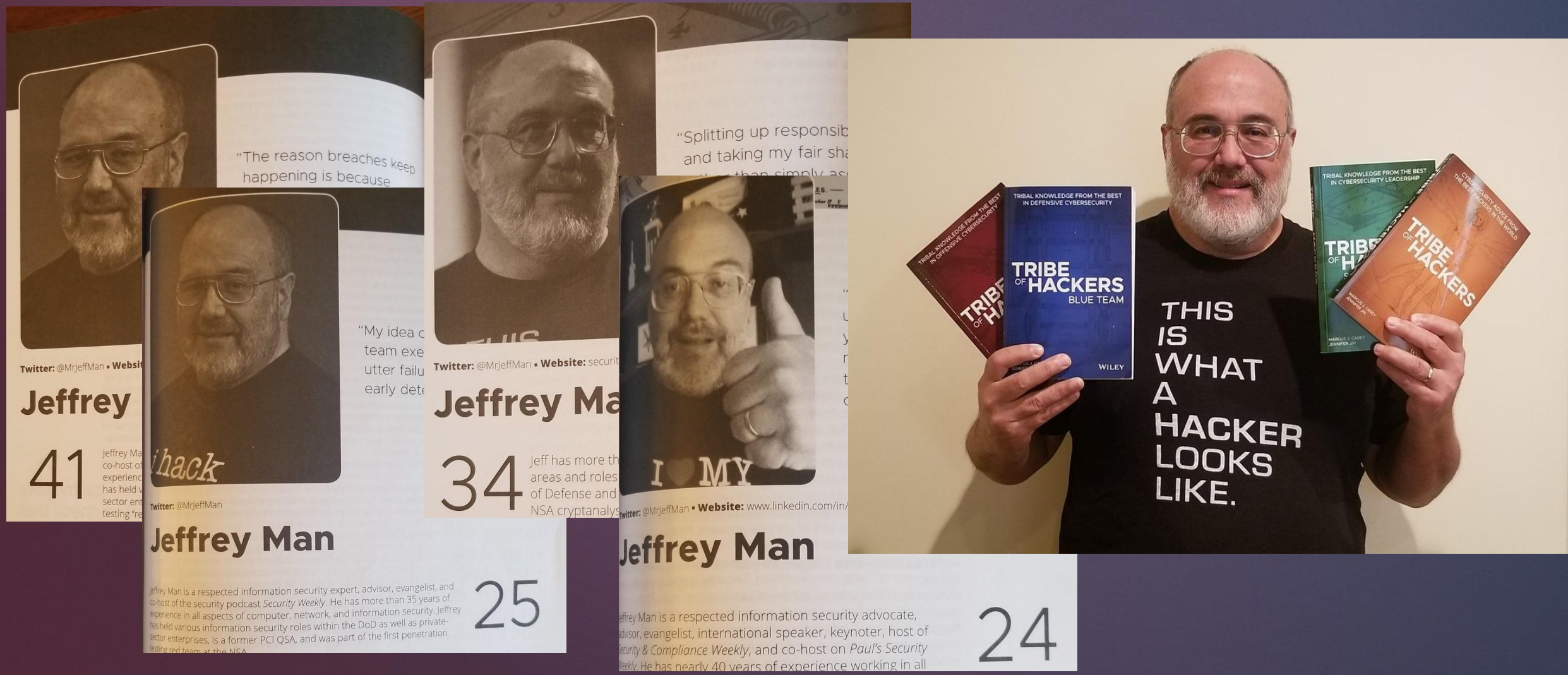




Co-Host on Paul's Security Weekly

online

Results. Guaranteed.



Tribe of Hackers Series



EP 83: NSA CRYPTOLOGISTS

advanced persistent threat

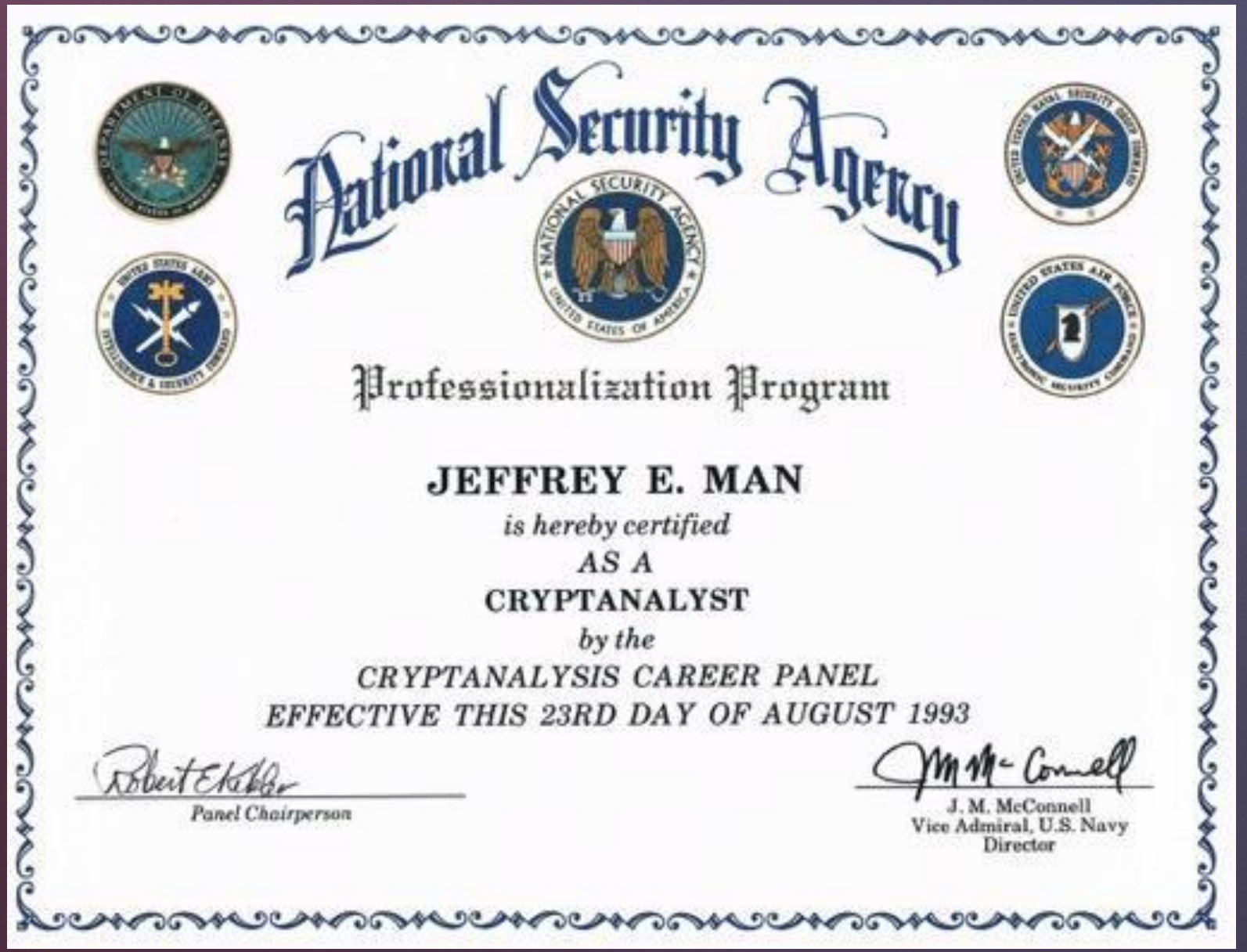
19 January 2021 | 82:56



NSA "Red Team" Hacker | Jeff Man | Ep. 269

online

Results. Guaranteed.



National Security Agency

Professionalization Program

JEFFREY E. MAN

is hereby certified

AS A

CRYPTANALYST

by the

CRYPTANALYSIS CAREER PANEL

EFFECTIVE THIS 23RD DAY OF AUGUST 1993

Panel Chairperson

J. M. McConnell
Vice Admiral, U.S. Navy
Director

online

Results. Guaranteed.

One-Time Pad



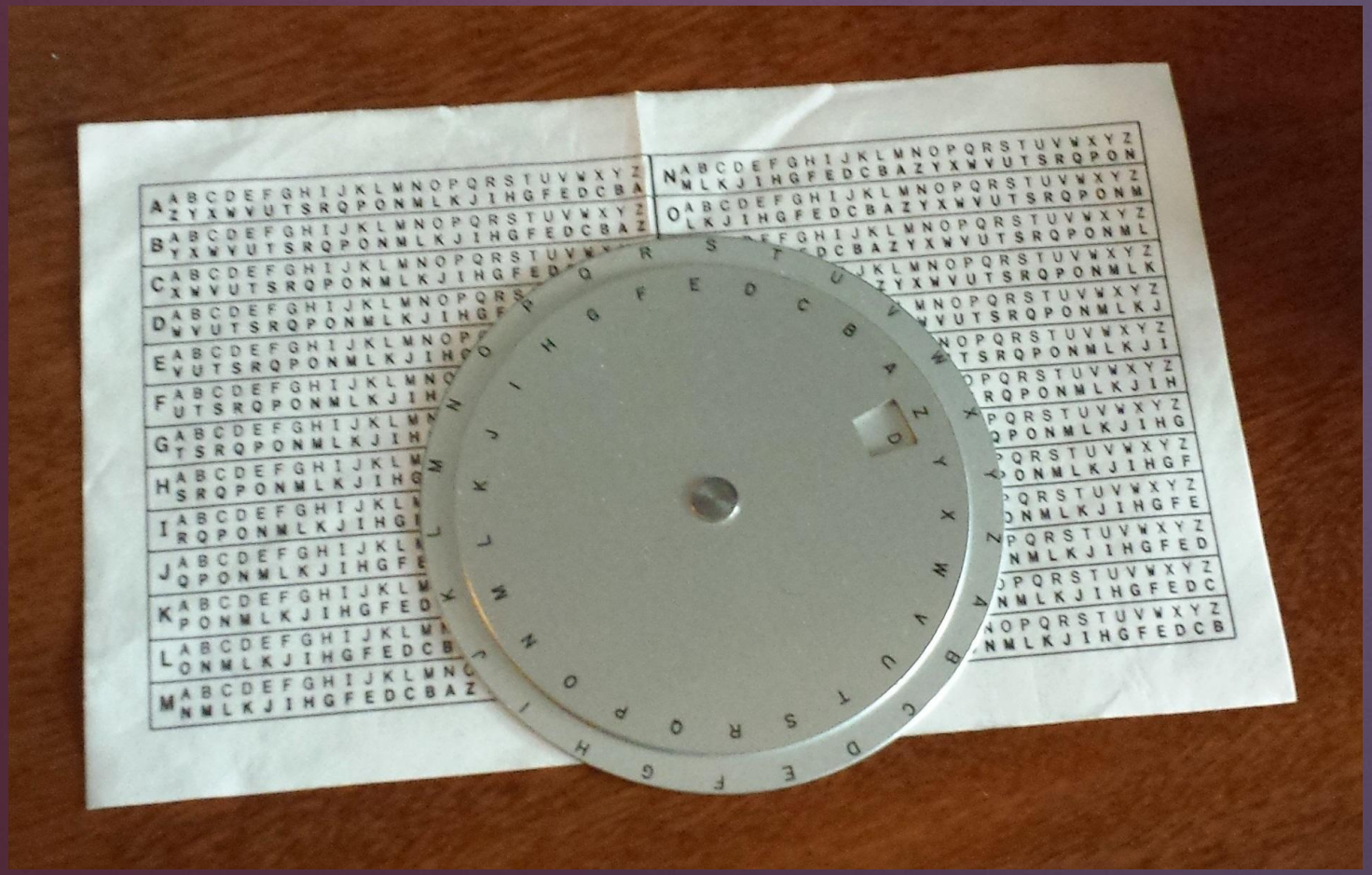




Designed and fielded NSA's First SW-Based Cryptosystem

online

Results. Guaranteed.



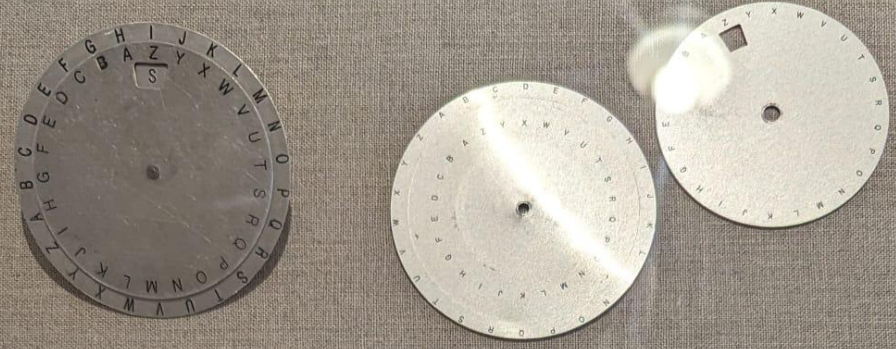


The Vigenere “Wheel” – Specialized Cipher Disc

National Cryptologic Museum







(Jeff) Man Reinvents the Wheel



Special operators get all the toughest jobs. The most secret. The most important. The most dangerous.

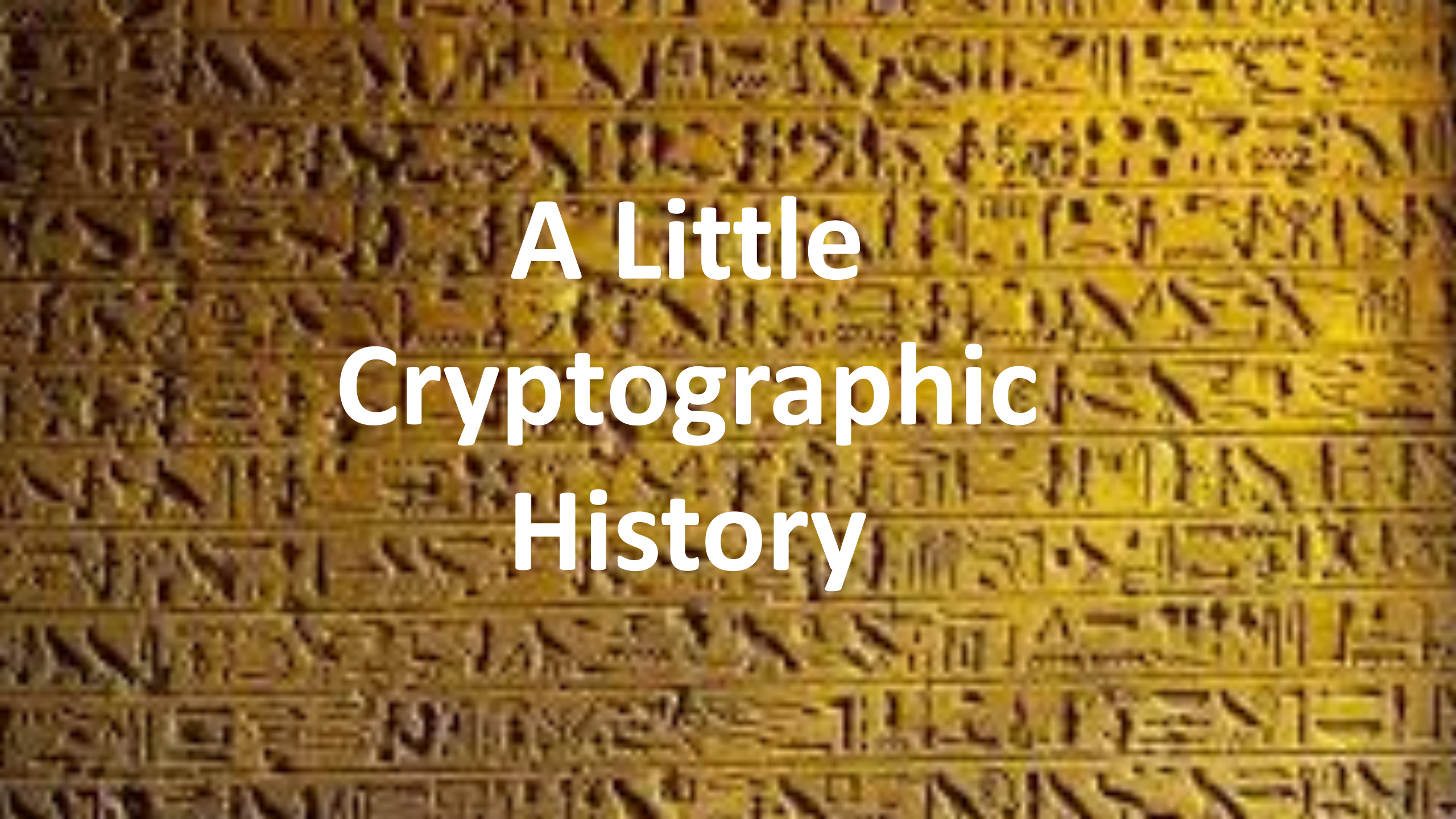
So NSA cryptanalyst Jeff Man thought he could make their work just a bit easier.

When units needed to send secret communications, they had to tediously cipher and decipher using one time pads. Man developed this HAL-001 Vigenere Wheel, more commonly known as the Whiz Wheel (yes, we know), to simplify the one time pad trigraph system of over one hundred 3-letter combinations. This cut down on time and chances for human error.

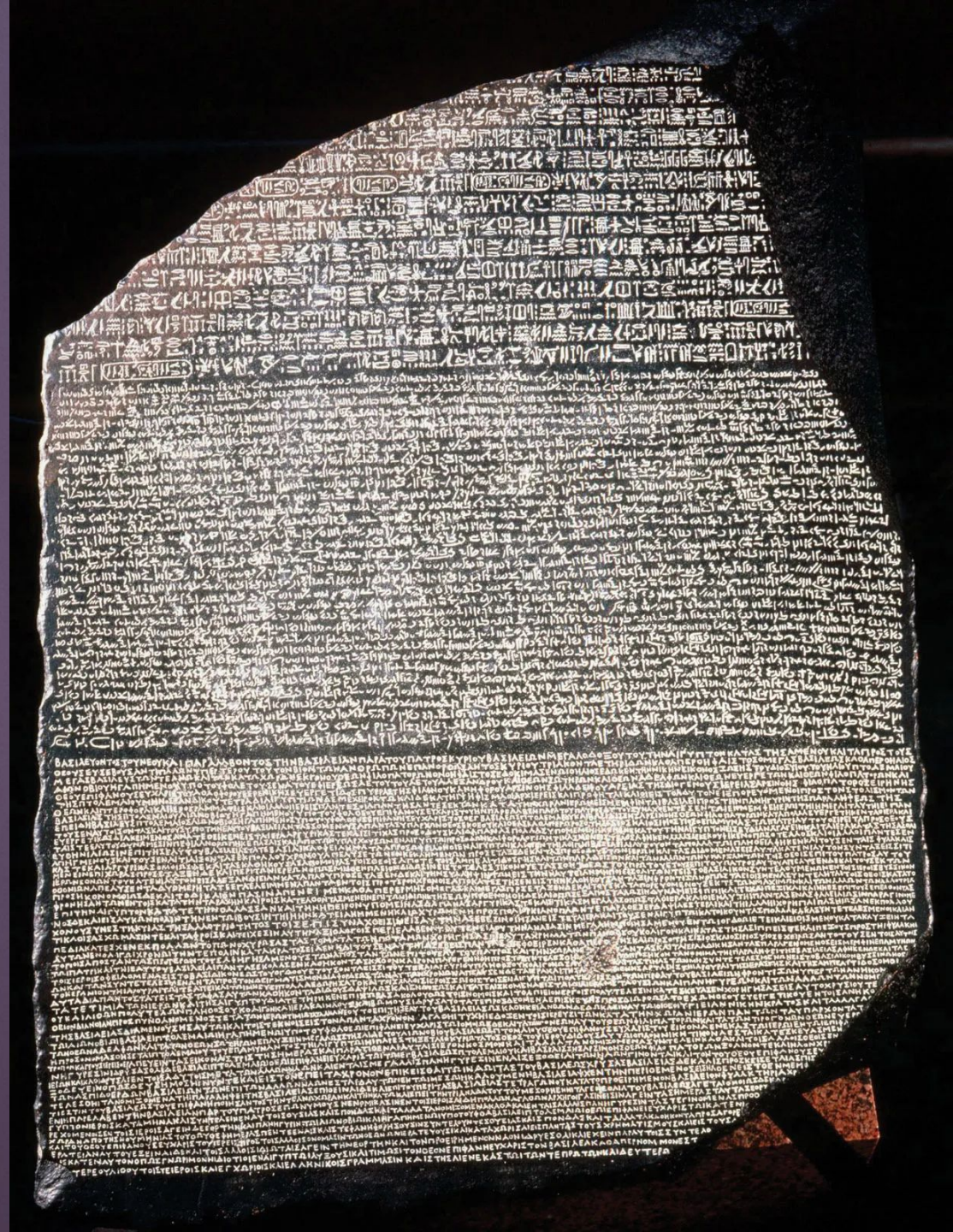
Less time spent on encryption/decryption, more time doing the stuff they would make movies about... in about 25 years or so...

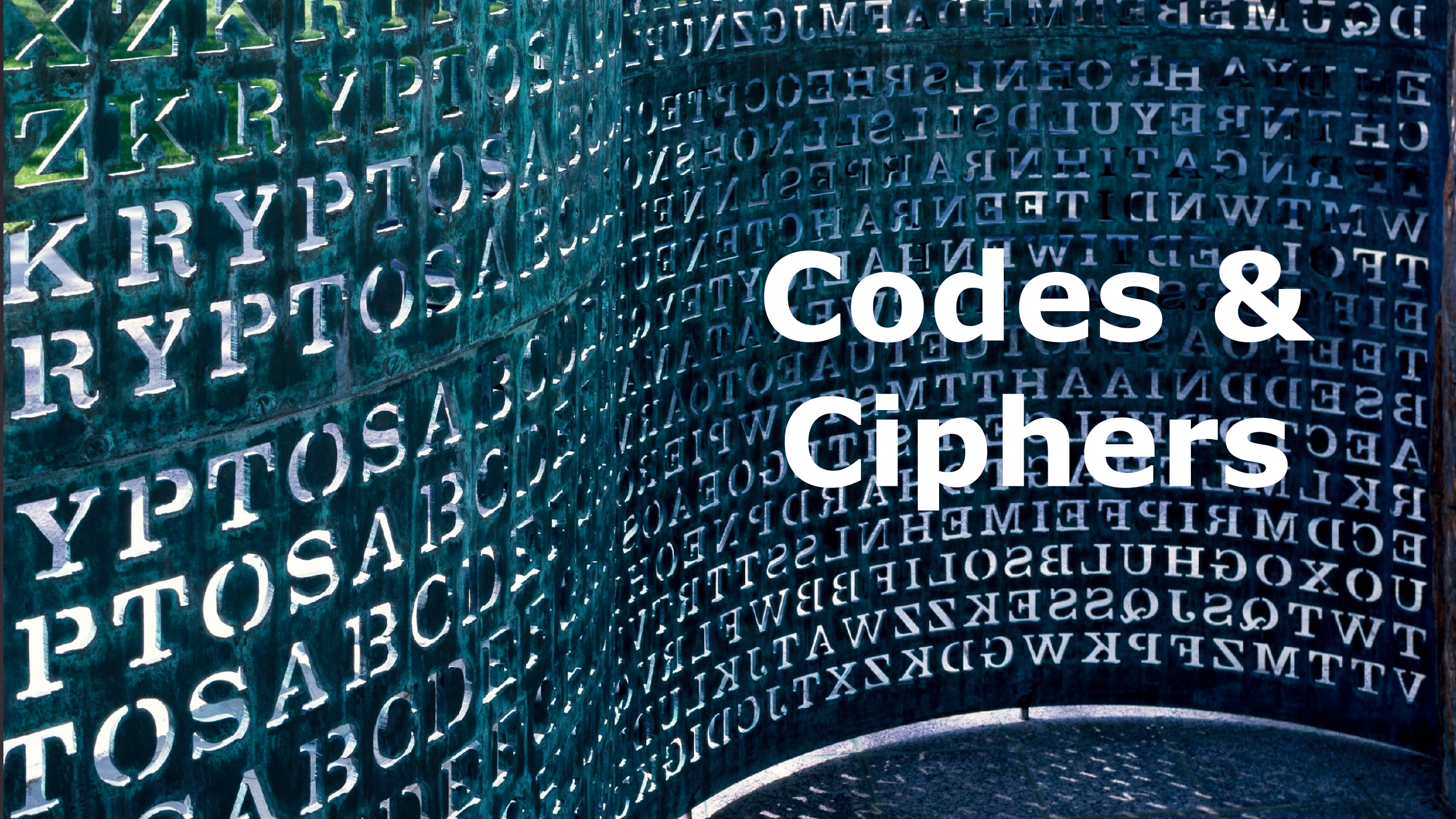
HAL-001 Vigenere (Whiz) Wheel Prototype, Jeff Man, 1988

HAL-001 Vigenere (Whiz) Wheel Production Model, NSA, 1988


A Little
Cryptographic
History

People have been keeping secrets for Thousands of years




Codes &
Ciphers

Paul Revere's Ride

"Listen, my children, and you shall hear
Of the midnight ride of Paul Revere…"

"One if by land, and two if by sea;
And I on the opposite shore will be,
Ready to ride and spread the alarm
Through every Middlesex village and farm,
For the country-folk to be up and to arm."

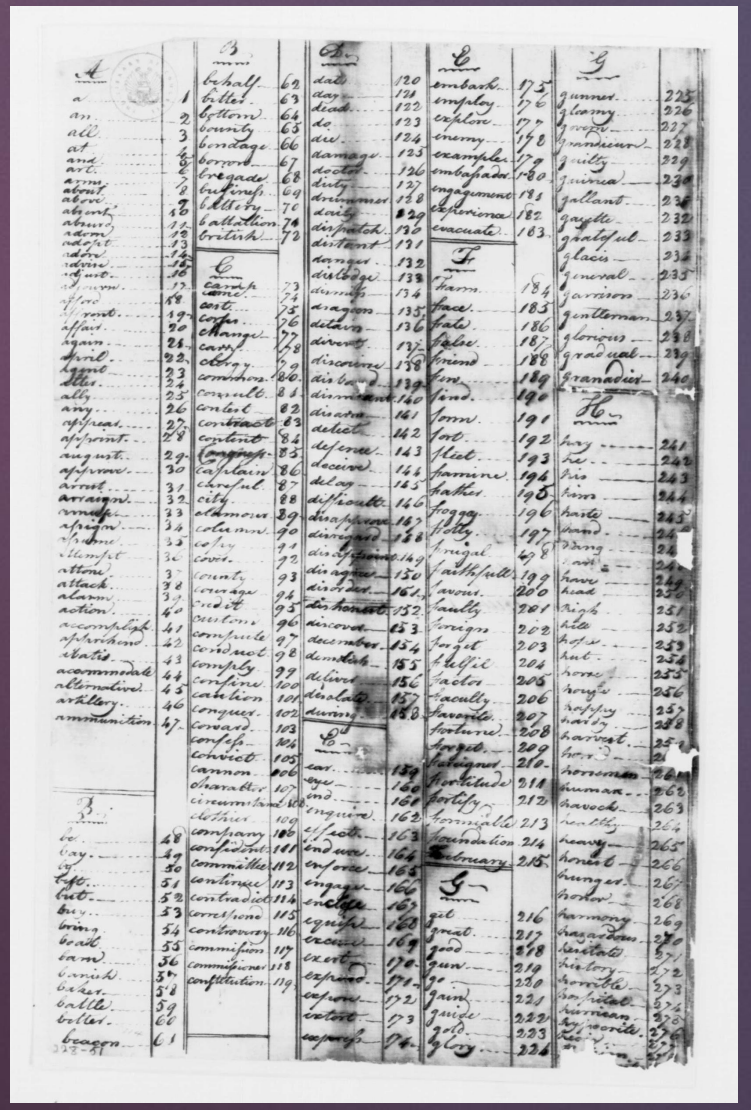
- Henry Wadsworth Longfellow



online

Results. Guaranteed.

Secret Codes

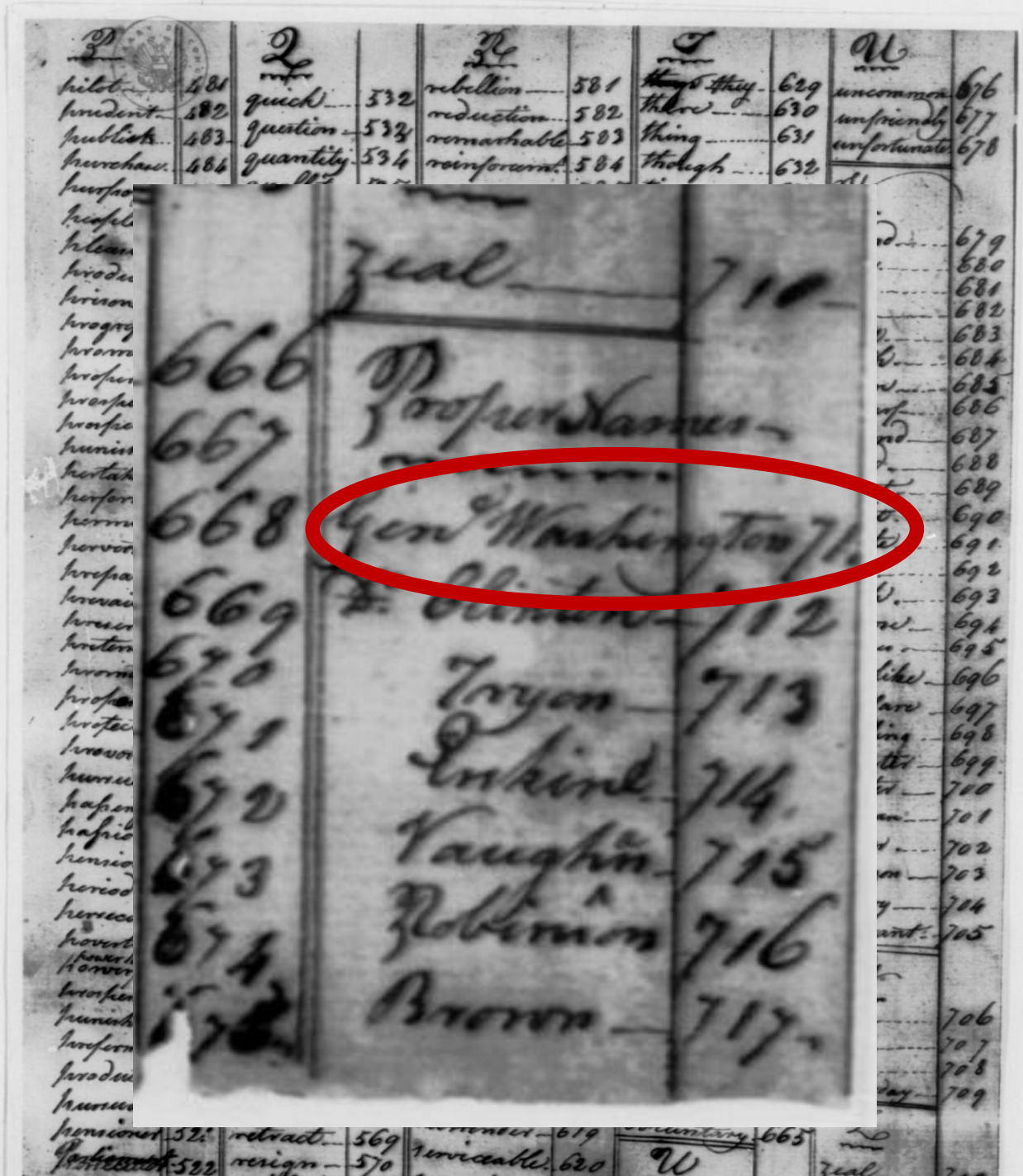




online

So who was Agent 711?

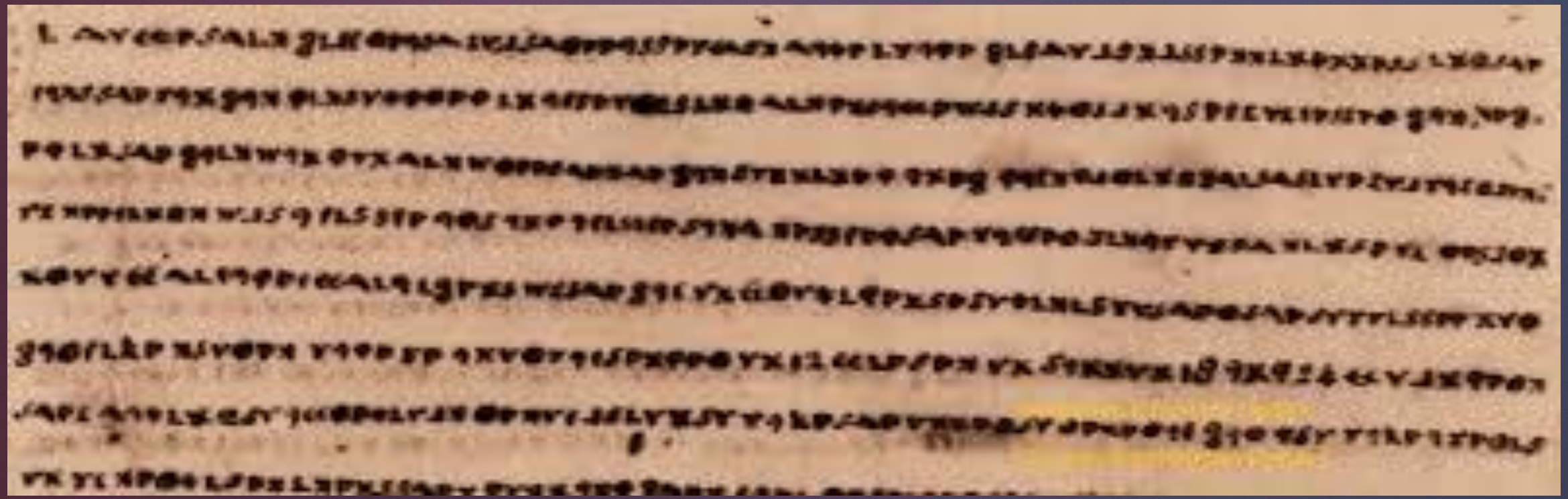
George Washington



online

Results. Guaranteed.

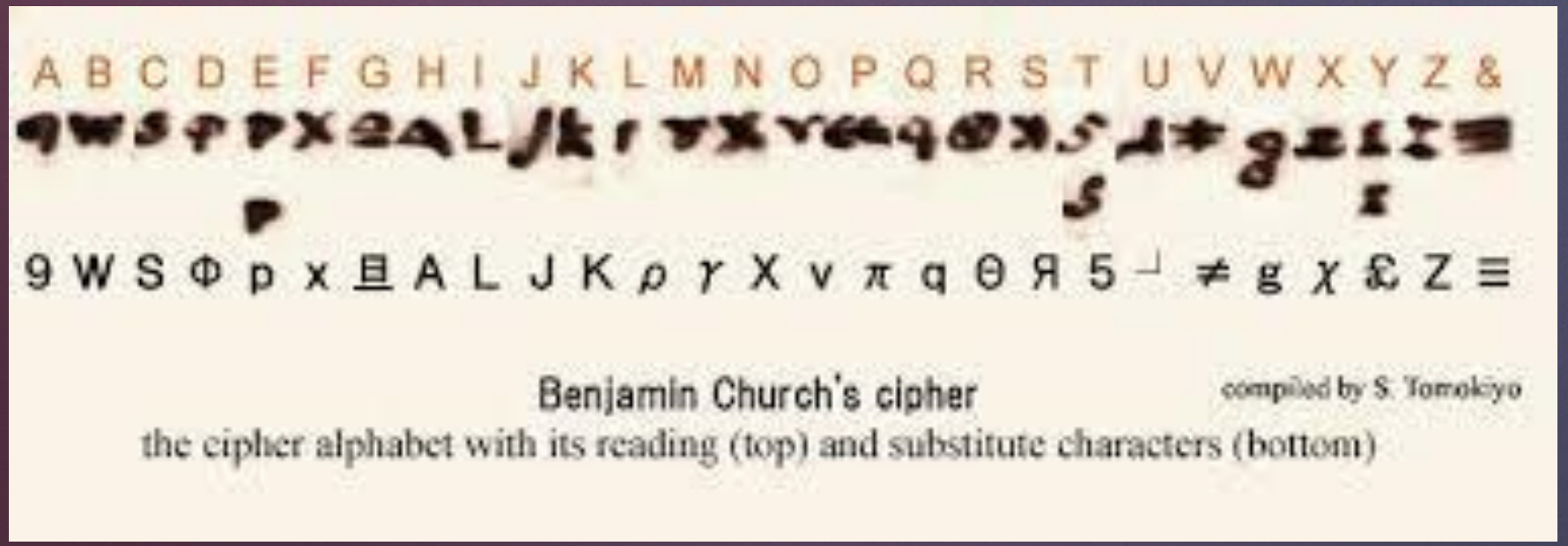
Benjamin Church Cipher



online

Results. Guaranteed.

Simple Substitution



Benjamin Church's cipher — compiled by S. Tomokiyo

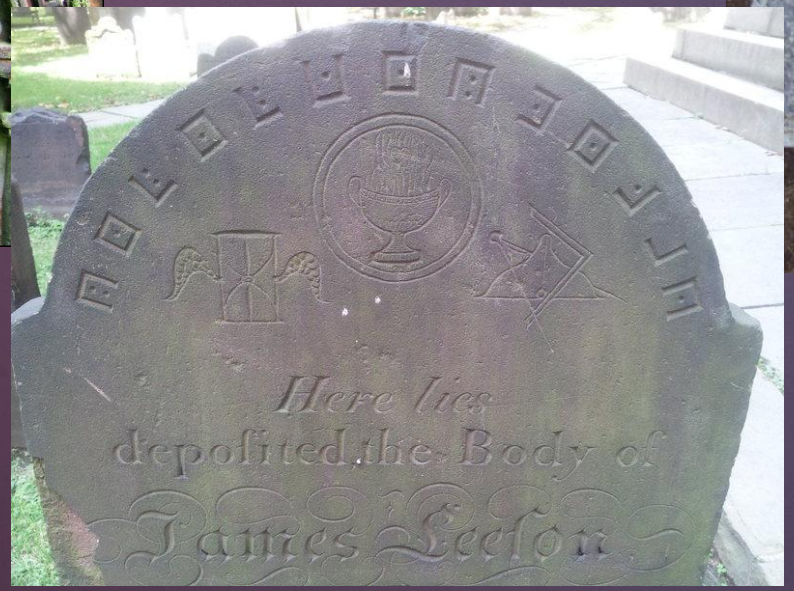
the cipher alphabet with its reading (top) and substitute characters (bottom)

Confederate Cipher Disk (Caesar Cipher)



online
Results. Guaranteed.





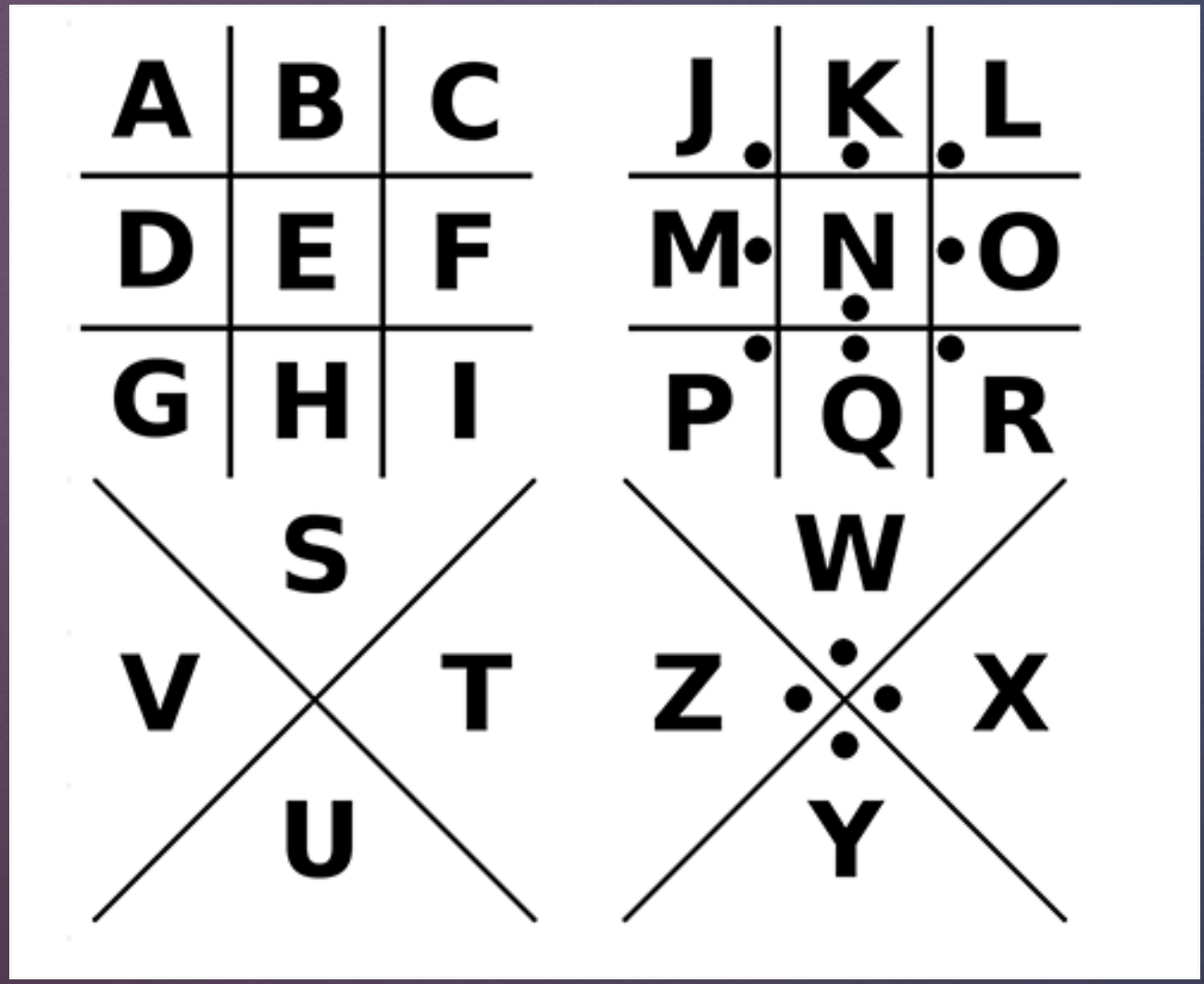


Freemasons like to keep secrets too!

online
Results. Guaranteed.

PigPen Cipher

Really a simple substitution cipher, just with symbols



online
Results. Guaranteed.

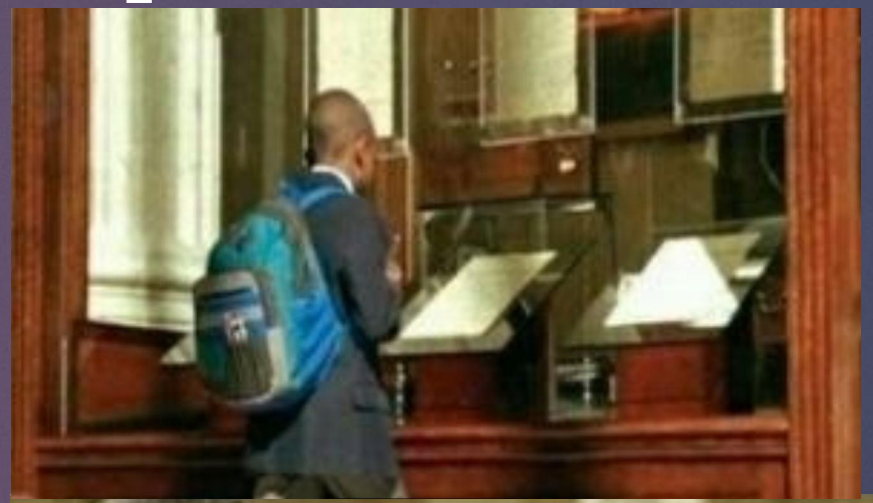


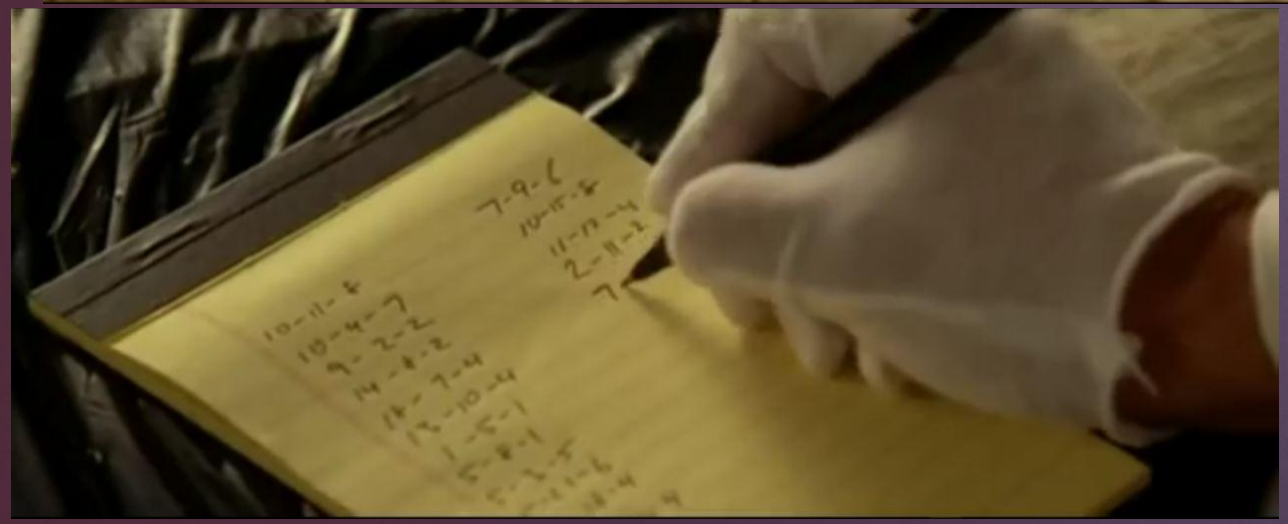
online

Results. Guaranteed.

“Ottendorf Cipher”





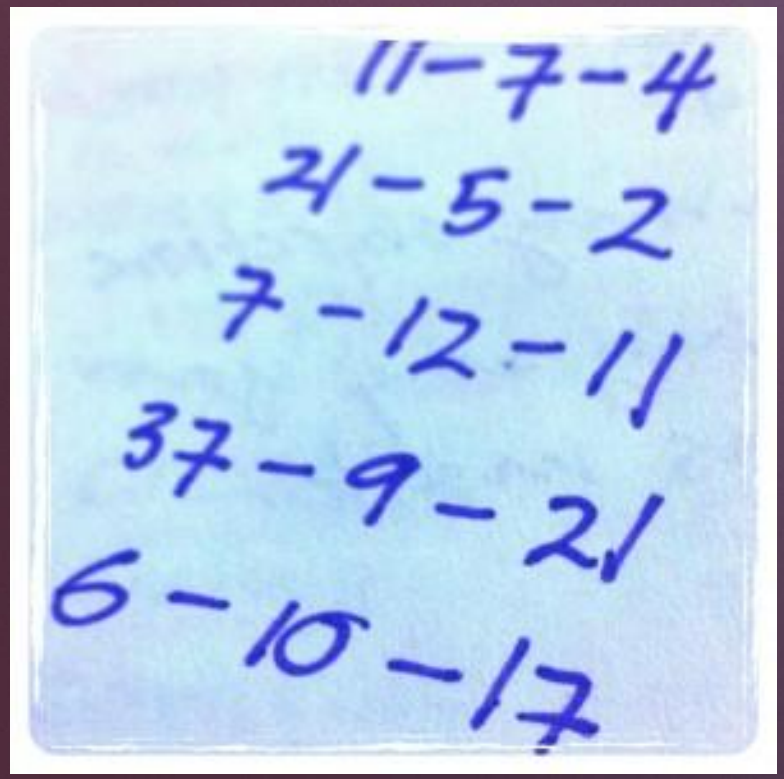


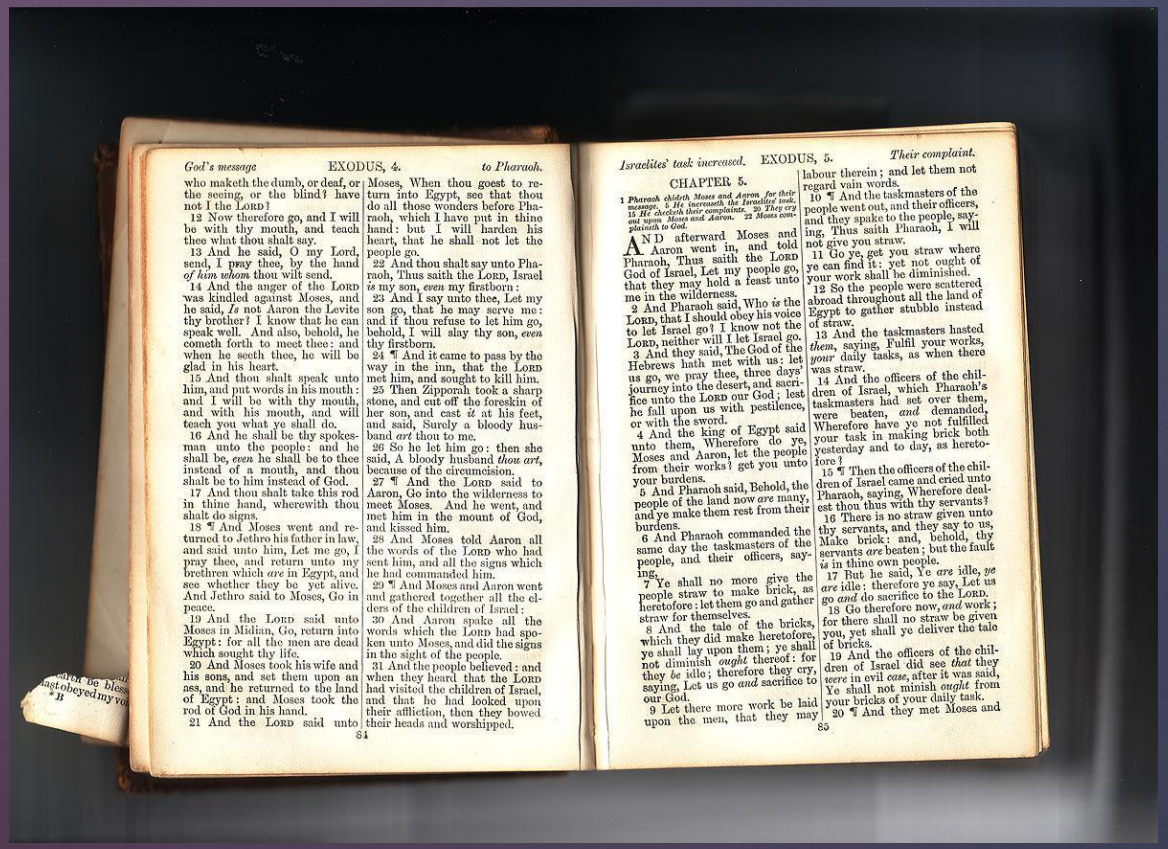


online

Results. Guaranteed.

Arnold Cipher





God's message EXODUS, 4. to Pharaoh.

who maketh the dumb, or deaf, or the seeing, or the blind? have not I the LORD?
12 Now therefore go, and I will be with thy mouth, and teach thee what thou shalt say.
13 And he said, O my Lord, send, I pray thee, by the hand *of him whom* thou wilt send.
14 And the anger of the LORD was kindled against Moses, and he said, *Is* not Aaron the Levite thy brother? I know that he can speak well. And also, behold, he cometh forth to meet thee: and when he seeth thee, he will be glad in his heart.
15 And thou shalt speak unto him, and put words in his mouth: and I will be with thy mouth, and with his mouth, and will teach you what ye shall do.
16 And he shall be thy spokesman unto the people: and he shall be, *even* he shall be to thee instead of a mouth, and thou shalt be to him instead of God.
17 And thou shalt take this rod in thine hand, wherewith thou shalt do signs.
18 ¶ And Moses went and returned to Jethro his father in law, and said unto him, Let me go, I pray thee, and return unto my brethren which *are* in Egypt, and see whether they be yet alive. And Jethro said to Moses, Go in peace.
19 And the LORD said unto Moses in Midian, Go, return into Egypt: for all the men are dead which sought thy life.
20 And Moses took his wife and his sons, and set them upon an ass, and he returned to the land of Egypt: and Moses took the rod of God in his hand.
21 And the LORD said unto Moses, When thou goest to return into Egypt, see that thou do all those wonders before Pharaoh, which I have put in thine hand: but I will harden his heart, that he shall not let the people go.
22 And thou shalt say unto Pharaoh, Thus saith the LORD, Israel *is* my son, *even* my firstborn:
23 And I say unto thee, Let my son go, that he may serve me: and if thou refuse to let him go, behold, I will slay thy son, *even* thy firstborn.
24 ¶ And it came to pass by the way in the inn, that the LORD met him, and sought to kill him.
25 Then Zipporah took a sharp stone, and cut off the foreskin of her son, and cast *it* at his feet, and said, Surely a bloody husband *art* thou to me.
26 So he let him go: then she said, A bloody husband *thou art*, because of the circumcision.
27 ¶ And the LORD said to Aaron, Go into the wilderness to meet Moses. And he went, and met him in the mount of God, and kissed him.
28 And Moses told Aaron all the words of the LORD who had sent him, and all the signs which he had commanded him.
29 ¶ And Moses and Aaron went and gathered together all the elders of the children of Israel:
30 And Aaron spake all the words which the LORD had spoken unto Moses, and did the signs in the sight of the people.
31 And the people believed: and when they heard that the LORD had visited the children of Israel, and that he had looked upon their affliction, then they bowed their heads and worshipped.

84

Israelites' task increased. EXODUS, 5. Their complaint.

CHAPTER 5.

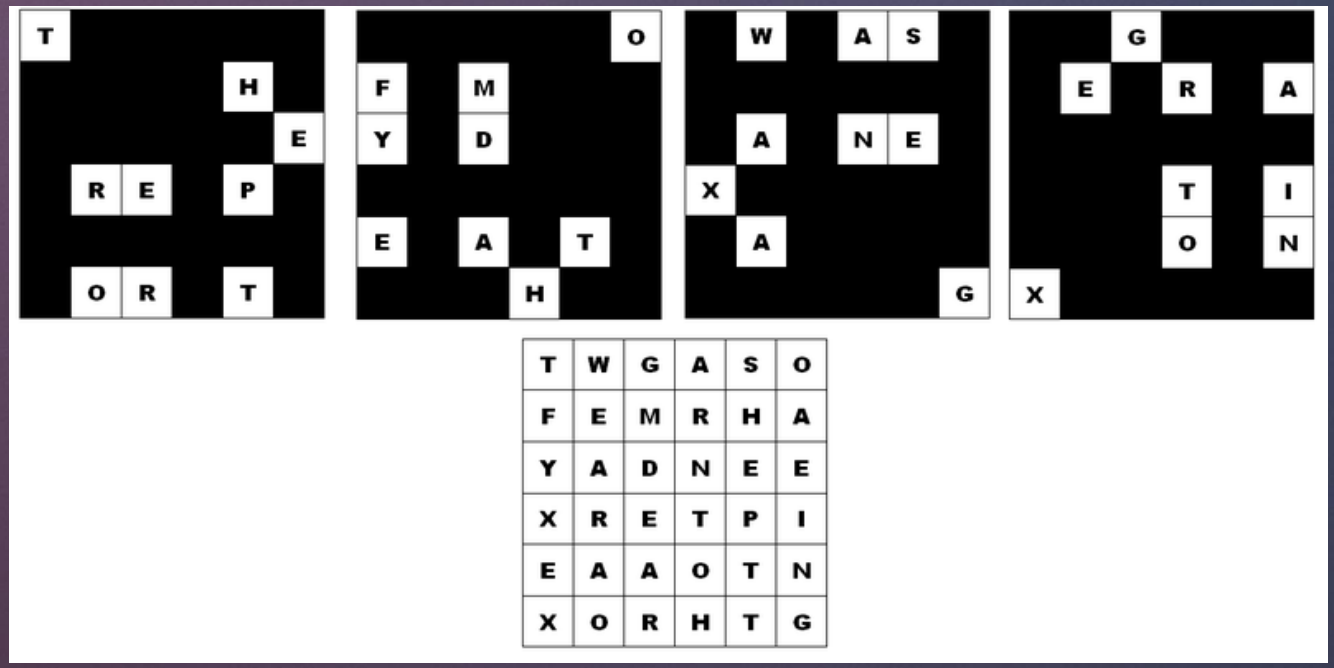
1 *Pharaoh chideth Moses and Aaron for their message.* 5 *He increaseth the Israelites' task.* 15 *He checketh their complaints.* 20 *They cry and upbraid Moses and Aaron.* 22 *Moses complaineth to God.*

AND afterward Moses and Aaron went in, and told Pharaoh, Thus saith the LORD God of Israel, Let my people go, that they may hold a feast unto me in the wilderness.
2 And Pharaoh said, Who *is* the LORD, that I should obey his voice to let Israel go? I know not the LORD, neither will I let Israel go.
3 And they said, The God of the Hebrews hath met with us: let us go, we pray thee, three days' journey into the desert, and sacrifice unto the LORD our God; lest he fall upon us with pestilence, or with the sword.
4 And the king of Egypt said unto them, Wherefore do ye, Moses and Aaron, let the people from their works? get you unto your burdens.
5 And Pharaoh said, Behold, the people of the land now *are* many, and ye make them rest from their burdens.
6 And Pharaoh commanded the same day the taskmasters of the people, and their officers, saying,
7 Ye shall no more give the people straw to make brick, as heretofore: let them go and gather straw for themselves.
8 And the tale of the bricks, which they did make heretofore, ye shall lay upon them; ye shall not diminish *ought* thereof: for they *be* idle; therefore they cry, saying, Let us go *and* sacrifice to our God.
9 Let there more work be laid upon the men, that they may labour therein; and let them not regard vain words.
10 ¶ And the taskmasters of the people went out, and their officers, and they spake to the people, saying, Thus saith Pharaoh, I will not give you straw.
11 Go ye, get you straw where ye can find it: yet not ought of your work shall be diminished.
12 So the people were scattered abroad throughout all the land of Egypt to gather stubble instead of straw.
13 And the taskmasters hasted *them*, saying, Fulfil your works, *your* daily tasks, as when there was straw.
14 And the officers of the children of Israel, which Pharaoh's taskmasters had set over them, were beaten, *and* demanded, Wherefore have ye not fulfilled your task in making brick both yesterday and to day, as heretofore?
15 ¶ Then the officers of the children of Israel came and cried unto Pharaoh, saying, Wherefore dealest thou thus with thy servants?
16 There is no straw given unto thy servants, and they say to us, Make brick: and, behold, thy servants *are* beaten; but the fault *is* in thine own people.
17 But he said, Ye *are* idle, *ye are* idle: therefore ye say, Let us go *and* do sacrifice to the LORD.
18 Go therefore now, *and* work; for there shall no straw be given you, yet shall ye deliver the tale of bricks.
19 And the officers of the children of Israel did see *that* they *were* in evil *case*, after it was said, Ye shall not minish *ought* from your bricks of your daily task.
20 ¶ And they met Moses and

85

Transposition Cipher Examples





online

Results. Guaranteed.

Playfair Substitution Cipher

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

KEYWORD = MONARCHY

Message: ATTACK AT DAWN

AT TA CK AT DA WN

Cipher: **RS SR DE RS BR NY**

Send: **RSSRD ERSBR NYXXX**

online

Results. Guaranteed.

Codes – WWII Navajo Code Talkers



online

Results. Guaranteed.

OFFICERS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Officers	A-la-jih-na-zini	Headmen
Major General	So-na-kih	Two stars
Brigadier General	So-a-la-ih	One star
Colonel	Atsah-besh-le-gai	Silver Eagle
Lt.Colonel	Che-chil-be-tah-besh-legai	Silver Oak Leaf
Major	Che-chil-be-tah-ola	Gold Oak Leaf
Captain	Besh-legai-ne-kih	Two Silver Bars
1st Lieutenant	Besh-legai-a-lah-ih	One Silver Bar
2d Lieutenant	Ola-alah-ih-ni-ahi	One Gold Bar

AIRPLANE NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Airplanes	Wo-tah-de-ne-ih	Air Force
Dive Bomber	Gini	Chicken Hawk
Torpedo Plane	Tas-chizzie	Swallow
Observation Plane	Ne-as-jah	Owl
Fighter Plane	Da-he-tih-hi	Humming Bird
Bomber	Jay-sho	Buzzard
Patrol Plane	Ga-gih	Crow
Transport Plane	Atsah	Eagle

SHIPS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Ships	Toh-dineh-ih	Sea Force
Battleship	Lo-tso	Whale
Aircraft Carrier	Tsidi-ney-ye-hi	Bird Carrier
Submarine	Besh-lo	Iron Fish



Machine Encryption

German Enigma Machine



VINSON Secure Voice System

Half Duplex



online

Results. CYBRARY

PARKHILL

Tactical Secure Voice System - Analog to Digital



online

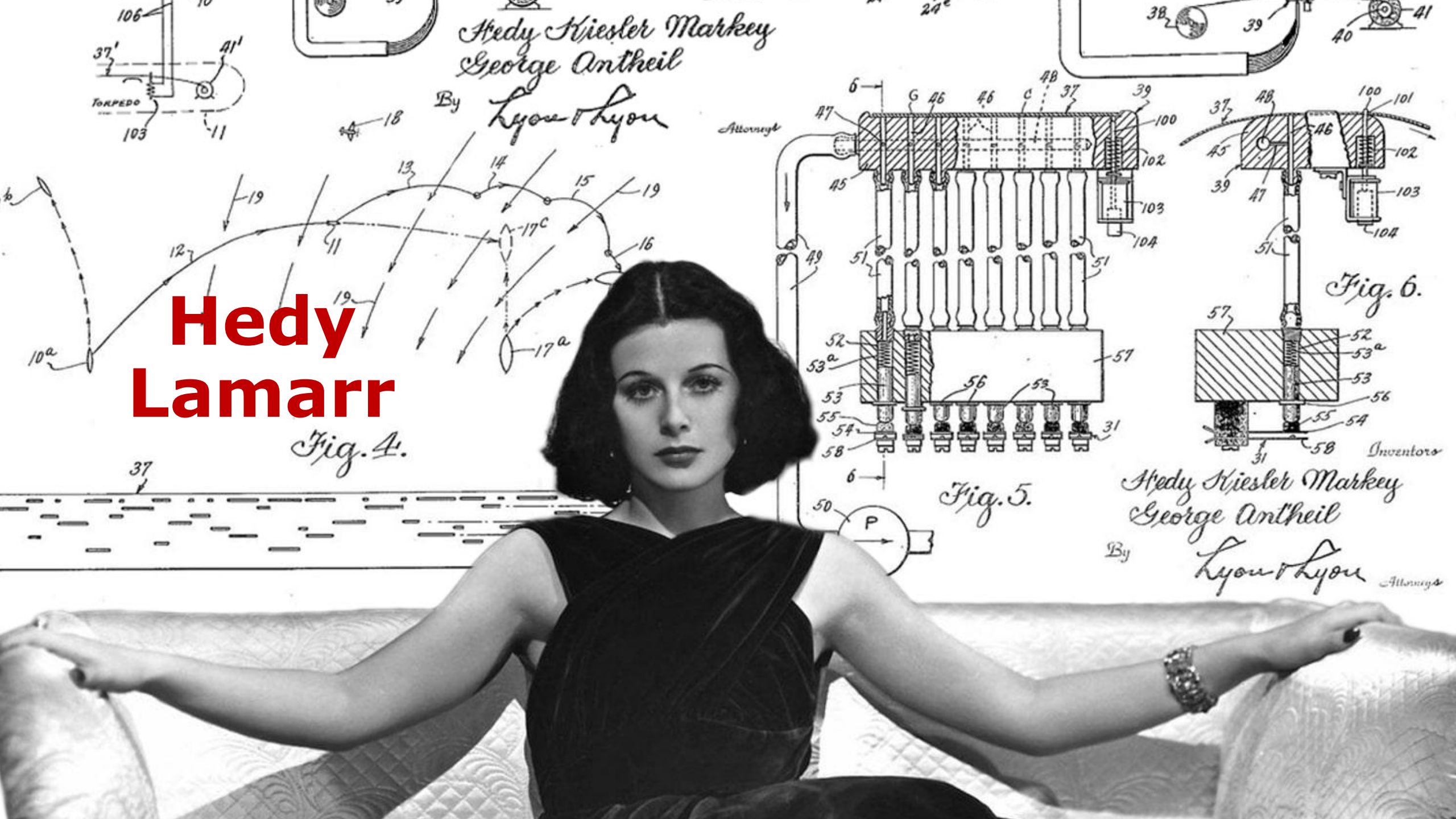
Results. Guaranteed.

SINCGARS – Frequency Hopping Radio



online

CYBRARY
Results. Guaranteed.


Hedy Kiesler Markey
George Antheil
By Lyon & Lyon
Attorneys
Fig. 4.
Fig. 5.
Fig. 6.
Inventors
Hedy Kiesler Markey
George Antheil
By Lyon & Lyon
Attorneys
TORPEDO
Hedy
Lamarr

Key Distribution Systems





online
Results Guaranteed.
CYBRARY

online

Results. Guaranteed.



Early Digital Encryption

online

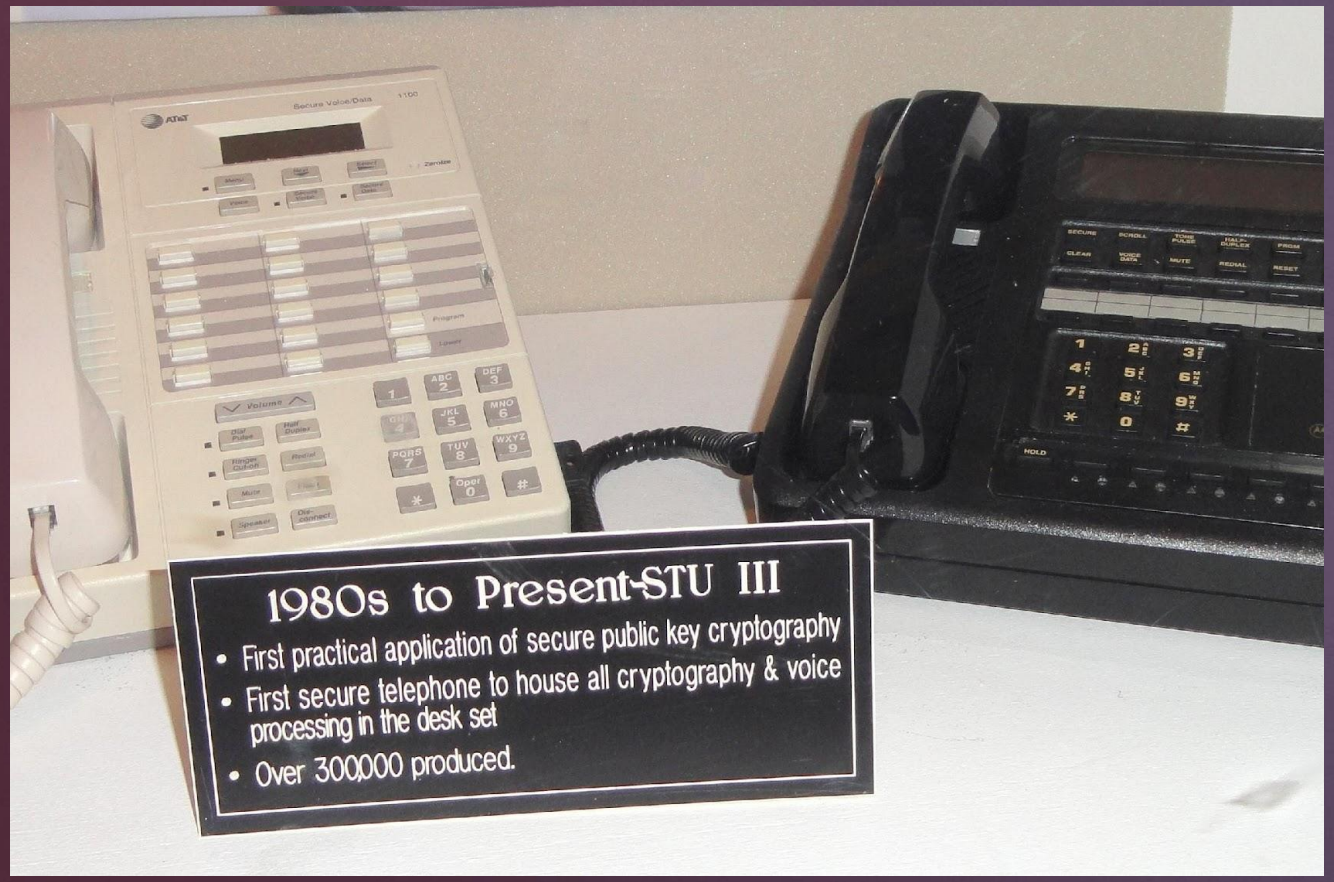
Results. Guaranteed.



Encrypted Cell Phones

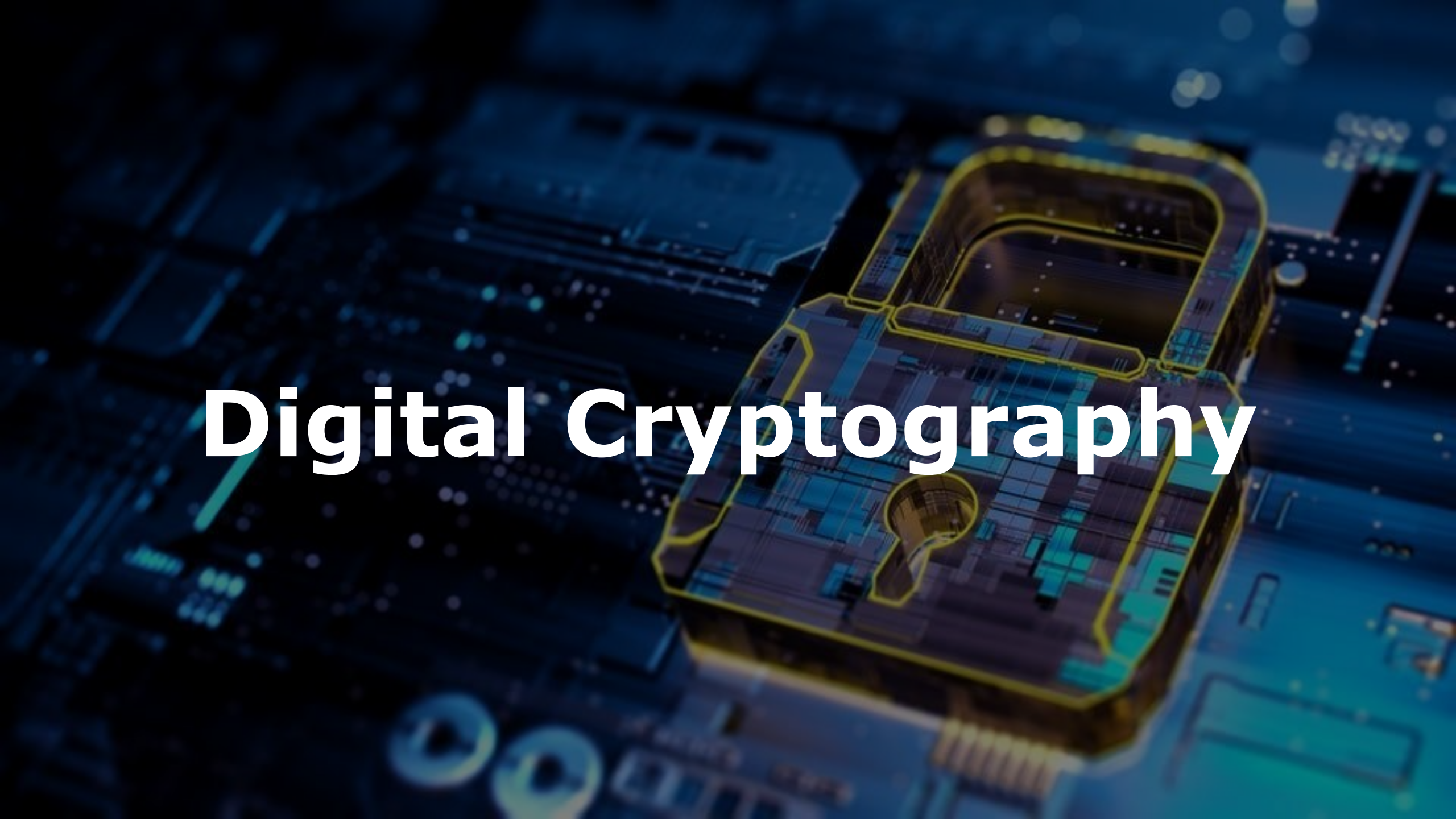
online

Results. Guaranteed.





Secure Voice Communications


Digital Cryptography

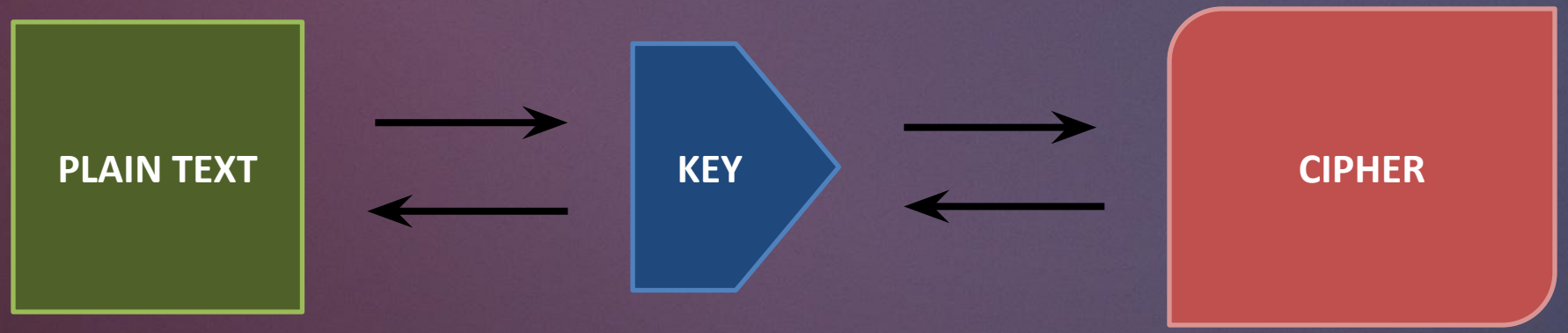
Keeping Secrets in the Digital Era

Reasons to protect data:

1. Confidentiality
2. Integrity
3. Availability
4. ***Non-Repudiation***

Symmetric Encryption

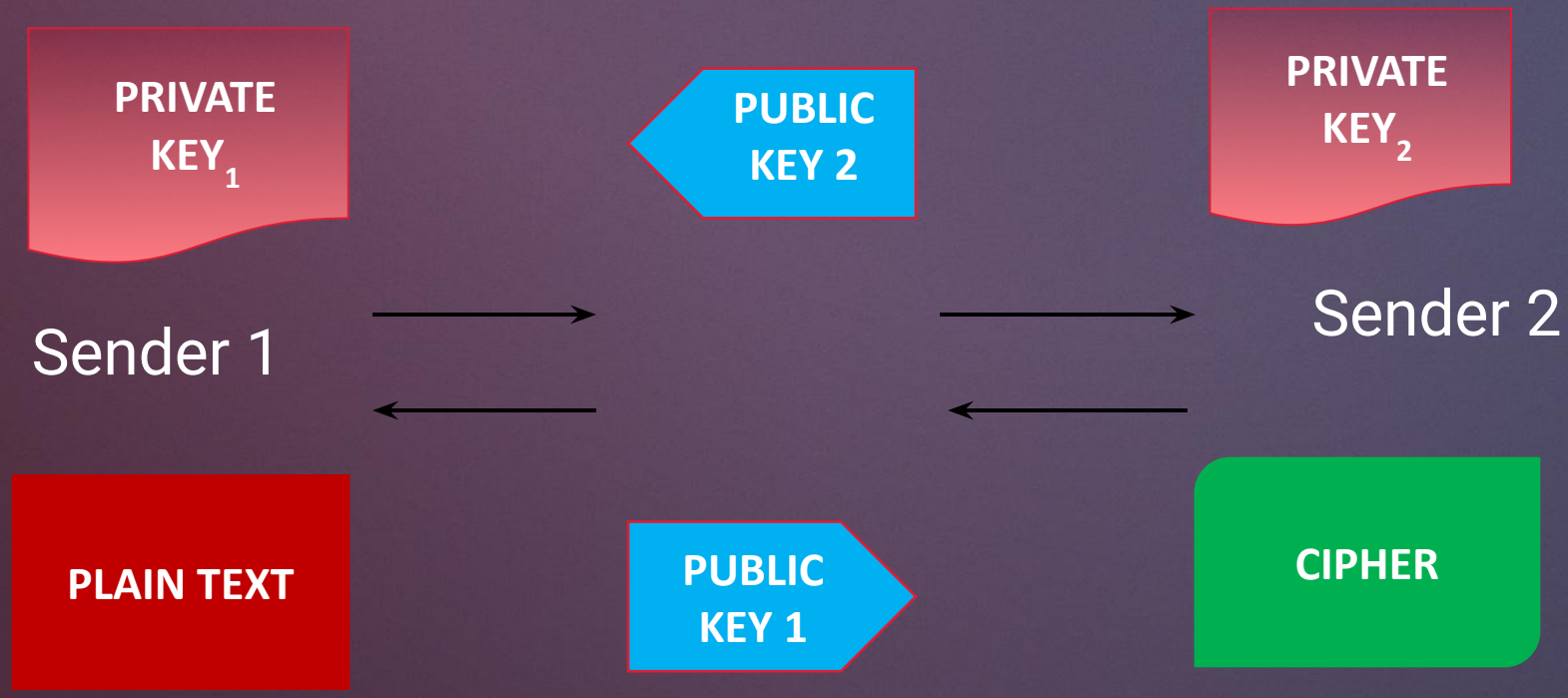
The same key is used by sending and receiving parties to read the message



- Most popular method especially for Internet-based communications, secure websites, VPNs, etc.
- Fast
- Key management
- Latency

Asymmetric Key Encryption (Public Key Cryptography)

Requires Key Pairs:



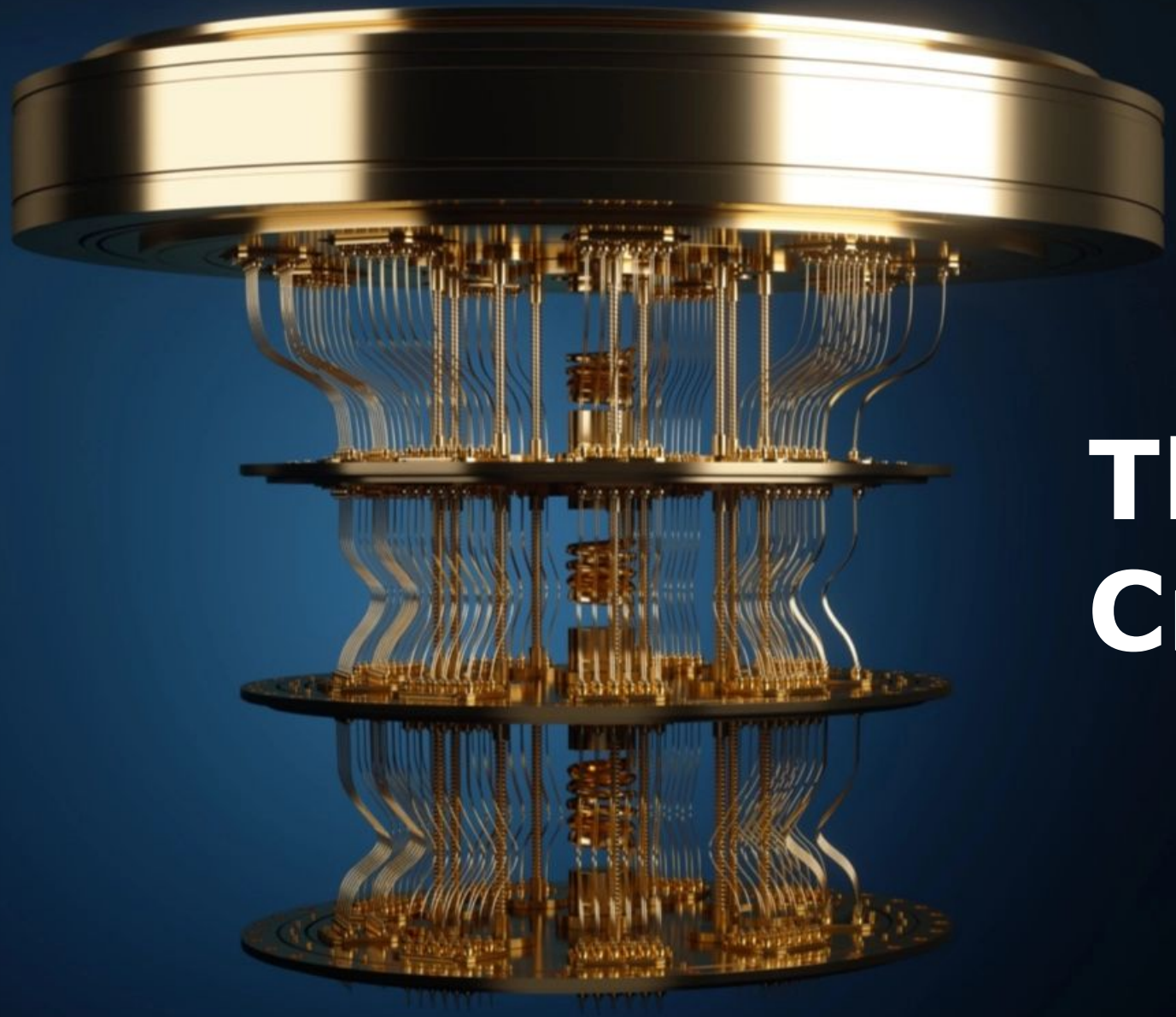
Whitfield Diffie

Dr. Whitfield Diffie is a globally renowned pioneer in computer security, best known for his 1975 joint invention of Public-Key Cryptology. Public Key now underlies all secure electronic commerce and stimulated development of an entirely new class of encryption process.

Another historic Diffie insight was the "digital signature." With this advance, digitally transmitted documents could easily – and for the first time – be irrefutably confirmed and documented, with an immense impact on commerce, as well as command and control systems.

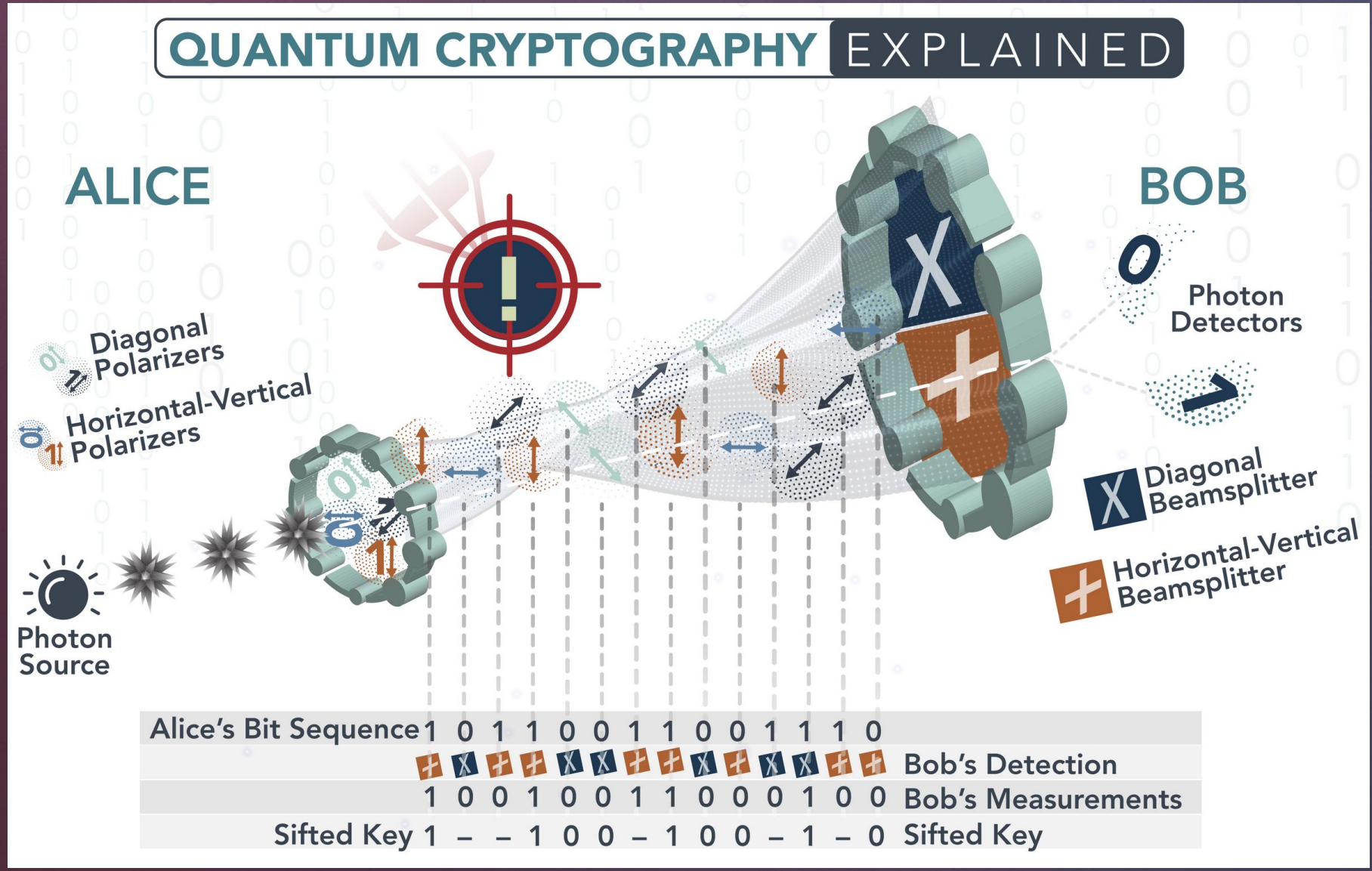
Diffie maintains good relations with NSA, while remaining a respectful critic when necessary. The Phoenix Society inducted him as an honorary member. He has served on the Board of the National Cryptologic Museum Foundation and has made presentations at the biennial Cryptologic History Symposium. Unique among independent cryptographers, Diffie is, in many ways, a member of the NSA family.





The Future of Cryptography

Post-Quantum Cryptography

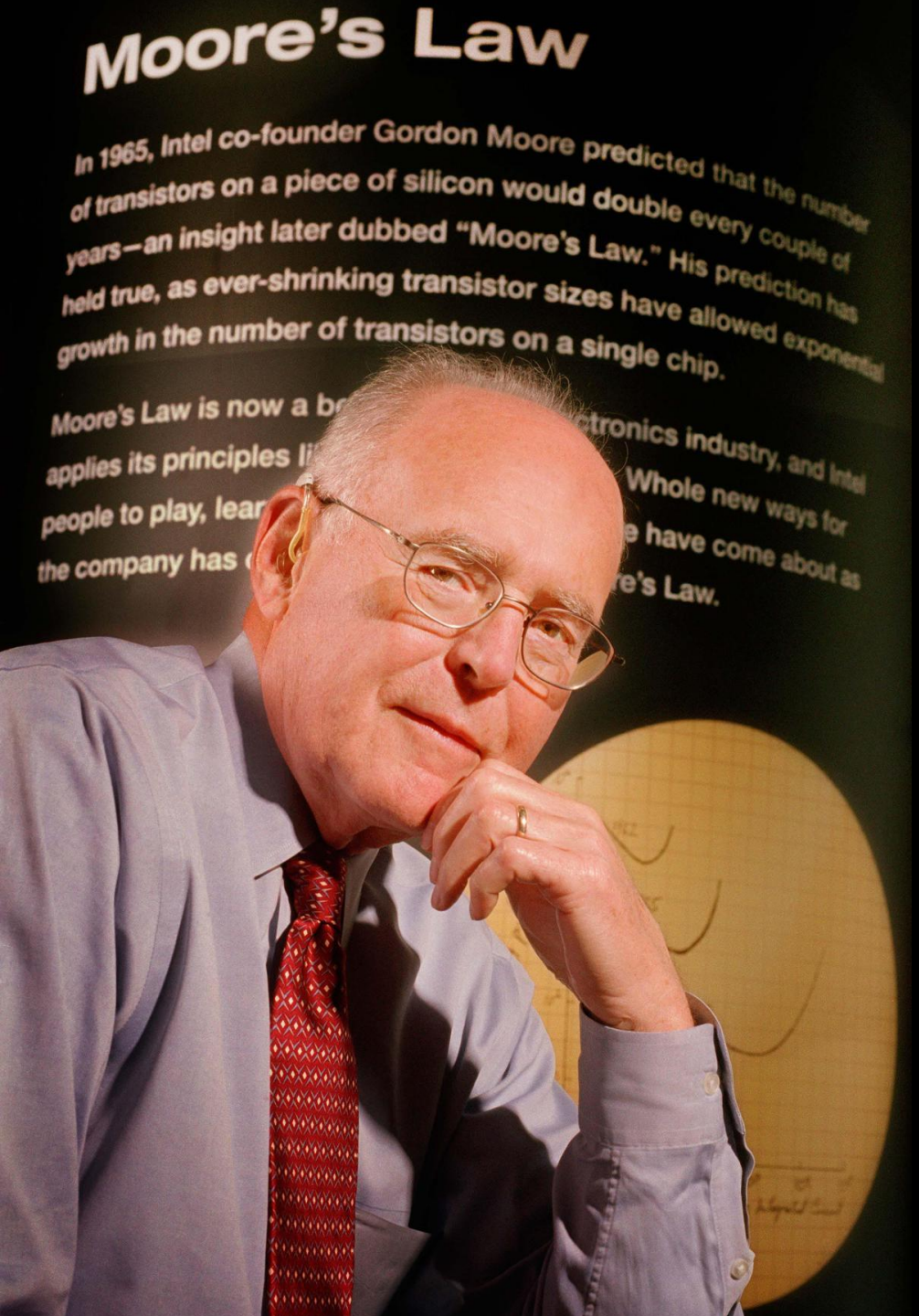


online
Results. Guaranteed.

Moore’s Law

Moore’s law stated and discuss it’s historical context

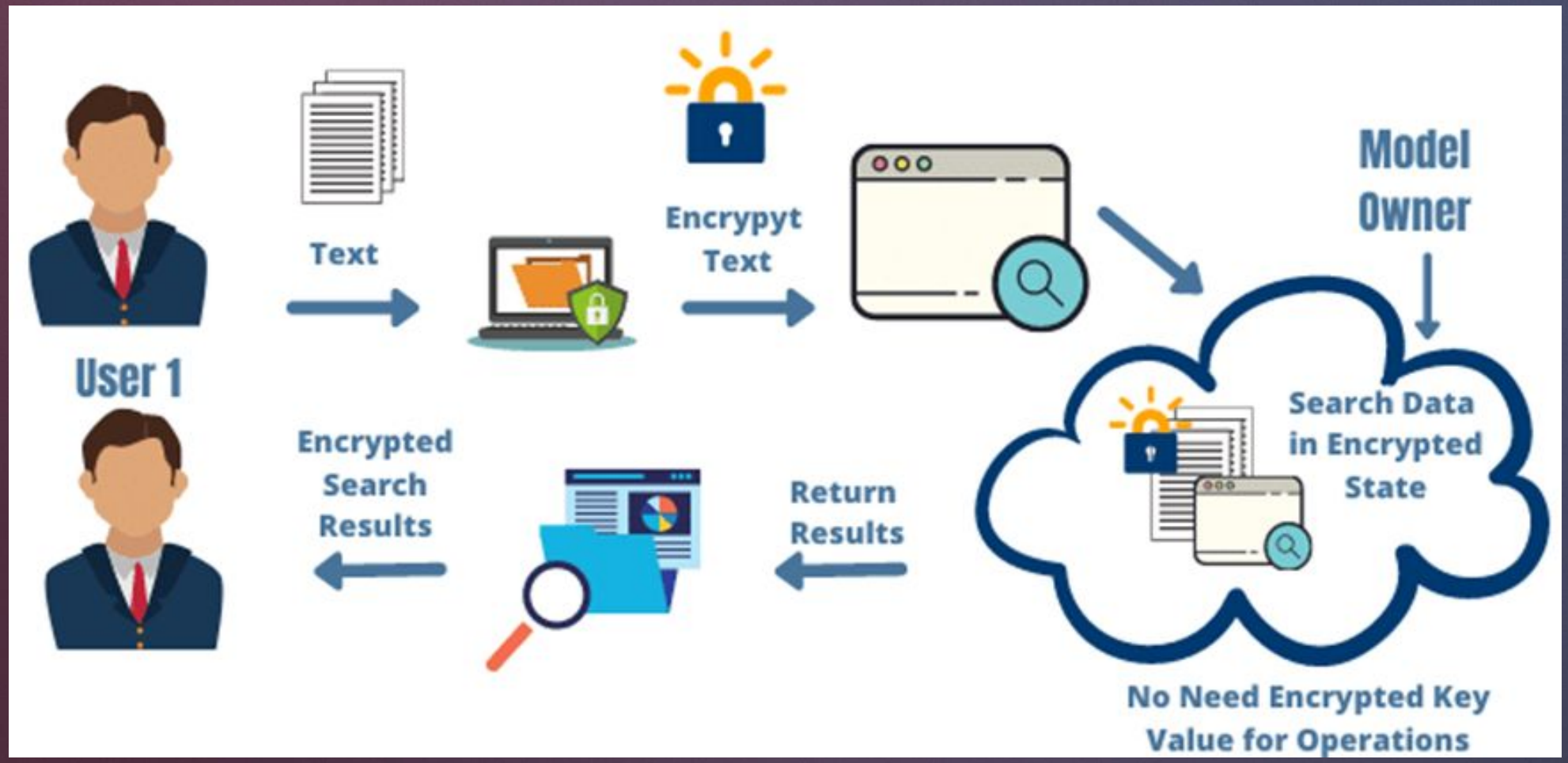
Moore's law is the observation that the number of transistors in an integrated circuit (IC) doubles about every two years. Moore's law is an observation and projection of a historical trend. Rather than a law of physics, it is an empirical relationship linked to gains from experience in production.



Gordon Moore

Moore's law is the observation that the number of transistors in an integrated circuit (IC) doubles about every two years. Moore's law is an observation and projection of a historical trend. Rather than a law of physics, it is an empirical relationship linked to gains from experience in production.

Homomorphic Encryption



The **conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form**.

online
Results. Guaranteed.


Curmudgeon
To Do List:
☑ Coffee
☐ No
☐ Get Off My Lawn
So what's been bothering me?


Security
Weekly
Poland Spring
CYBERSECURITY
MYTHS and
MISCONCEP

Encryption

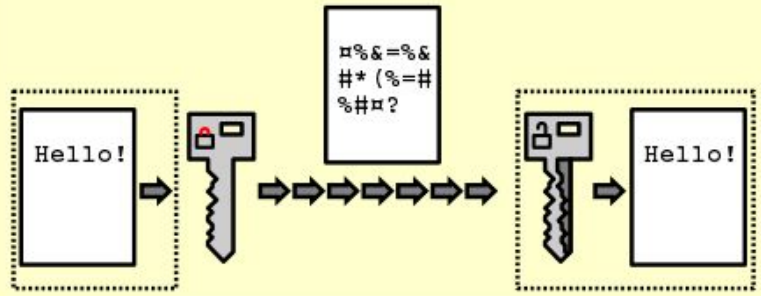
66 languages

From Wikipedia, the free encyclopedia

This article is about algorithms for encryption and decryption. For an overview of cryptographic technology in general, see Cryptography. For the album by Pro-jekt, see Encryption (album).

"Encrypt" redirects here. For the film, see Encrypt (film).

In cryptography, **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.



A simple illustration of public-key cryptography, one of the most widely used forms of encryption

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Also this...

Security.com

encryption

By Peter Loshin

What is encryption?

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called *cryptography*.

In computing, unencrypted data is also known as *plaintext*, and encrypted data is called *ciphertext*. The formulas used to encode and decode messages are called *encryption algorithms,* or *ciphers*.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a *key*, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

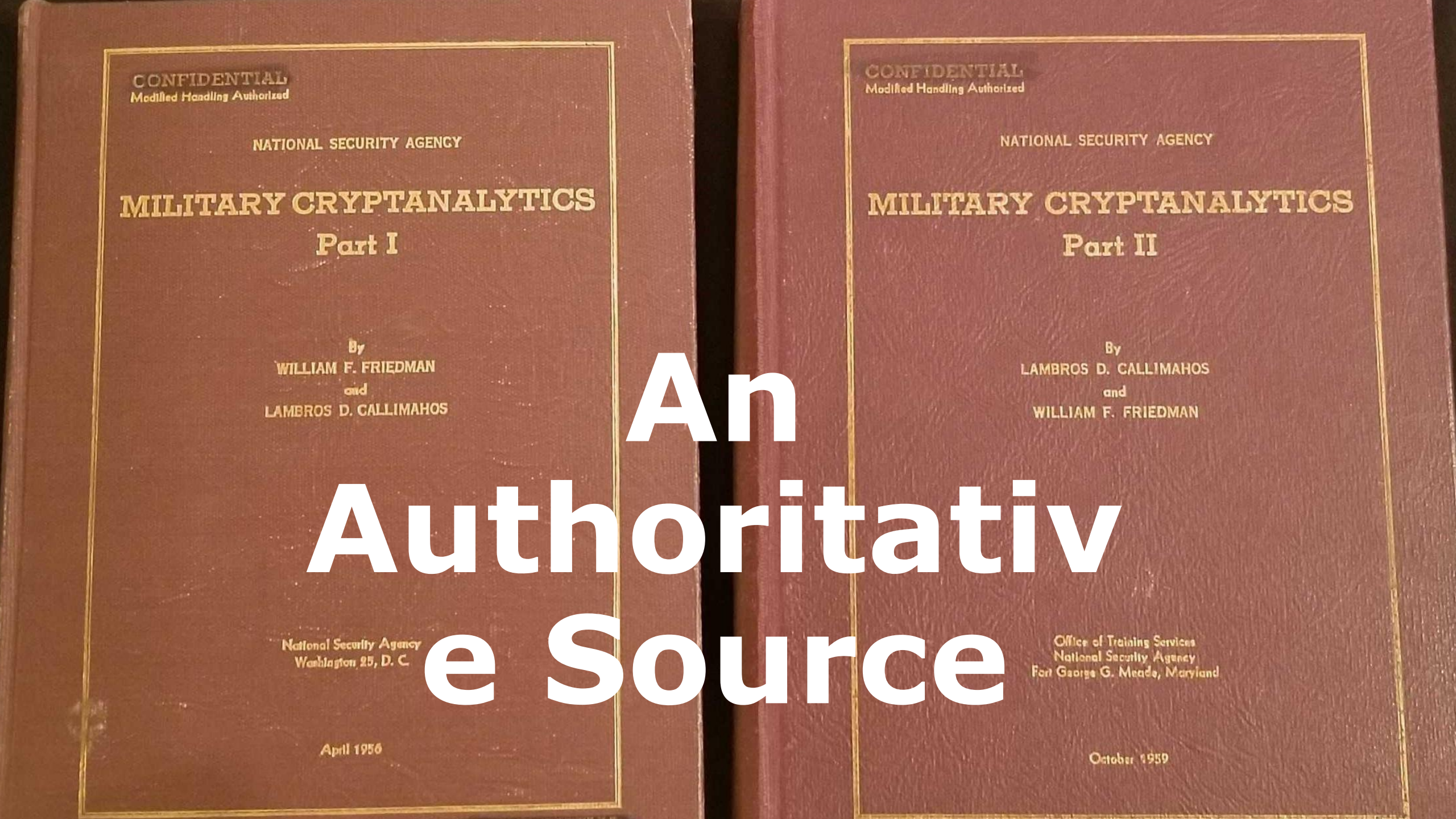
Codes and Ciphers – What's the Difference?

Codes

- Use something completely different to represent letters, numbers, words, phrases
- Can be used to keep secrets
- Often used to make message shorter

Ciphers

- Two kinds
  - Transposition
  - Substitution
- Transposition systems scramble the message in some fashion
- Substitution systems change the original letters to other letters or symbols

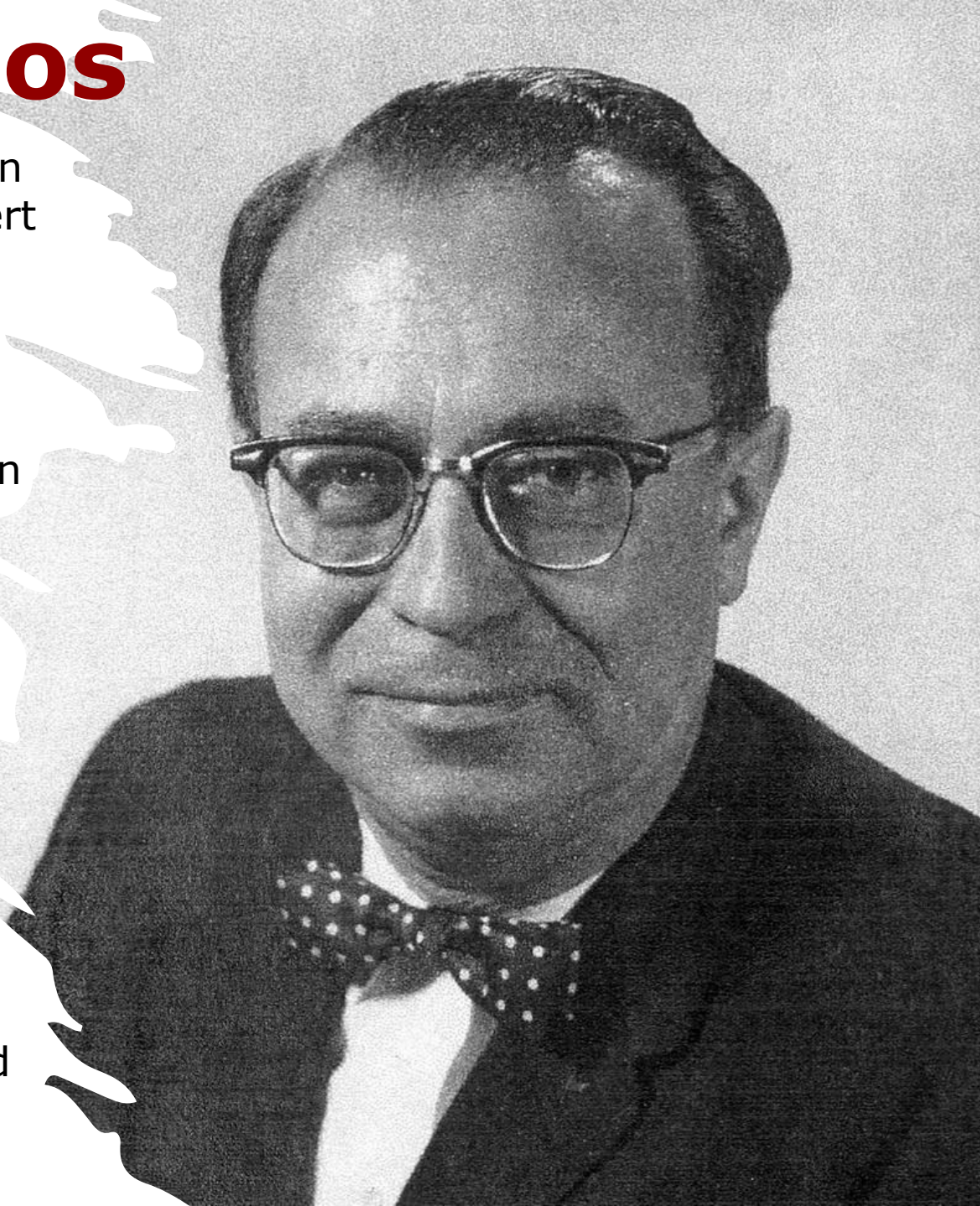

CONFIDENTIAL
Modified Handling Authorized
NATIONAL SECURITY AGENCY
MILITARY CRYPTANALYTICS
Part I
By
WILLIAM F. FRIEDMAN
and
LAMBROS D. CALLIMAHOS
National Security Agency
Washington 25, D. C.
April 1956
CONFIDENTIAL
Modified Handling Authorized
NATIONAL SECURITY AGENCY
MILITARY CRYPTANALYTICS
Part II
By
LAMBROS D. CALLIMAHOS
and
WILLIAM F. FRIEDMAN
Office of Training Services
National Security Agency
Fort George G. Meade, Maryland
October 1959
An
Authoritativ
e Source

Lambros D. Callimahos

Studied law at Rutgers before graduating from Julliard in 1933 with a degree in music. After a few years of concert touring as a flutist, Mr. Callimahos, an avid amateur cryptologist, joined the U.S. Army in 1941 and entered the cryptologic service.

Through the 1950s, Mr. Callimahos collaborated with Friedman on a variety of projects and developed his own famous class CA-400. Graduates of CA-400, the elite among cryptanalysts, became members of the Dundee Society, a society made up by Mr. Callimahos named after the empty Dundee marmalade jar on his desk because he couldn't disclose the real purpose of the group, and played a crucial role in shaping cryptologic development at NSA.

A prolific writer of cryptologic literature, Mr. Callimahos was the author of over 40 books, monographs, and articles. He helped establish NSA's Technical Journal in 1955 and served as technical advisor to the publication for the rest of his career. He wrote articles on codes and ciphers for numerous reference works, including Encyclopedia Britannica.





William F. Friedman

After receiving a B.S. and doing some graduate work in genetics at Cornell University, William Friedman was hired by Riverbank Laboratories, what would today be termed a "think tank," outside Chicago. There he became interested in the study of codes and ciphers, thanks to his concurrent interest in Elizebeth Smith, who was doing cryptanalytic research at Riverbank. Friedman left Riverbank to become a cryptologic officer during World War I, the beginning of a distinguished career in government service.

Friedman's contributions thereafter are well known--prolific author, teacher, and practitioner of cryptology. Perhaps his greatest achievements were introducing mathematical and scientific methods into cryptology and producing training materials used by several generations of pupils. His work affected for the better both signals intelligence and information systems security, and much of what is done today at NSA may be traced to William Friedman's pioneering efforts.

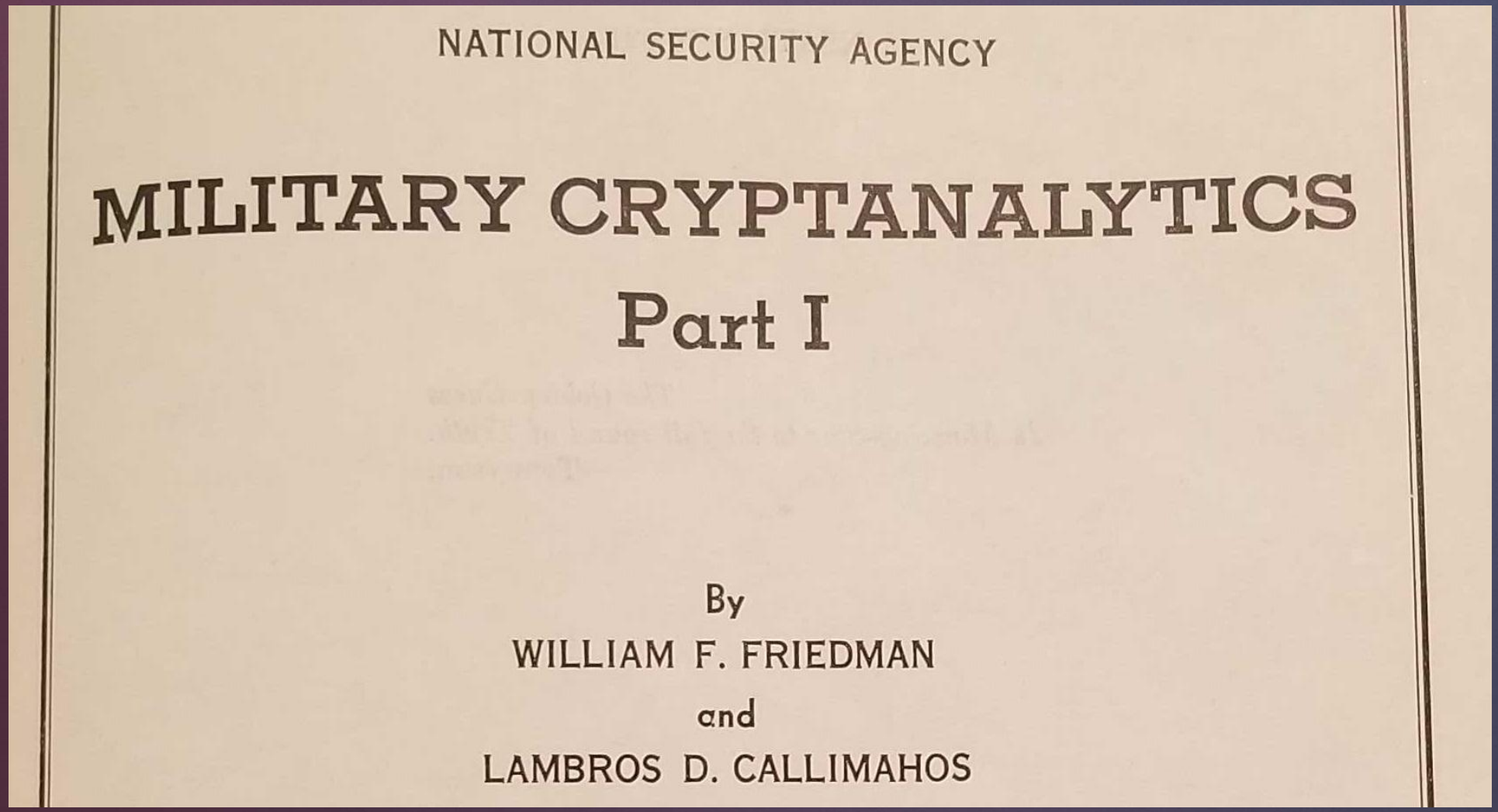
Elizebeth S. Friedman

Elizebeth Smith Friedman--wife, mother, writer, Shakespeare enthusiast, cryptanalyst, and pioneer in U.S. cryptology. Although she is often referred to as the wife of William Friedman, she enjoyed many successes in cryptology in her own right and has been dubbed "America's first female cryptanalyst." In fact, although her husband is credited with numerous contributions to cryptology, it was Mrs. Friedman who introduced him to the field.

Although Mrs. Friedman worked closely with her husband William as part of a team, many of her contributions to cryptology were unique. She deciphered many encoded messages throughout the Prohibition years and solved many notable cases single-handedly, including some codes which were written in Mandarin Chinese. As has been determined, the complexity or difficulty mattered not. After fifty years at her business, Elizebeth Smith Friedman had indeed proved to be a pioneer in code breaking.



“Bible”



NATIONAL SECURITY AGENCY

MILITARY CRYPTANALYTICS

Part I

By

WILLIAM F. FRIEDMAN

and

LAMBROS D. CALLIMAHOS

online

Results. Guaranteed.

Encryption & Decryption

7. **Cryptography, encrypting, and decrypting.**—*a. Cryptography* is that branch of cryptology which treats of various means, methods, and apparatus for converting or transforming plaintext messages into cryptograms and for reconverting the cryptograms into their original plaintext forms by a simple reversal of the steps used in their transformation.

b. To *encrypt* is to convert or transform a plaintext message into a cryptogram by following certain rules, steps, or processes constituting the *key* or *keys* and agreed upon in advance by correspondents, or furnished them by higher authority.

c. To *decrypt* is to reconvert or to transform a cryptogram into the original equivalent plaintext message *by a direct reversal of the encrypting process*, that is, by applying to the cryptogram the key or keys (usually in a reverse order) used in producing the cryptogram.

d. A person skilled in the art of encrypting and

online

Results. Guaranteed.

Codes and Ciphers

c. To *decrypt* is to reconvert or to transform a cryptogram into the original equivalent plaintext message *by a direct reversal of the encrypting process*, that is, by applying to the cryptogram the key or keys (usually in a reverse order) used in producing the cryptogram.

d. A person skilled in the art of encrypting and decrypting, or one who has a part in devising a cryptographic system is called a *cryptographer;* a clerk who encrypts and decrypts, or who assists in such work, is called a *cryptographic clerk.*

8. Codes, ciphers, and enciphered code.—*a.* Encrypting and decrypting are accomplished by means collectively designated as *codes* and *ciphers.* Such means are used for either or both of two purposes: (1) secrecy, and (2) economy or brevity. Secrecy usually is far more important in military cryptography than economy or brevity. In ciphers or *cipher systems*, cryptograms are produced by applying the cryptographic treatment to *individual letters* of the plaintext messages, whereas, in codes or *code systems*, cryptograms are produced by applying the cryptographic treatment to entire *words, phrases, and sentences* of the plaintext messages. The specialized meanings of the terms *code* and *cipher* are explained in detail later (subpar. 11*d*).

b. A cryptogram produced by means of a cipher system is said to be *in cipher* and is called

---

[4] Visible writing may be intelligible but the meaning it obviously conveys may not be its real meaning, that is, the meaning intended to be conveyed. To quote a simple example of an apparently innocent message containing a secret or hidden meaning, prepared with the intention of escaping censorship, the sentence "Son born today" may mean "Three transports left today." Secret communication methods or artifices of this sort are impractical

online

Results. Guaranteed.

Application of a Key

of the characters comprising the code text, thus producing what is called an enciphered code

message, or *enciphered code*. *Encoded cipher*, that is, the case where the final cryptogram is produced by enciphering the plain text and then encoding the cipher text obtained from the first operation, is also possible, but rare.

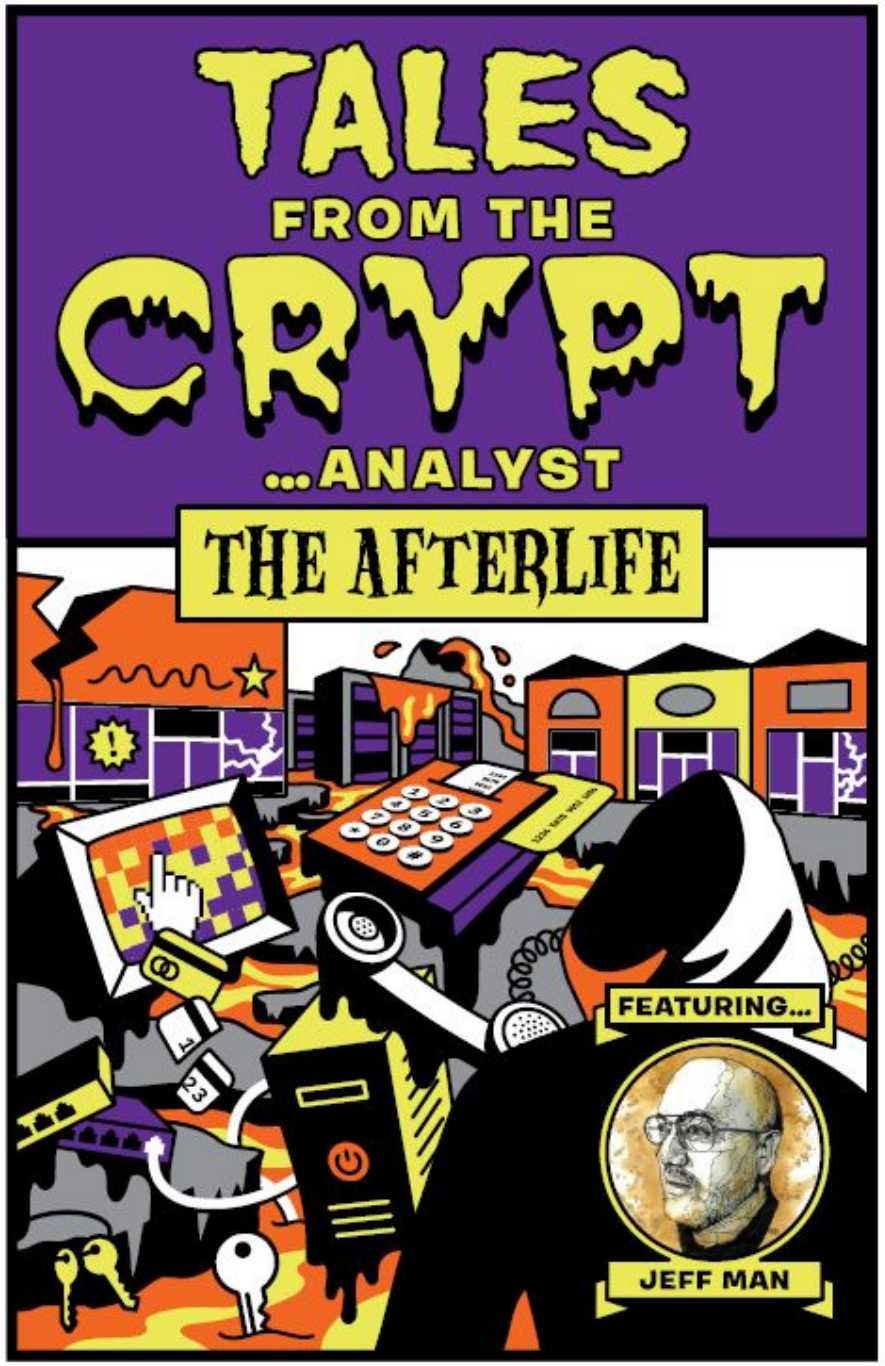
9. **General system, specific key, and cryptosystem.**—*a*. There are a great many different methods of encrypting messages, so that correspondents must first of all be in complete agreement as to which of them will be used in their secret communications, or in different types or classes of such communications. Furthermore, it is to be understood that all the detailed rules, processes, or steps comprising the cryptography agreed upon will be *invariant*, that is, constant or unvarying in their use in a given set of communications. The totality of these basic, invariable rules, processes, or steps to be followed in encrypting a message according to the agreed method constitutes the general cryptographic system or, more briefly, the *general system*.

b. It is usually the case that the general system operates in connection with or under the control of a number, a group of letters, a word, a phrase, or sentence which is used as a *key*, that is, the element which specifically governs the manner in which the general system will be applied in a specific message, or the exact *setting* of a cipher device or a cipher machine at the initial point of encipherment or decipherment of a specific message. This element—usually of a variable nature or changeable at the will of the correspondents, or prearranged for them by higher authority—is called the *specific key*. The specific key may also involve the use of a set of specially prepared tables, a special document, or even a book.

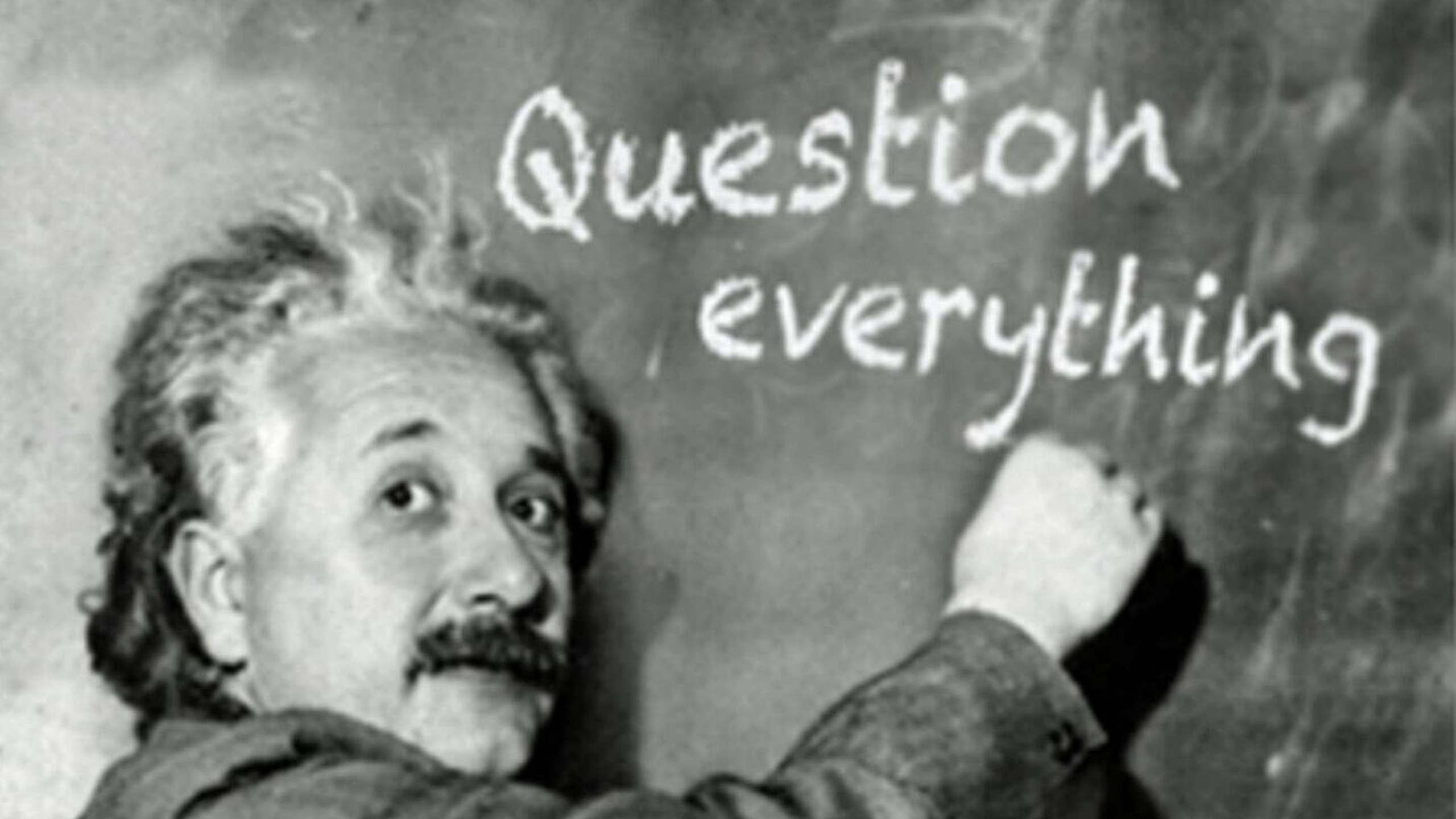
c. The term *cryptosystem*[7] is used when it is desired to designate or refer to all the cryptomaterial (device, machine, instructions for use, key lists, etc.) as a unit to provide a single, com-

online

Results. Guaranteed.



I've got stickers!


Question
everything