LEARN CRYPTOGRAPHY

Blockchain Secrets

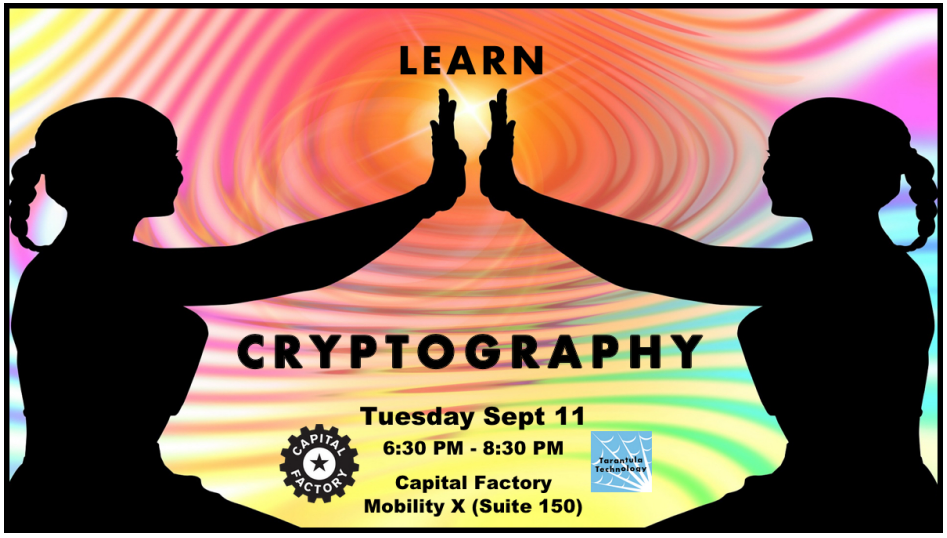
Session 1 of 3

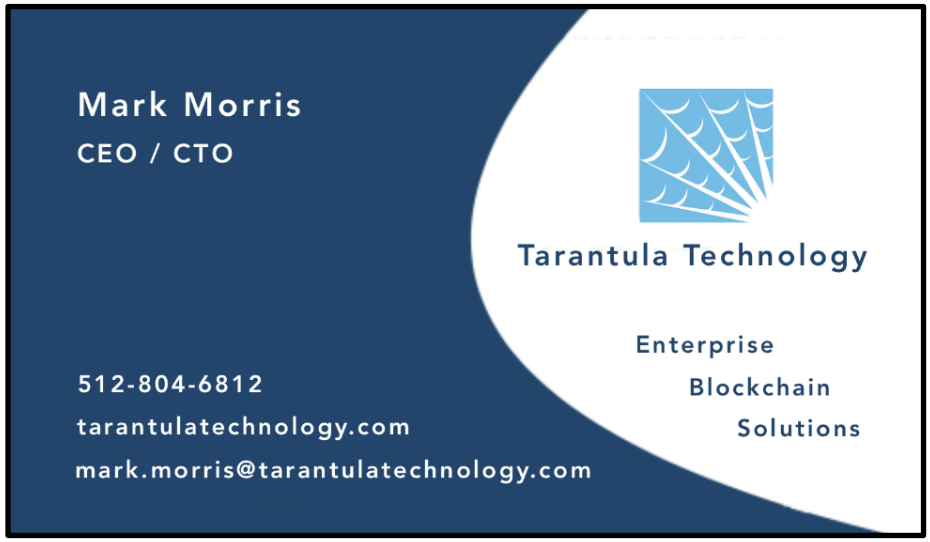
FUNDEMENTALS

Your partner for …

your blockchain consulting, development, and hosting needs.

-Mark





Tarantula Technology

blockchain solutions

"It was the **secrets** of heaven and earth that I desired to learn."

Mary Shelly (1797–1851),
English novelist
— from Frankenstein

Cryptography

Cryptography or cryptology (from Greek κρυπτός kryptós, "**hidden secret**"; and γράφειν graphein, "**writing**", or -λογία -logia, "**study**", respectively) is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

More generally, cryptography is about **constructing and analyzing protocols** that **prevent** third parties or the public from **reading** private messages; various aspects in information security such as **data confidentiality**, **data integrity**, **authentication**, and **non-repudiation** are central to modern cryptography.

Modern cryptography exists at the intersection of the disciplines of **mathematics**, **computer science, electrical engineering, communication science**, and **physics**.

Applications of cryptography include **electronic commerce, chip-based payment cards, digital currencies, computer passwords**, and **military communications**.

A secret created more than **3600** years ago (1800-1600 BCE) that nobody, to this day, has been able to decode!

It exists and is carved on a clay disk, called the **Phaistos** (pronounced **feye-stos**) disk, roughly 16 centimeters (6.3 inches) in diameter, unearthed from the (old) palace of **Phaistos**, one of the most important locations of **Minoan** culture on the island of **Crete**, now part of **Greece**

15 June 1951

MEMORANDUM TO AFSA-14

SUBJECT: Translation of article on Egyptian cryptography

1. There is forwarded herewith for inclusion in the AFSA Technical Library a translation from the French of an article on Ancient Egyptian cryptography by Canon Etienne Drioton, Director of the Museum of Antiquities at Cairo. It is highly interesting history.

2. This translation is one of four translations of articles on historical cryptography which have recently been done for me by Mr. William Heuser of your Division, and I should like to express to you my appreciation for the care with which Mr. Heuser has performed this task, and for his excellent translations.

3. Copies of the translation will be forwarded to you in each instance.

William F. Friedman

WILLIAM F. FRIEDMAN
Technical Consultant

Egyptian Cryptography*

by Canon Étienne Drioton

The marked inclination which the peoples of the East, and the Egyptians in particular, have always shown for enigmas is proverbial. From the Life of Aesop the Phrygian, popularized as an introduction to his own Fables by La Fontaine, everyone knows how Nectanebo, King of Egypt, suggested some enigma contests to Lycerus, King of Babylon. An Egyptian story[1)], the manuscript of which dates from the XIIIth century before Christ, tells how the usurper, Apophis, who ruled at Avaris, had a similar challenge sent to the King of Thebes, Seknenre, the stake being supremacy over all Egypt.

I. Ordinary Cryptography

By ordinary cryptograph is understood that which presents an aspect of hieroglyphic writing and which differs from ordinary writing only in the choice or value of the symbols.

I. Ordinary Cryptography

 (the mouth in profile) replaces  (full-face mouth) = r

 (the house from the side) =  (ground plan of the house) = per

 (the table of offerings with a pitcher and three loaves of bread) replaces  (the table of offerings with a loaf of bread) = hetep

II. Ornamental Cryptography

Another and more elaborate kind of cryptography uses the same fundamental conventions but selects the symbols in such a way as to produce, by means of a number of persons placed one after the other, the impression of a procession decorating frieze. This cryptography can be called ornamental cryptography.

Tarantula Technology
blockchain solutions

II. Ornamental Cryptography

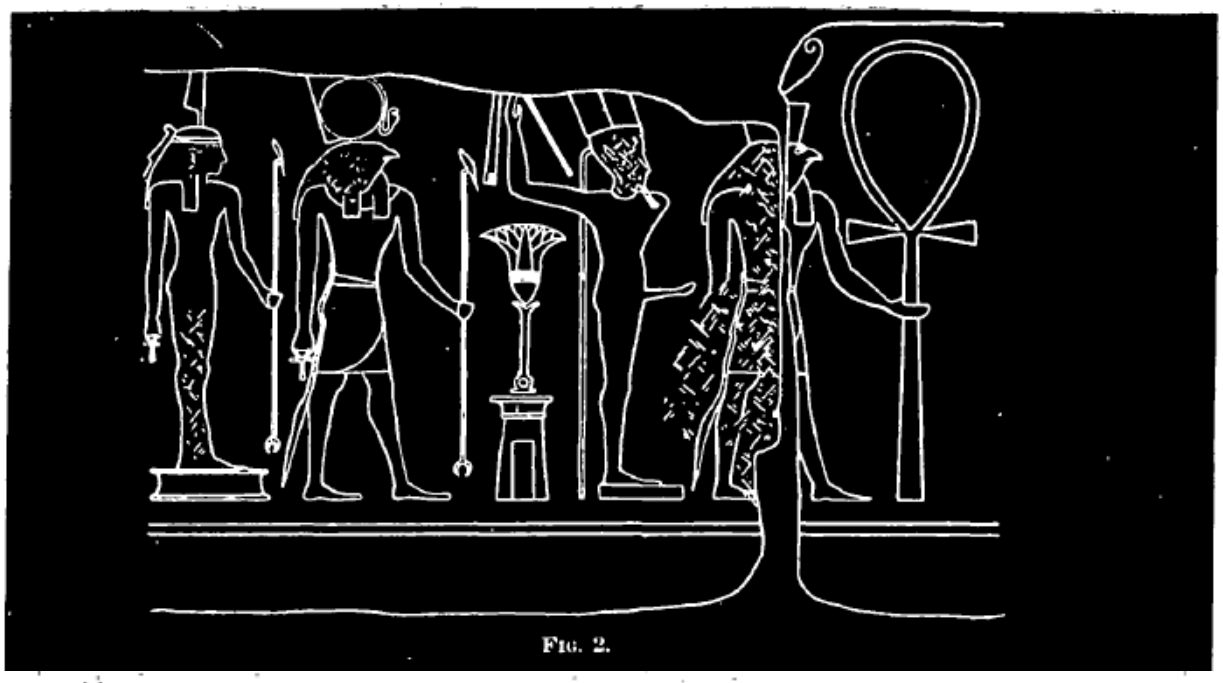


Fig. 2.

Another and more elaborate kind of cryptography uses the same fundamental conventions but selects the symbols in such a way as to produce, by means of a number of persons placed one after the other, the impression of a procession decorating frieze. This cryptography can be called ornamental cryptography.

II. Ornamental Cryptography

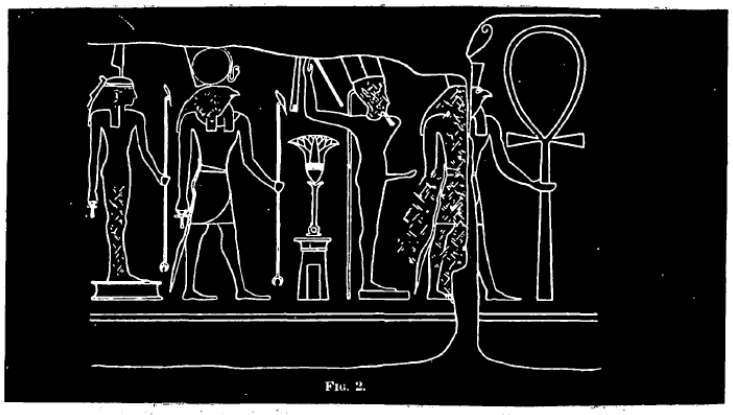


Fig. 2.

The eastern architrave of the first court of the temple at Luxor bears a bas-relief representation, the beginning of which is given in Figure 2.

Actually it is writing and the phrase thus disguised should be read according to the following equivalents: "Long live Horus, the victorious Bull beloved of Justice":

The symbol of life held by Horus the God Kamephis the god Montou	..... by direct representation by antonomasia "the bull" by antonomasia "the Victorious"	ânkh (long live) Her (the Horus) ka (the Bull nekht (victorious)
the phonetic symbol merey supporting the goddess Justice	by direct representation	merey (beloved) naat (of Justice)

III. Thematic Cryptography

Things would have been entirely different and the illusion would have been more difficult to recognize and to shatter if, instead of drawing processions of persons with accessories or extraordinary objects, the ancient cryptographer had been ingenious enough to select his representations in a unique cycle of images and had arranged them systematically in such a way as to form a coherent and plausible scene though without any connection with the concealed meaning of the inscription. Since this cryptography operates on an apparent theme, it is justly called "thematic cryptography". In actuality, it existed in ancient Egypt.

III. Thematic Cryptography

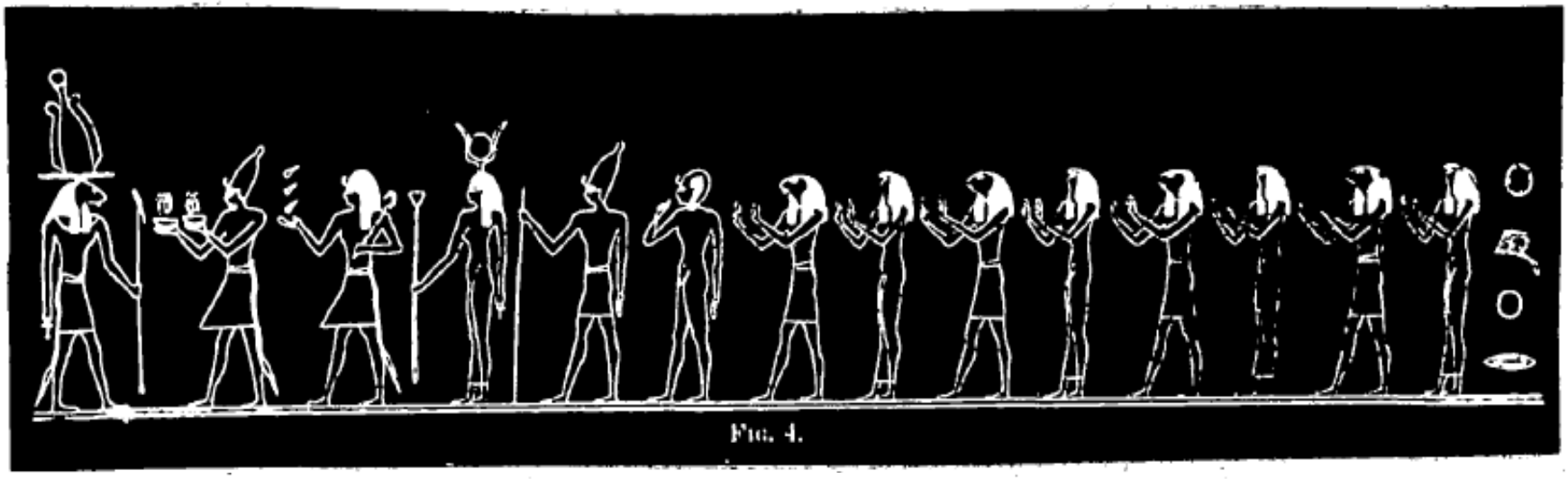


Fig. 4.

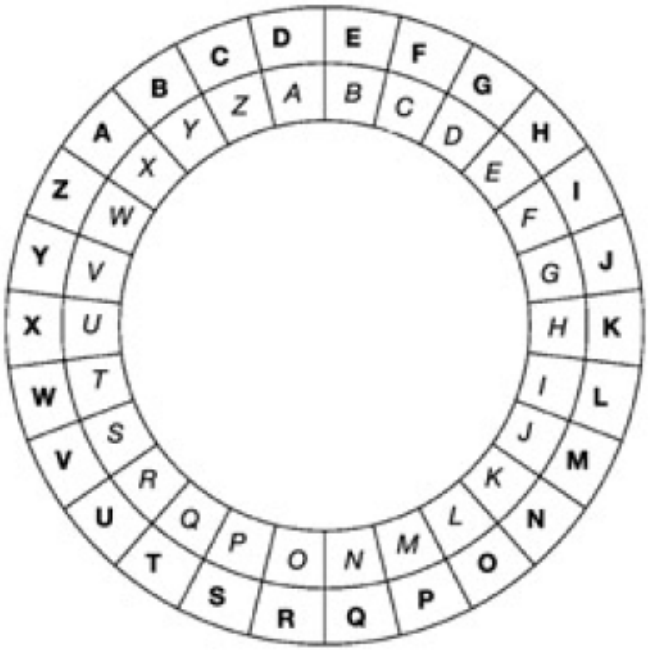
The theme was formed thus:

a man caressing the chin of a woman	mer(ew) "loving" by rebus: mer(ey)	"beloved"
the possession of this woman	netef "he who wets" by rebus: net(y)e(w)f	"of his fellow-citizens"
a harpist singing beside the bed	hes(ev) "singer" by rebus: hes(ey)	"praised"

Plain text: "by the peoples of his province".

Caesar Cipher

One of the earliest examples of a cipher was the Caesar Cipher described by Julius Caesar in the Gallic Wars. In this cipher each of the letters A to W is encrypted by being represented by the letter that occurs three places after it in the alphabet. The letters X, Y, Z are represented by A, B, and C respectively. Although Caesar used a 'shift' of 3, a similar effect could have been achieved using any number from 1 to 25. In fact any shift is now commonly regarded as defining a Caesar Cipher.



Simple Substitution Cipher (monoalphabetic cipher)

For a Simple Substitution Cipher we write the alphabet in a randomly chosen order underneath the alphabet written in strict alphabetical order.
An example is given here.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

The encryption and decryption keys are equal. They are simply the order in which the bold letters are written. The encryption rule is 'replace each letter by the one beneath it' while the decryption rule is the opposite procedure. Thus, for example, for the key in this figure, the cryptogram corresponding to GET is ZTP, while the message corresponding to IYZ is BIG. Note, by the way, that the Caesar Cipher is a special case of a Simple Substitution Cipher where the order in which the bold letters are written is merely a shift of the alphabet.

The statistics of the English language

Letter	%	Letter	%
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	2.0
L	4.0	Y	0.1
M	2.4	Z	0.1

The Playfair Cipher

The Playfair Cipher was invented by Sir Charles Wheatstone and Baron Lyon Playfair in 1854 and was used by the British War Office up to the beginning of the 20th century, including use in the Boer War. It is an example of a 'Bigram' Cipher. This means that letters are encrypted in pairs, as opposed to individually. The key is a 5 by 5 square (with entries comprised of the 25 letters obtained by deleting J from the alphabet) and thus there are 25! Or 15,511,210,043,330,985,984,000,000 keys.

The Playfair Cipher

Before encrypting using a Playfair Cipher the message has to be rearranged slightly. To do this you:

- replace Js with Is;
- write message in pairs of letters;
- do not allow identical pairs - if they occur insert Z between them;
- if the number of letters is odd, add Z to the end.

In order to illustrate how the cipher works we choose a specific key. However, there is nothing special about our choice.

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

The Playfair Cipher

Once the message has been suitably rearranged we give the rule for encryption. In order to clarify our description we extend the key by adding a sixth column and a sixth row to the original key. The sixth row is identical to the first row, while the sixth column is identical to the first column. Thus, for our example, the extended key can be set out as in the diagram.

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

The Playfair Cipher

The rule for encryption is as follows.

- If the two letters lie in the same row of the key then each letter is replaced by the one on its right in the extended key.
- If two letters lie in the same column of the key then each letter is replaced by the one below it in the extended key.
- If the two letters are not in the same row or column then the first letter is replaced by the letter that is in the row of the first letter and the column of the second letter. The second letter is replaced by the fourth corner of the rectangle formed by the three letters used so far.

The Playfair Cipher

We now encrypt the message: GOOD BROOMS SWEEP CLEAN
Since there are no Js in the message we have only to write the message in pairs of letters with the appropriate insertion of extra Zs.

This gives: GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Thus, for our chosen key, GO becomes FP; OD becomes UT; OM becomes PO.

The complete cryptogram is FP UT EC UW PO DV TV BV CM BG CS DY

Simple Substitution Cipher (monoalphabetic cipher)

Homophonic Coding

Another option for improving on the Simple Substitution Cipher might be to expand the alphabet by introducing some extra characters so that, for instance, the plaintext letter E is represented by more than one ciphertext character.

A	*A*	5	C	*D*	*E*	E	F	G	*H*	*I*	7	K	L	M	*N*
01	07	14	21	04	13	17	20	29	31	06	28	12	30	17	00
N	O	O	P	Q	R	R	*S*	T	T	*U*	V	*W*	*X*	F	Z
18	26	19	09	10	25	23	02	08	24	22	05	16	15	11	03

If we do this then the word TEETH, which has two pairs of repeated letters, might be written as 24 17 13 08 31.

Polyalphabetic Ciphers

When a homophonic cipher is used, the frequency histogram of the cryptogram is made flatter by increasing the size of the alphabet. This ensures that more than one ciphertext character may represent the same plaintext character. T

here is always the danger of an attacker compiling a dictionary of known plaintext and ciphertext pairs for a given key.

Another way of achieving the objective of flattening the frequency histogram is by the use of a polyalphabetic cipher. **When a polyalphabetic cipher is used, the ciphertext character replacing a particular plaintext letter may vary through the cryptogram and might, for instance, depend on its position in the plaintext message or the content of the plaintext that precedes it.**

For these ciphers it is now true that the same character may represent different plaintext letters. This is not true for homophonic coding.

Vigenère Ciphers

The Vigenère Cipher is probably the best known of the 'manual' polyalphabetic ciphers and is named after Blaise de Vigenère, a 16th century French diplomat.

Although it was published in 1586, it was not widely recognized until nearly 200 years later and was finally broken by Babbage and Kasiski in the middle of the 19th century.

Vigenère Ciphers

It is interesting to note that the Vigenère Cipher was used by the Confederate Army in the American Civil War.

The Civil War occurred after the cipher had been broken.

This is illustrated by the quotation by General Ulysses S. Grant: 'It would sometimes take too long to make translations of intercepted dispatches for us to receive any benefit from them, but sometimes they gave useful information.'

The Vigenère Cipher uses a Vigenère Square to perform encryption. The left-hand (key) column of this square contains the English alphabet and, for each letter, the row determined by that letter contains a rotation of the alphabet with that letter as the leading character. So each letter in the left-hand column gives a Caesar Cipher whose shift is determined by that letter. Thus, for example, the letter g gives the Caesar Cipher with shift 6.

Vigenère Ciphers

The Vigenère Cipher uses a Vigenère Square to perform encryption.
The left-hand (key) column of this square contains the English alphabet and, for each letter, the row determined by that letter contains a rotation of the alphabet with that letter as the leading character.

So each letter in the left-hand column gives a Caesar Cipher whose shift is determined by that letter.

Thus, for example, the letter g gives the Caesar Cipher with shift 6.

Vigenère Ciphers

Key	Plaintext																							
	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Ciphers

One of the most common methods for using the square to obtain a cipher involves choosing a keyword (or key phrase) with no repeated letters. If the plaintext message is longer than the keyword, then, by repeating the key as often as is necessary, we obtain a sequence of letters which is as long as the message. We then write this sequence of letters beneath our message.

Thus, for example, if our message is PLAINTEXT and our keyword is 'fred' we obtain:

Message P L A I N T E X T
Key f r e d f r e d f

We now use the square to encrypt the message as follows. To encrypt the initial letter P we use the key letter beneath it which, in this case, is f. Thus to encrypt P we go to the row of the square determined by f and read off the letter beneath P, which is U.

Similarly we encrypt L by taking the letter underneath it in the row determined by r, which is C. The process for encrypting P with key letter f is illustrated here.

Vigenère Ciphers

The process for encrypting
P with key letter f is illustrated here.

Key	Plaintext																									
	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Transposition Ciphers

Ciphers which based on the idea of transposing the order in which the letters are written.

These are known as Transposition Ciphers.

Transposition Ciphers

In our example the key is a small number. We use 5 as the key. In order to encrypt a message using this key, we write the key in rows of 5 letters and encrypt by writing the letters of the first column first, then the second column etc. If the length of the message is not a multiple of 5 then we add the appropriate number of Zs at the end before we encrypt. The process is most easily understood by working through a small example.

We encrypt the message WHAT WAS THE WEATHER LIKE ON FRIDAY.
Since the key is 5 the first step involves writing the message in rows of 5 letters.
This is:
WHATW
ASTHE
WEATH
ERLIK
EONFR
IDAY

Transposition Ciphers

Since the length of the message is not a multiple of 5, we must add one Z to get:

WHATW
ASTHE
WEATH
ERLIK
EONFRIDAYZ

We now read down each column in turn to get the following cryptogram:

WAWEEIHSERODATALNATHUFYWEHKRZ

Transposition Ciphers

To obtain the decryption key we merely divide the length of the message by the key.

In this case we divide 30 by 5 to get 6.

The deciphering algorithm is then identical to encryption.

So, for this example, we write the cryptogram in rows of 6 to get:
WAWEEI
HSEROD
ATALNA
THTIFY
WEHKRZ

It is now easy to verify that reading down each column in turn gives the original message.

Transposition Ciphers

Transposition Ciphers of the type given here are easy to break.

Since the key must be a divisor of the cryptogram length, an attacker has only to count the length of the cryptogram and try each divisor in turn.

Modular arithmetic

Modular arithmetic is only concerned with integers, commonly known as whole numbers. If N is a positive integer, then arithmetic modulo N uses only the integers 0, 1, 2, 3,..., N-1, that is, integers from 0 to N-1.

There are a number of values of N for which arithmetic modulo N is common to most people, although they may not be familiar with the mathematical terminology.

For instance when we use a 12-hour clock we use addition modulo 12. If it is now 2 o'clock then everyone 'knows' that the time in 3 hours is 5 o'clock, as it will also be in 15 hours.

This is because 15 = 12 + 3 and the time repeats every 12 hours.

Other natural numbers are N = 7 (for the days of the week) and N = 2 (for odd and even).

Historic Events

Mary Queen of Scots used a variant of the Simple Substitution Cipher in secret letters in the 16th century. This correspondence contained her plans both to escape from imprisonment and to assassinate Queen Elizabeth of England so that she could claim the English throne. The letters were intercepted, decrypted, and used as evidence in her trial. Mary and her conspirators openly discussed their plans in these encrypted letters, as they believed no one else would be able to read them. It was an error that cost Mary her life.

The German armed forces in the Second World War used a device called an Enigma machine to encrypt much of their important and unimportant military traffic. The mechanisms used by Enigma for encryption appear intricate and complicated, and a basic Enigma machine had over 1020 possible keys which is more than some modern algorithms. This led the users to believe that Enigma was unbreakable. As is now well known, the Allied Forces were at various times able to break Enigma, partially exploiting usage and key management mistakes.

Perfect secrecy

When the number of keys is the same as the number of messages, the chances of guessing correct are equal.

This is perfect secrecy.

The one-time pad

A perfectly secure cipher system is the one-time pad. If the message is a passage of English text containing n letters with all punctuation and spaces removed, then the key, which is only used once to protect a single message, is a randomly generated sequence of n letters from the alphabet.

The encryption rule is precisely that used for the Vigenère Cipher with the key replacing the keyword. Thus, if we associate each letter A to Z with the numbers 0 to 25 in the usual way, for message m1, m2,..., mn and key k1, k2,..., kn, the ith component of the cryptogram is given by: $ci = (mi + ki) \bmod 26$

Note that the fact that the key is the same length as the message guarantees that there is no need to start repeating the key during the encryption process.

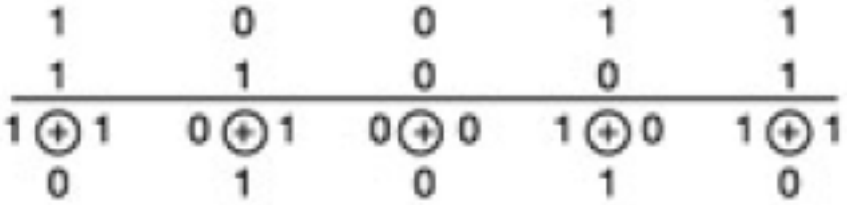
Another common version of this algorithm often called a Vernam Cipher where the alphabet used is binary, that is 0 and 1, and the cryptogram is obtained by adding the message and key modulo 2. For digital communications, the Vernam Cipher is almost certainly the version of the one-time pad that is used.

Modern Algorithms

Bit-strings 000=0, 001=1, 010=2, 011 = 3, 100=4, 101=5, 110=6, 111 = 7

In general a binary sequence of length n can be regarded as representing an integer from 0 to 2n - 1 and so, once we have agreed a block length s, an arbitrarily long binary sequence may be written as a sequence of integers in the range 0 to 2s - 1

XOR



0000 = 0	0001 = 1	0010 = 2	0011 = 3
0100 = 4	0101 = 5	0110 = 6	0111 = 7
1000 = 8	1011 = 9	1010 = A	1011 = B
1100 = C	1101 = D	1101 = E	1111 = F.

Modern Algorithms

Stream ciphers

The message is enciphered word by word (or character by character), where the rule for the encryption of each word (character) is determined by its position in the message--the plaintext is enciphered bit by bit.

Modern Algorithms

Block ciphers

For a block cipher, the bit-string is divided into blocks of a given size and the encryption algorithm acts on that block to produce a cryptogram block that, for most symmetric ciphers, has the same size.

Modern Algorithms

Hash functions

The basic idea of a hash function is that the resultant hash value is a condensed representative image of the message. The hashed value has a number of names including digital fingerprint, message digest, or, not surprisingly, a hash. Hashing has a number of applications, including the provision of data integrity and as part of the digital signature process.

In general hash functions accept inputs of arbitrary length but produce outputs of a fixed length.

Modern Algorithms

Public key systems

With symmetric algorithms the sender and receiver share a secret key. This, of course, implies trust between the two parties. Prior to the late 1970s, these were the only algorithms available.

The basic idea of a public key cryptosystem is that each entity has a public key and a corresponding private key. These keys are chosen so that it is practically impossible to deduce the private key from the public key. Anyone wishing to use this system to send a secret message to someone else needs to obtain that person's public key and use it to encrypt the data.

Modern Algorithms

Practical exhaustive key searches

In order to get some feel for sizes we note that there are 31,536,000 seconds in a year which is somewhere between 2^24 and 2^25.

If someone were able to try one key per second, then it would take them over a year to complete a search through 2^25 keys.

If, however, they had a computer capable of trying a million keys per second, the time required to search through 2^25 keys would be significantly less than a minute.

Modern Algorithms

Practical exhaustive key searches

The most well-known symmetric block cipher is the Data Encryption Standard (DES).

It was published in 1976 and has been widely used by the financial sector.

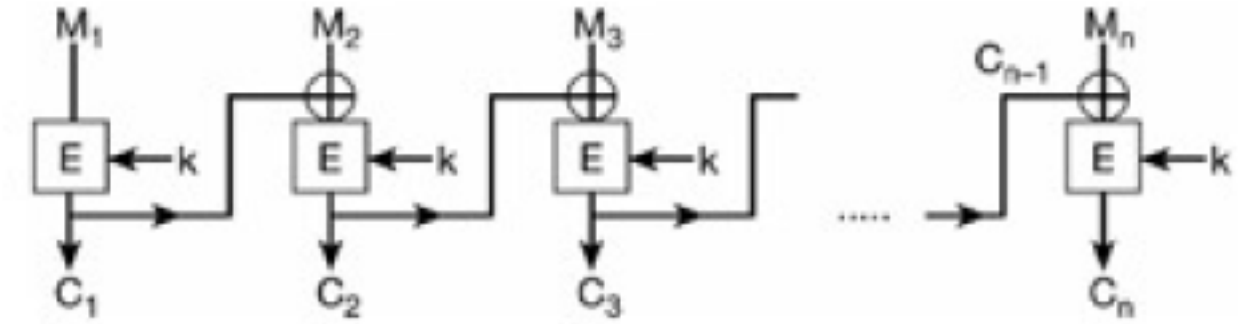
DES has 2^56 keys and, ever since it was first released, there have been arguments about whether or not it can be regarded as strong.

In 1998, an organization called the Electronic Frontier Foundation (EFF) designed and built a dedicated piece of hardware to conduct exhaustive DES key searches.

For $250,000 it is possible to build a machine that completes a search through 2^56 keys in about a week.

Modern Algorithms

Using symmetric algorithms for confidentiality



Cipher Block Chaining

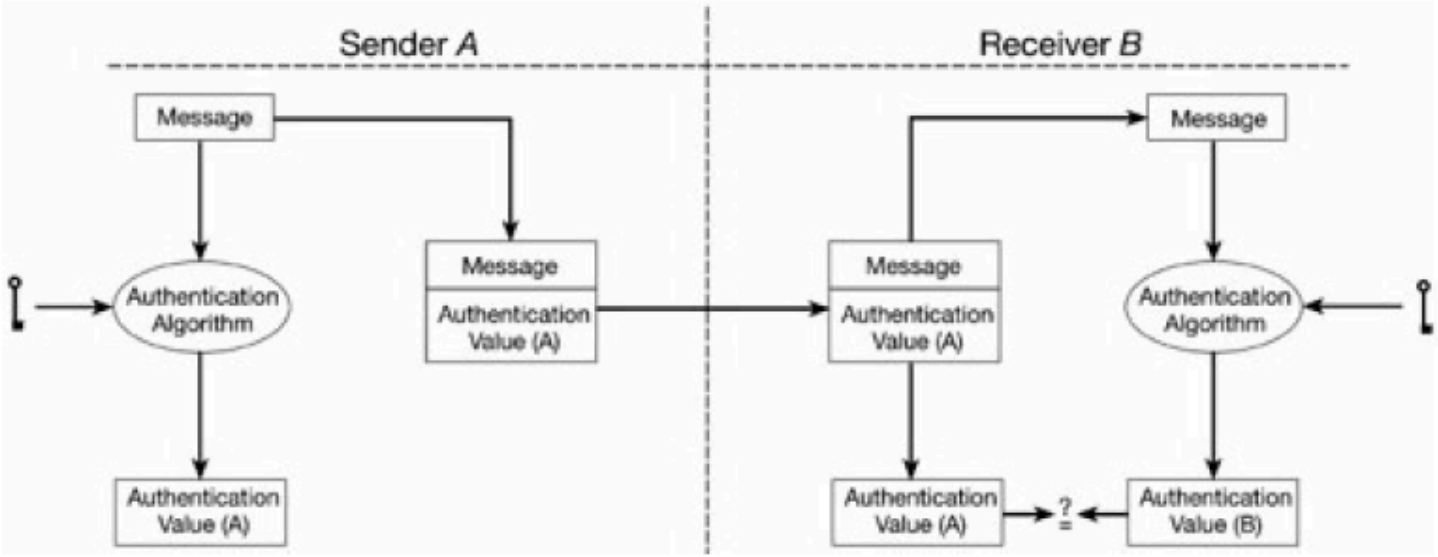
Modern Algorithms

Authentication

- something known: this might, for example, be a password or a PIN that the user keeps secret;
- something owned: examples include plastic cards or hand-held personalized calculators;
- some characteristic of the user: these include biometrics, such as fingerprints and retina scans, hand-written signatures or voice recognition.

Modern Algorithms

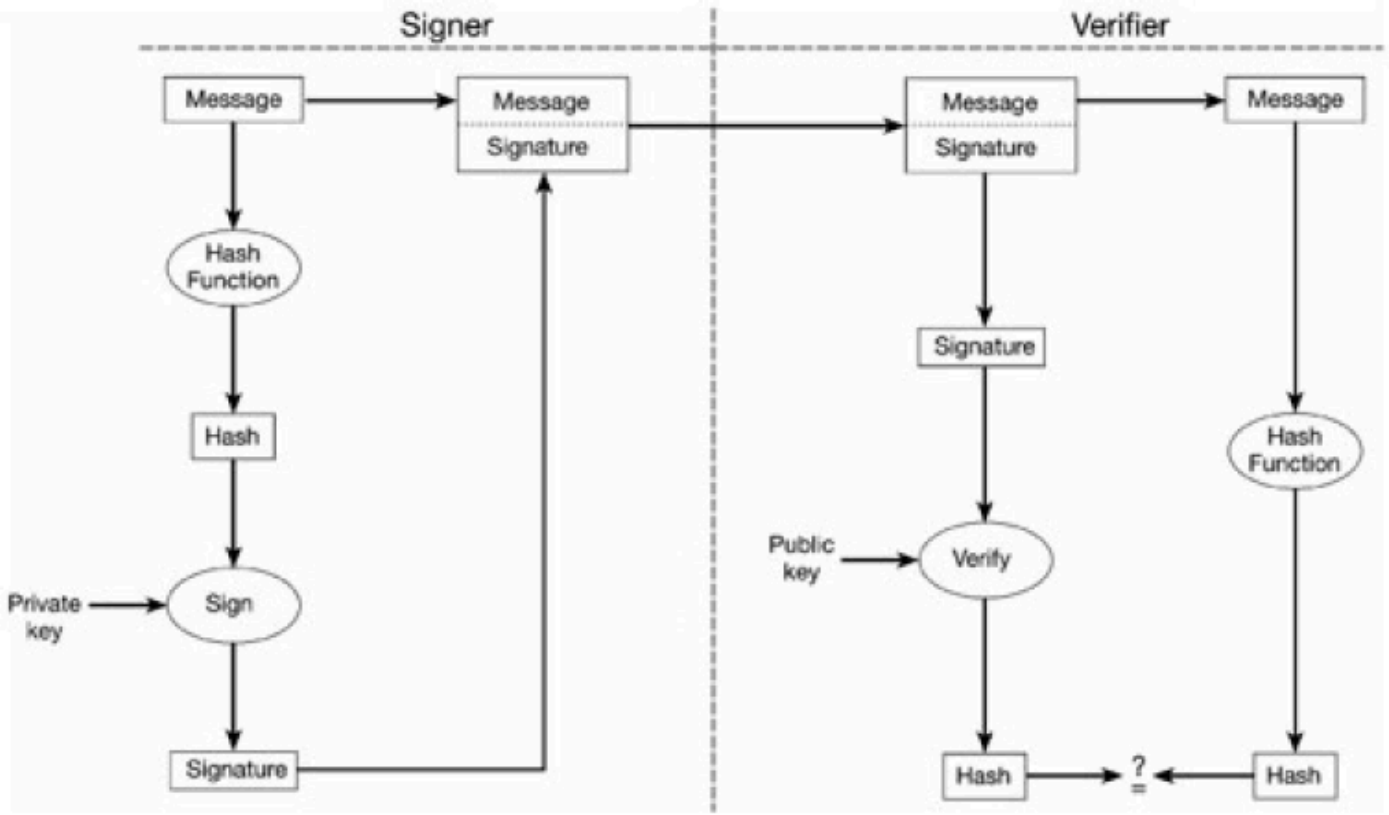
Using symmetric algorithms for authentication and data integrity



Authentication with symmetric authentication

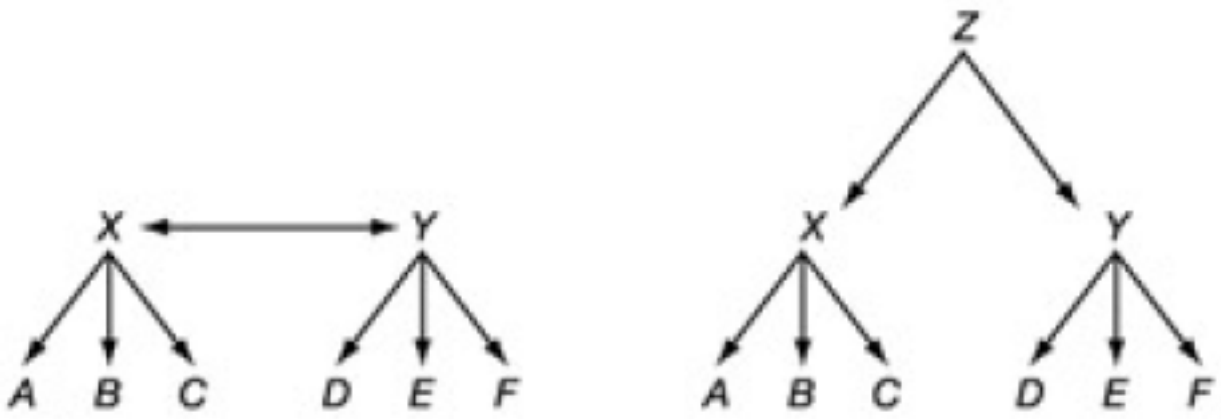
Modern Algorithms

Digital signatures



Modern Algorithms

Certification authorities



(a)
Cross certification

(b)
A certification hierarchy

Modern Algorithms

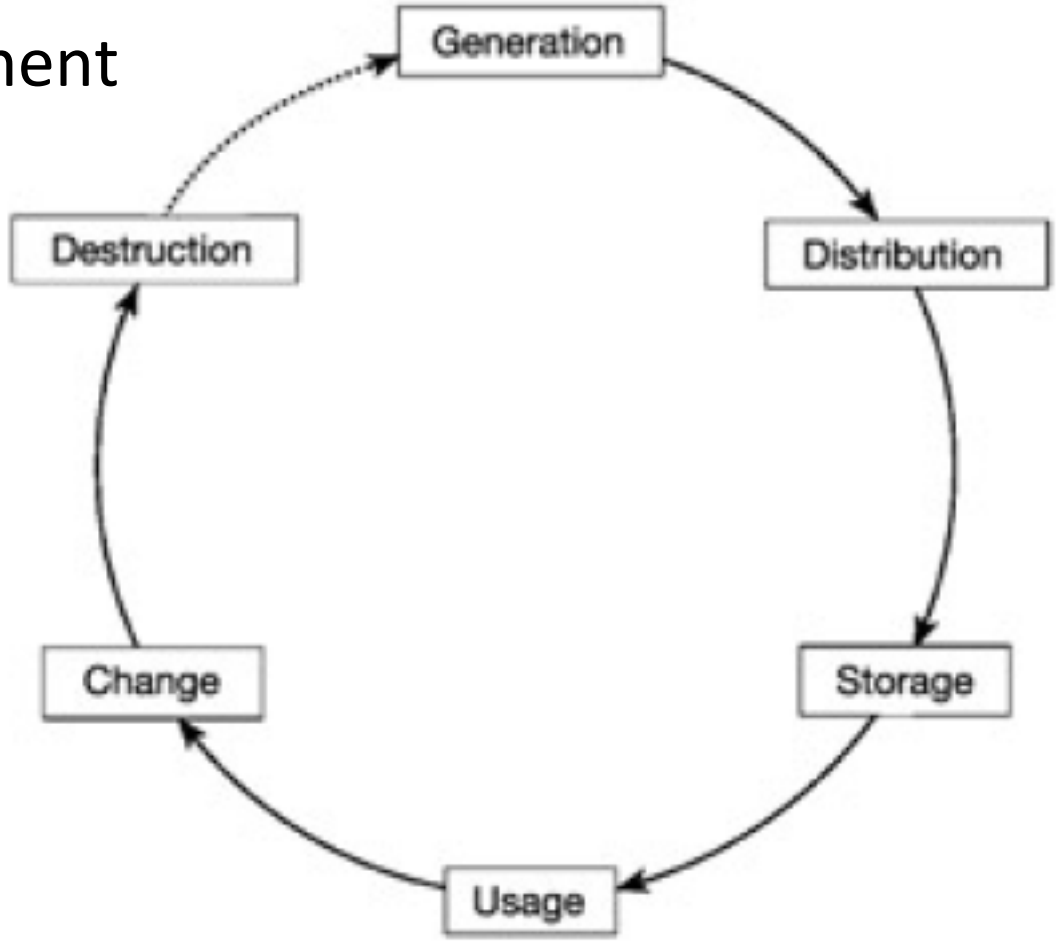
Public Key Infrastructure

When a PKI is established, the following processes need to take place, though not necessarily in the order listed:

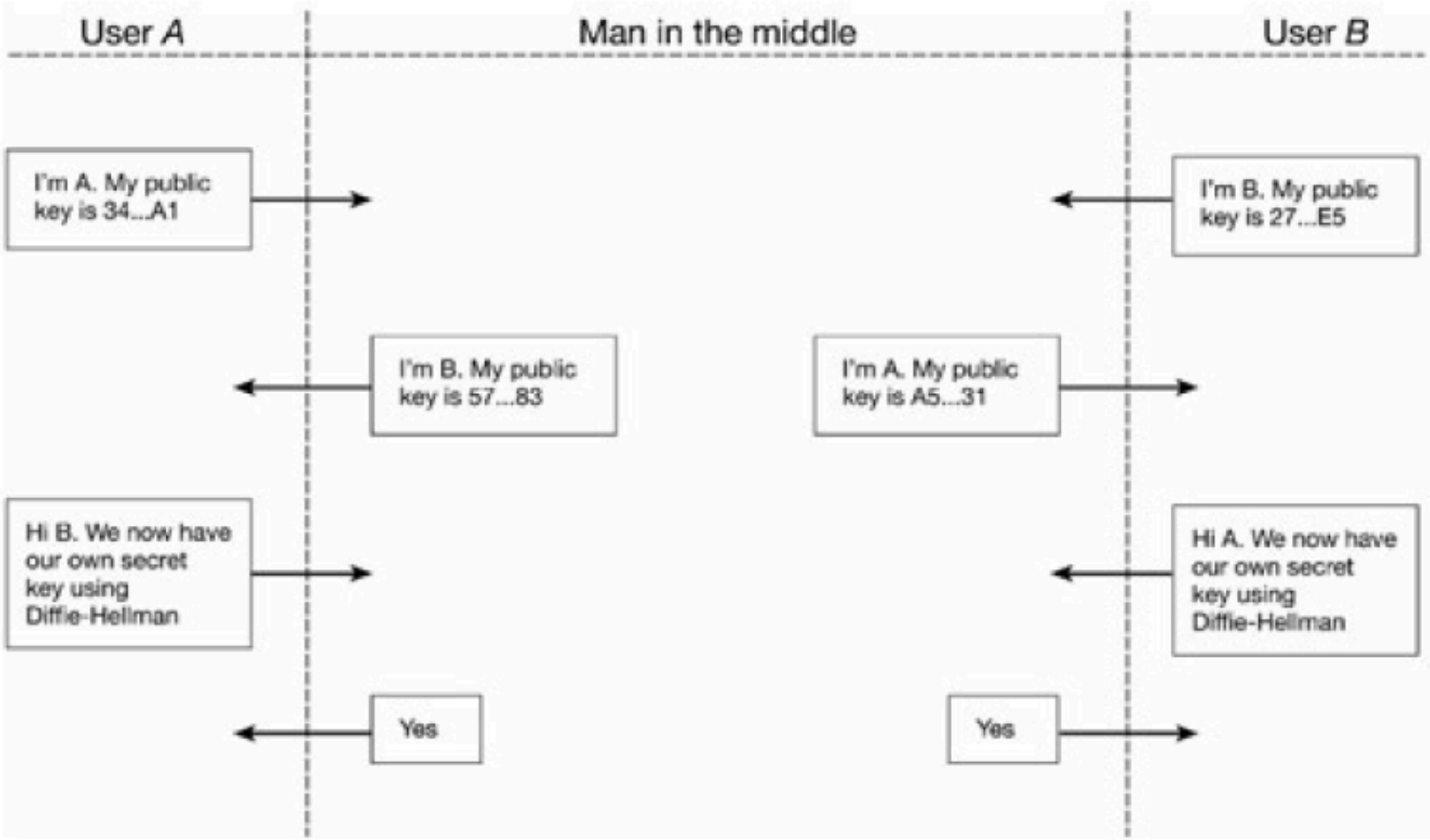
- The key pairs for CAs must be generated.
- The key pairs for users must be generated.
- Users must request certificates.
- Users' identities must be verified.
- Users' key pairs must be verified.
- Certificates must be produced.
- Certificates must be checked.
- Certificates must be removed/updated (when necessary).
- Certificates must be revoked (when necessary).

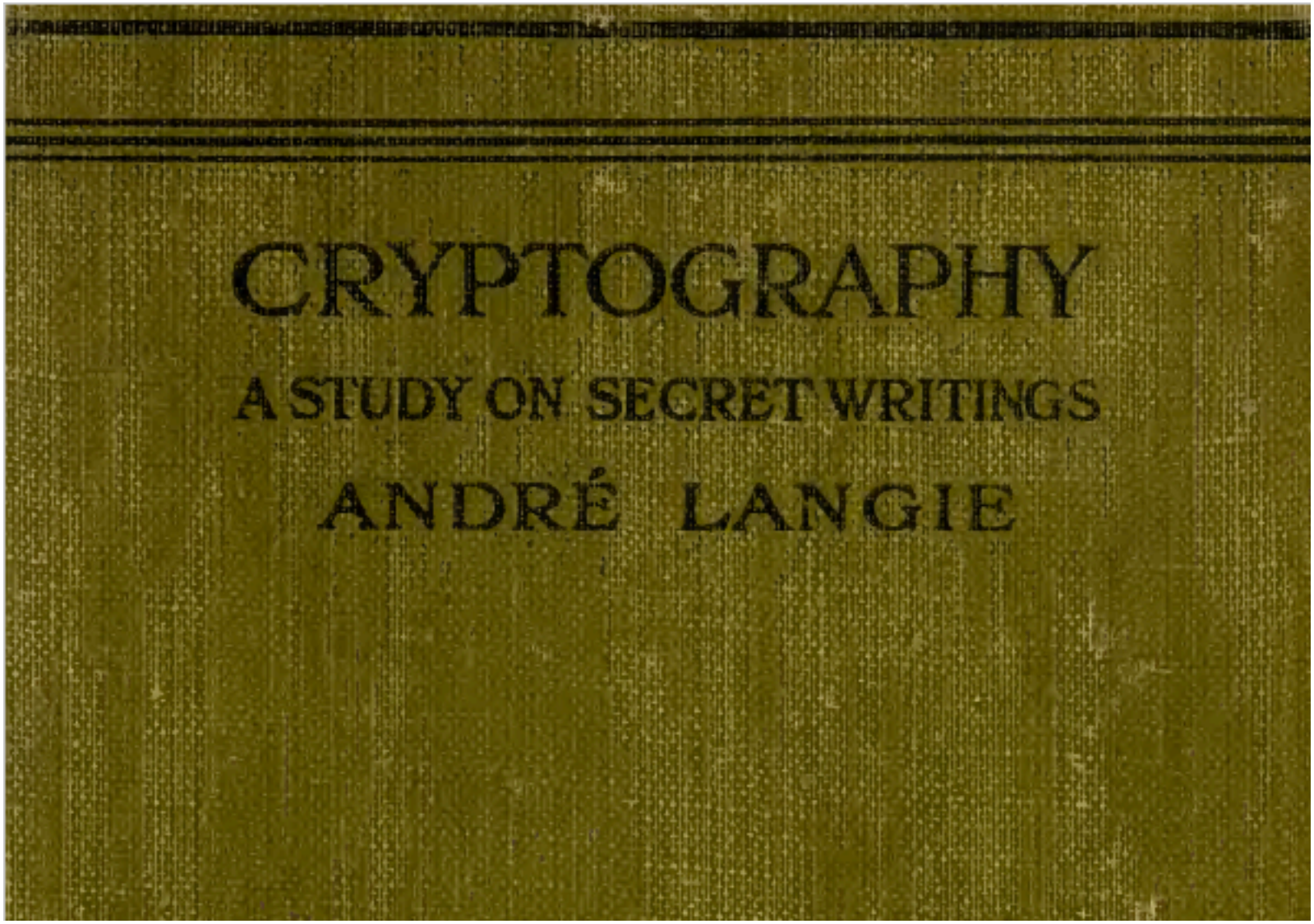
Modern Algorithms

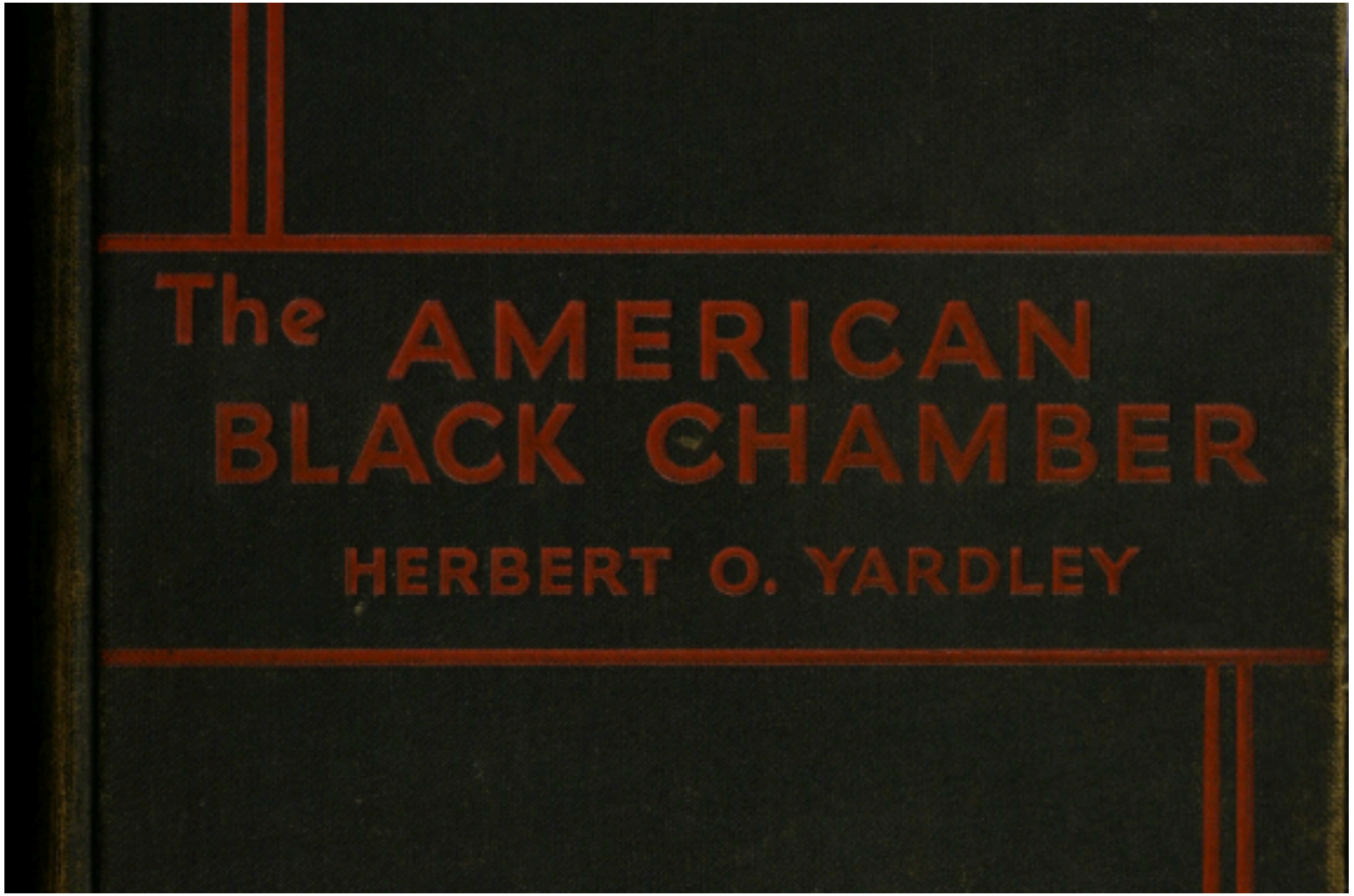
Key Management



Modern Algorithms

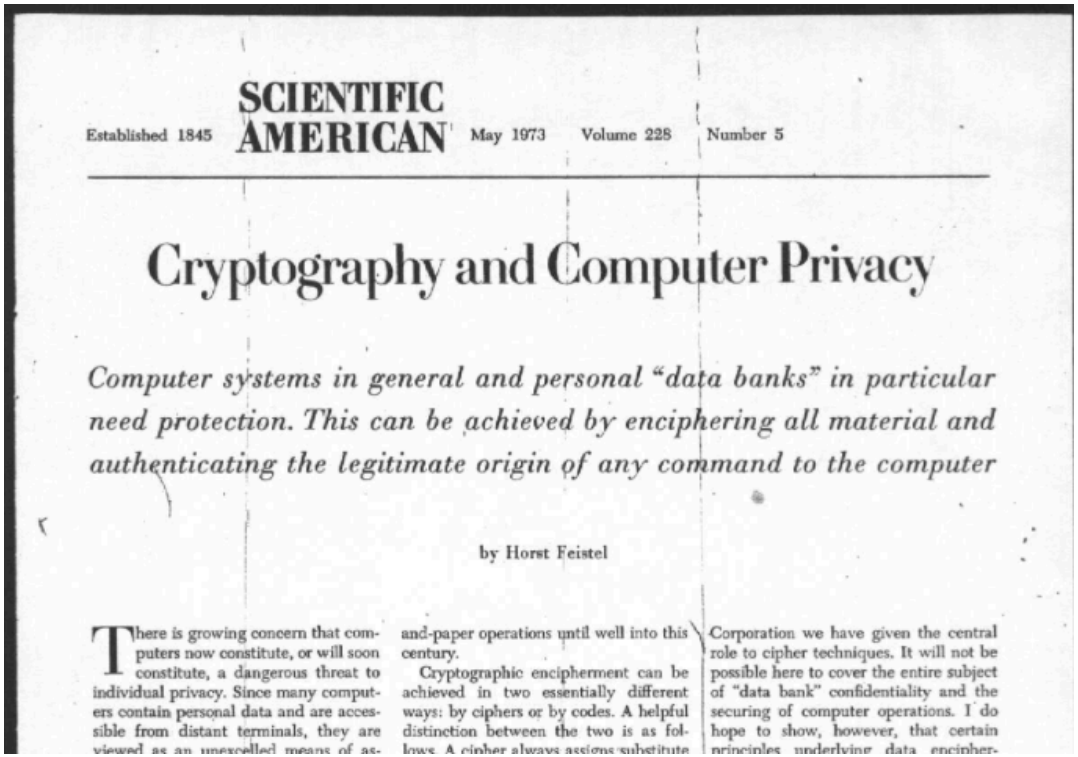



CRYPTOGRAPHY
A STUDY ON SECRET WRITINGS
ANDRÉ LANGIE


The AMERICAN
BLACK CHAMBER
HERBERT O. YARDLEY

Herbert Osborn Yardley (April 13, 1889 – August 7, 1958) was an American cryptologist. He founded and led the cryptographic organization the Black Chamber. Under Yardley, the cryptanalysts of The American Black Chamber broke Japanese diplomatic codes and were able to furnish American negotiators with significant information during the Washington Naval Conference of 1921-1922. Recipient of the Distinguished Service Medal. He wrote The American Black Chamber (1931) about his experiences there. He later helped the Nationalists in China (1938–1940) to break Japanese codes.

Horst Feistel (January 30, 1915 – November 14, 1990) was a German-born cryptographer who worked on the design of ciphers at IBM, initiating research that culminated in the development of the Data Encryption Standard (DES) in the 1970s.



Established 1845 **SCIENTIFIC AMERICAN** May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of as-

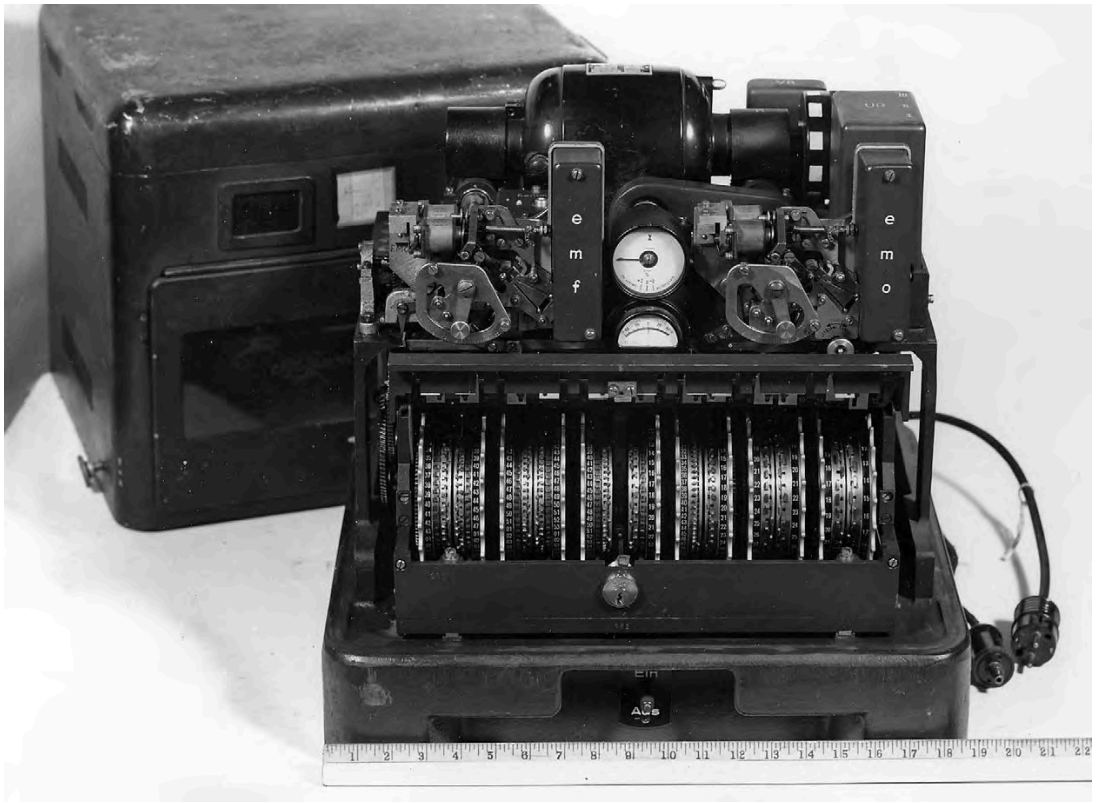
and-paper operations until well into this century.

Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipher-

In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network.

Center for Cryptologic History
National Security Agency
2015



The World War II **German Lorenz machine**.
This machine was complex cryptographically and was also designed to work directly in-line with the communications systems, thereby speeding up the entire communication process. It was used primarily in support of higher level military organizations.

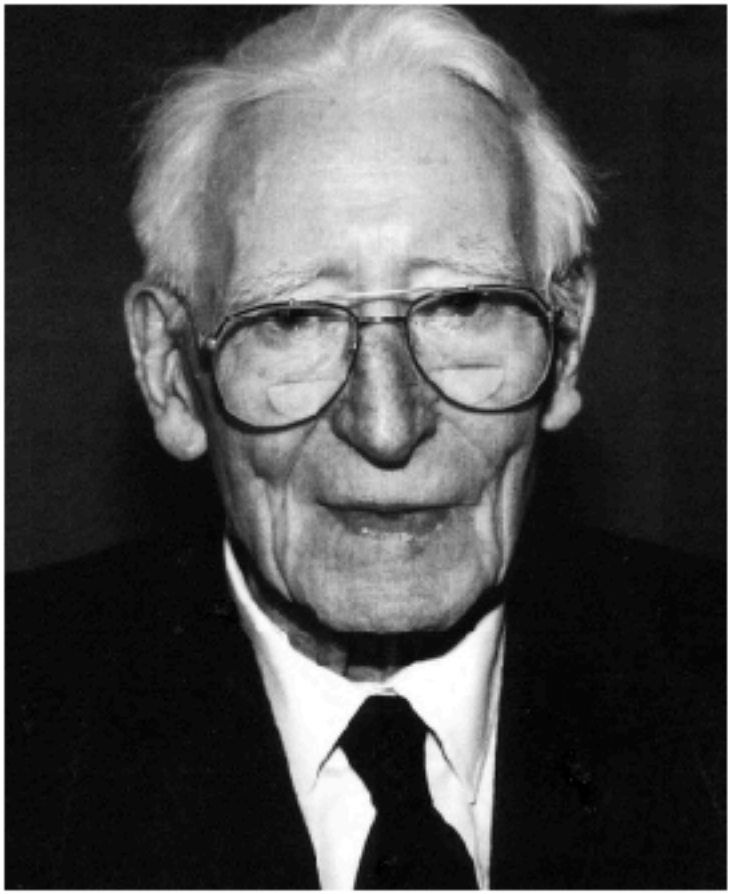


Fig. 2. Dr. Tommy Flowers (1905-1998), ca. 1996. His talents were essential to the successful design and production of the COLOSSUS system. After the war he continued to work at the British Post Office. His wartime accomplishments were not made public until the 1970s. He was made a member of the Order of the British Empire.

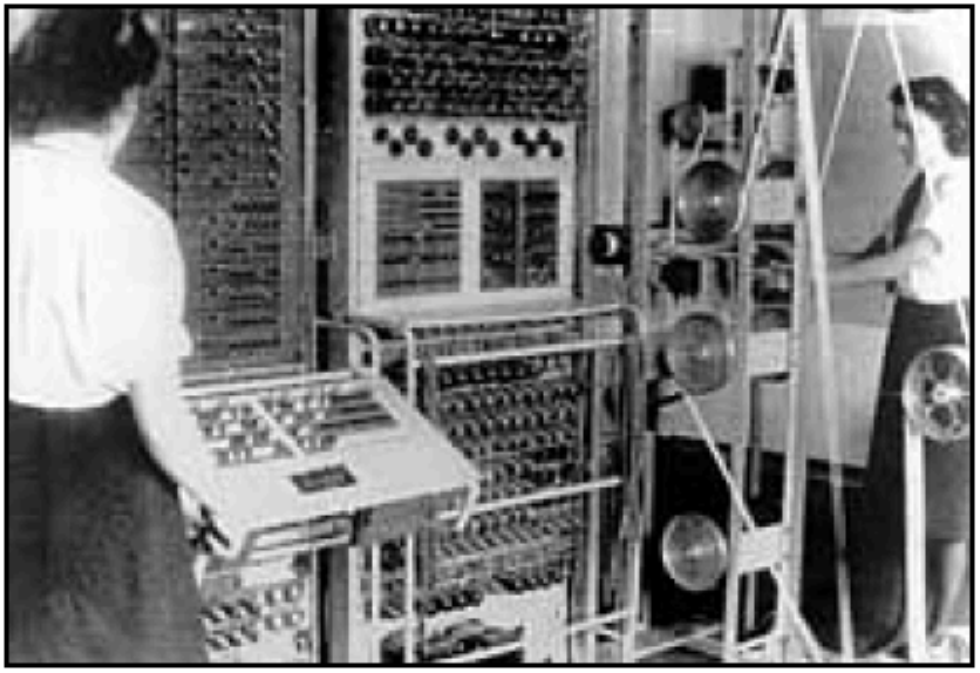


Fig. 3. A World War II COLOSSUS computer system. The system input was by means of punched paper tape on the reel system, called a "bedstead," on the right of this picture. Switch panels and plugboards near the center were used for the programming, and the special electric typewriter on the stand was the output device. (Photo courtesy of Tony Sale)

COLOSSUS Highlights

- First unit was placed into operation at Bletchley Park in January 1944.
- The cipher text input was provided by means of a 5-hole punched paper tape loop.
- A unique optical sensor system read the input at 5,000 characters per second.
- The system clock rate of about 5 khz was derived from the input tape.
- The system logic was programmed by manual means (cords, plugs, switches).
- The output was provided directly to an electric typewriter.
- Message processing time was improved from weeks to a matter of hours, which drastically improved the value of the output.
- By the end of the war, there were ten improved COLOSSUS systems in regular operation at Bletchley Park, each requiring about 2,500 vacuum tubes.
- For reasons of secrecy, eight of the ten units were destroyed soon after the war ended and the remaining two, along with the documentation, were destroyed in the 1960s.
- The program was not declassified until the 1970s

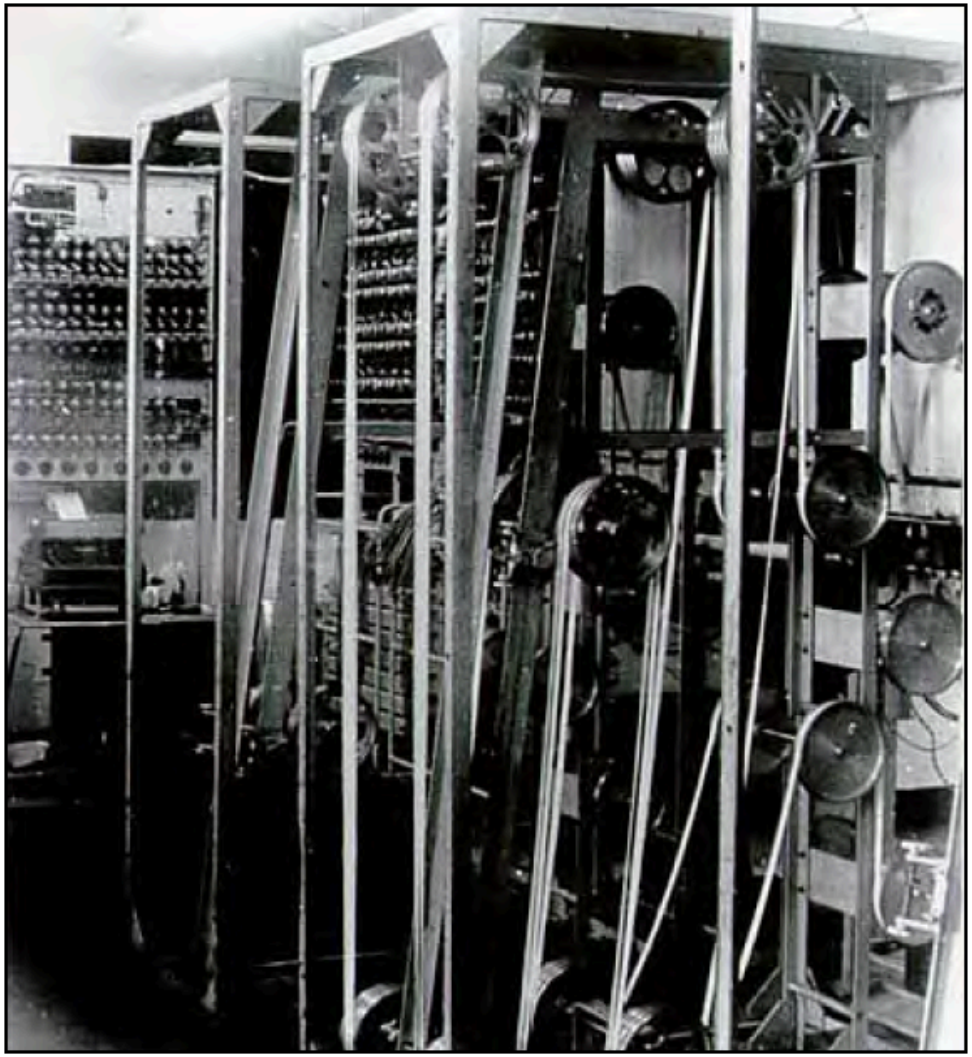


Fig. 4. Another view of the same COLOSSUS system showing more detail of the physical construction. The telephone system heritage of the designers played a large role in this reliable assembly. (Photo courtesy of Tony Sale)

ATLAS I

- Designed and built by Electronic Research Associates (ERA)
- Used a logical design based on von Neumann principles with single-address instructions and forty-one special instructions
- Employed a unique magnetic drum memory with a capacity of 16,383 words of 24 bits each
- Memory access time was 17 milliseconds. The addition of special features brought this down to 32 microseconds.
- Unit No. 1 was delivered in December 1950 and was in operation within one week.

ABNER

- Designed and built in-house at ASA
- Subcontractors made important contributions; Technitrol Corp. provided the mercury delay line memories, and the Raytheon Corporation built the magnetic tape drives.
- It used a four-address design and thirty-one special instructions that emphasized nonarithmetic operations.
- The system could perform computations simultaneously with input and output instructions.
- Operations could be conducted with multiple and mixed input-output devices such as paper tape, magnetic tape, printers, etc.
- First unit was operational in April 1952.

ATLAS II

- Designed and built by ERA
- It used a two-address basic design.
- The first unit of this series used electrostatic storage vacuum tubes for high-speed memory.
- The second unit used magnetic cores for high-speed memory, and it is believed to be the first core-memory computer to be delivered in the U.S.
- The first ATLAS II was delivered in October 1953 and the second in November 1954.

BOGART

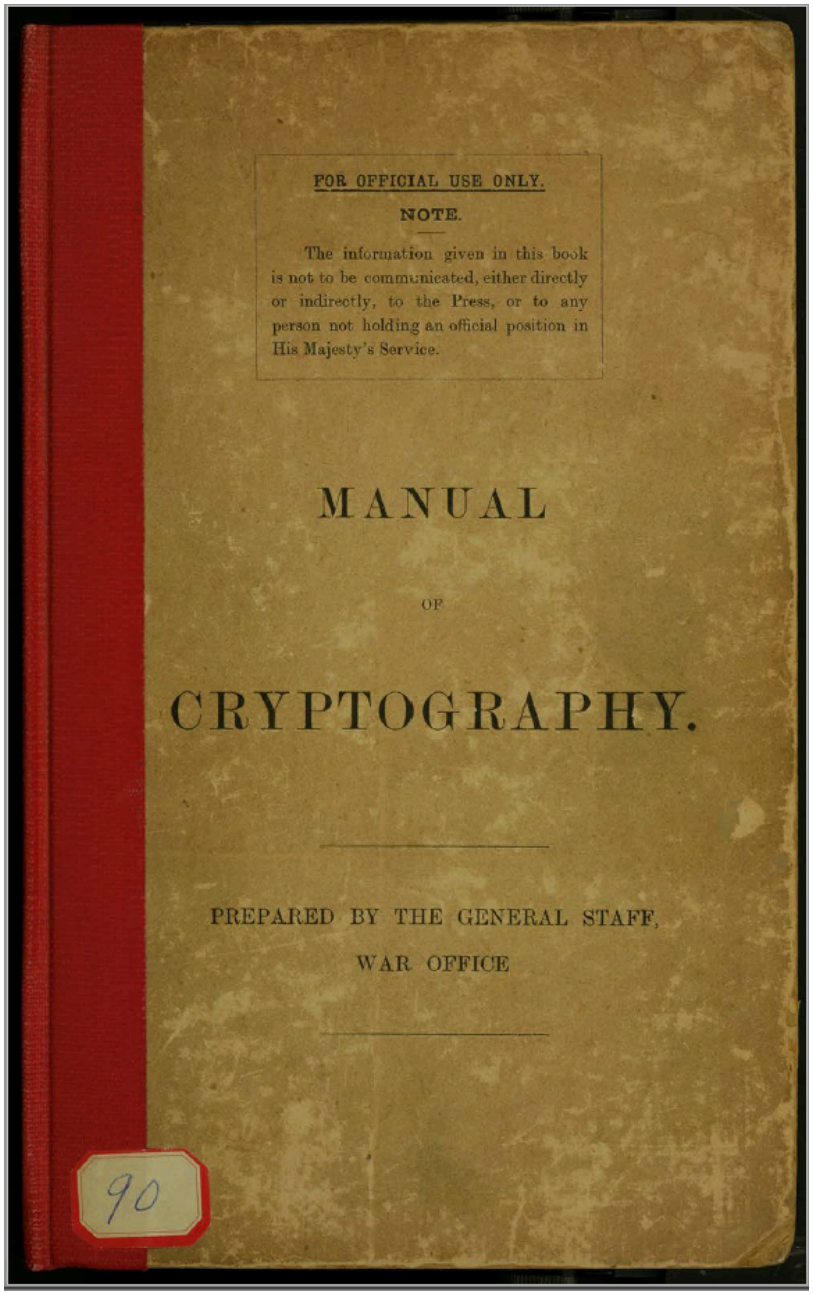
- Designed and built by ERA
- Probably the first computer to use magnetic diode/core logic elements in memory. It permitted 20 microsecond cycle times.
- The final version used 24-bit words and IBM type 727 magnetic tape drives.
- It was probably the first computer designed by use of automated design tools and influenced many later designs by Control Data Corporation (CDC).
- The first unit was delivered in July 1957.

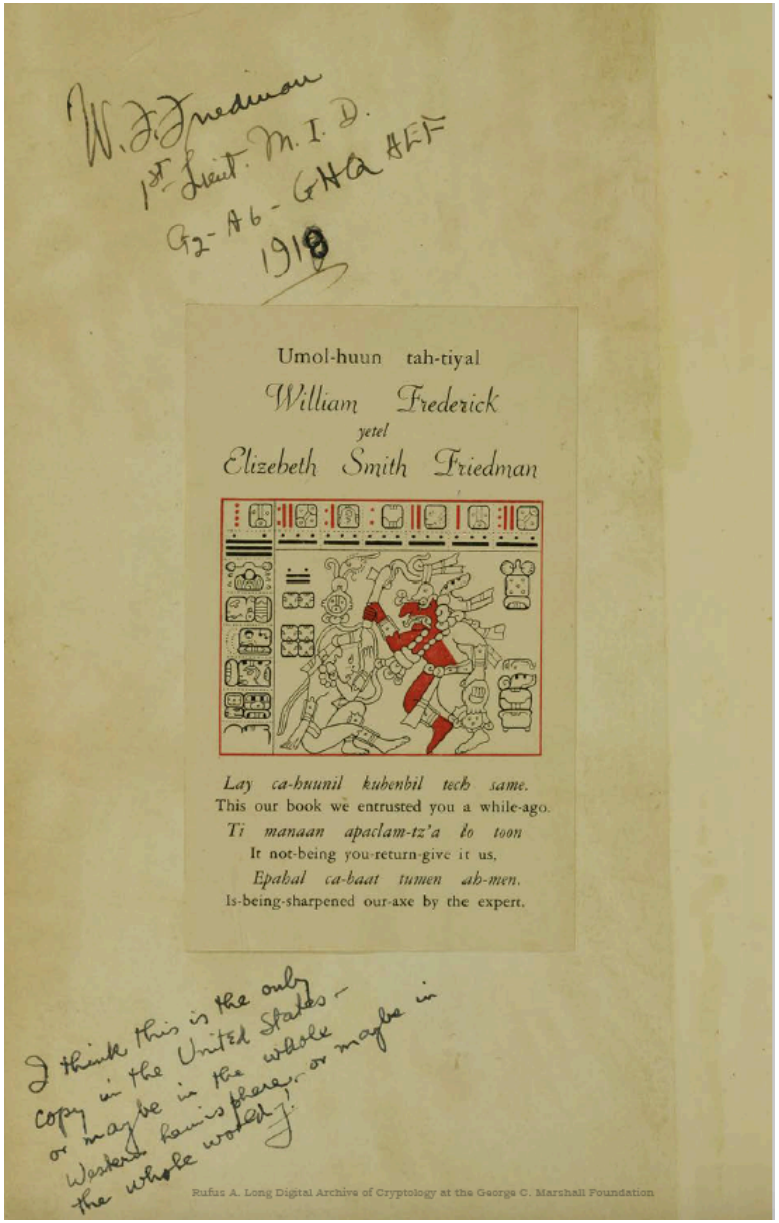
SOLO

- Designed by the Philco Corporation in cooperation with NSA; UNIVAC supplied the core-memory and Magnetic Control Corp. the power supplies.
- It was the first computer to rely exclusively on transistors (then of the surface-barrier type) as the principal circuitry component.
- The logic design was a duplicate of ATLAS II.
- It was delivered in March 1958 and was used primarily for testing and training.

Fig. 14. The HARVEST operating area in 1962. This staged photo does not illustrate the dynamics of this busy area, but it does give a general idea of the size and scope of this landmark system. (Photo, CCH)

Fig. 15. Bombe operations center (see note 8)


FOR OFFICIAL USE ONLY.
NOTE.
The information given in this book is not to be communicated, either directly or indirectly, to the Press, or to any person not holding an official position in His Majesty's Service.
MANUAL
OF
CRYPTOGRAPHY.
PREPARED BY THE GENERAL STAFF,
WAR OFFICE
90



W. F. Friedman
1st Lieut. M. I. D.
G2-A6-GHQ AEF
1918

Umol-huun tah-tiyal
William Frederick
yetel
Elizebeth Smith Friedman

Lay ca-huunil kubenbil tech same.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a to toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

I think this is the only copy in the United States — or maybe in the whole Western hemisphere — or maybe in the whole world?

Rufus A. Long Digital Archive of Cryptology at the George C. Marshall Foundation

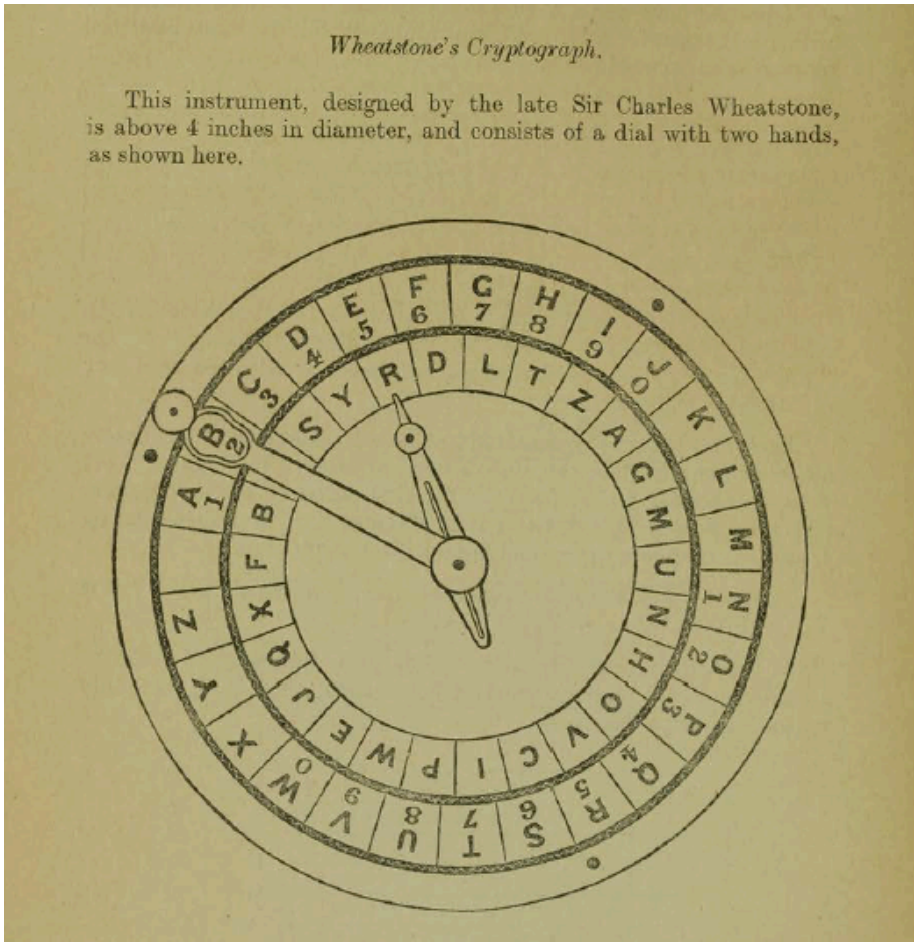
Bacon's Cipher.

In this cipher, designed by Lord Bacon, the letters of the alphabet are represented by permutations of two letters, A and B, in groups of five, as shown below :—

a.	b.	c.	d.	e.	f.
AAAAA	AAAAB	AAABA	AAABB	AABAA	AABAB
g.	h.	i.	k.	l.	m.
AABBA	AABBB	ABAAA	ABAAB	ABABA	ABABB
n.	o.	p.	q.	r.	s.
ABBAA	ABBAB	ABBBA	ABBBB	BAAAA	BAAAB
t.	u.	v.	w.	x.	y.
BAABA	BAABB	BABAA	BABAB	BABBA	BABBB

z.
BBABB.

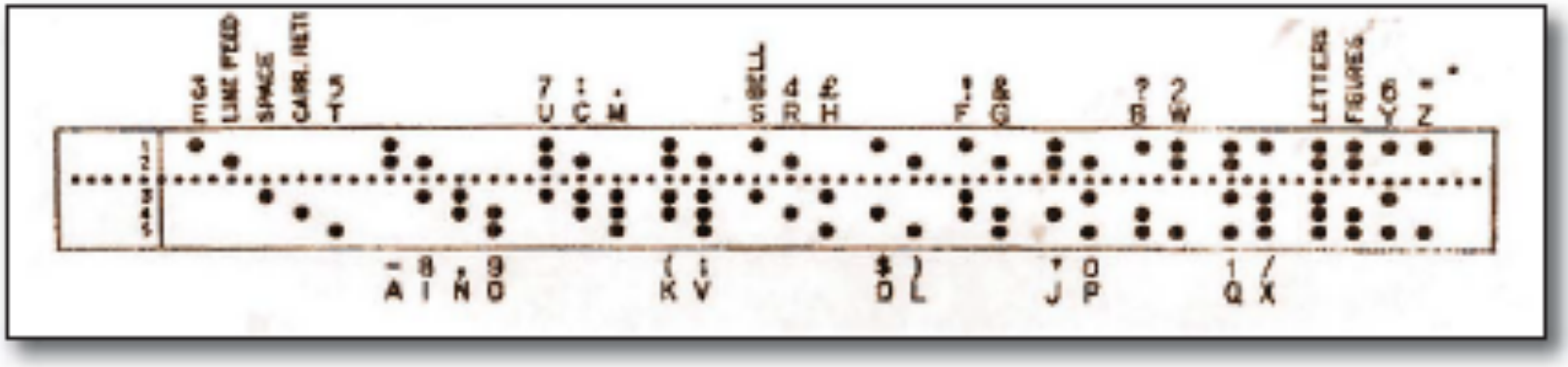
Sir Charles Wheatstone / ˈwiːtstən/[1] FRS (6 February 1802 – 19 October 1875), was an English scientist and inventor of many scientific breakthroughs of the Victorian era, including the English concertina, the stereoscope (a device for displaying three-dimensional images), and the Playfair cipher (an encryption technique). However, Wheatstone is best known for his contributions in the development of the Wheatstone bridge, originally invented by Samuel Hunter Christie, which is used to measure an unknown electrical resistance, and as a major figure in the development of telegraphy.



William Frederick Friedman (September 24, 1891 – November 12, 1969) was a US Army cryptographer who ran the research division of the Army's Signal Intelligence Service (SIS) in the 1930s, and parts of its follow-on services into the 1950s. In 1940, subordinates of his led by Frank Rowlett broke Japan's PURPLE cipher, thus disclosing Japanese diplomatic secrets before America's entrance into World War II.

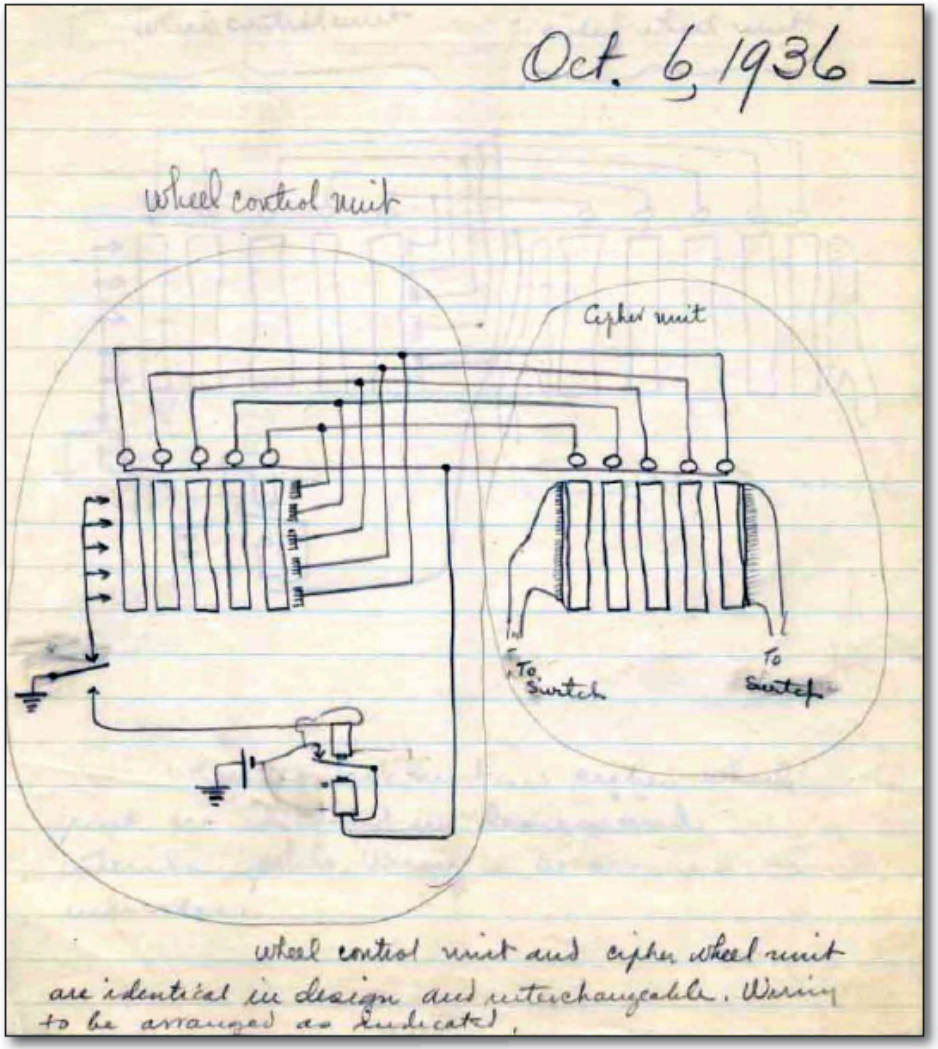
William Friedman with AT&T printing telegraph, 1920 (courtesy of the George C. Marshall Foundation, Lexington, Virginia)

The crypto rotor wheels William Friedman envisioned for his device were flattened cylinders with an alphabet around the circumference. One face of the cylinder had twenty-six spring-loaded copper pins protruding from it; the other face had twenty-six flush copper contacts. Inside each cylinder was a wire maze connecting the electrical contacts on one side to the pins on the other.

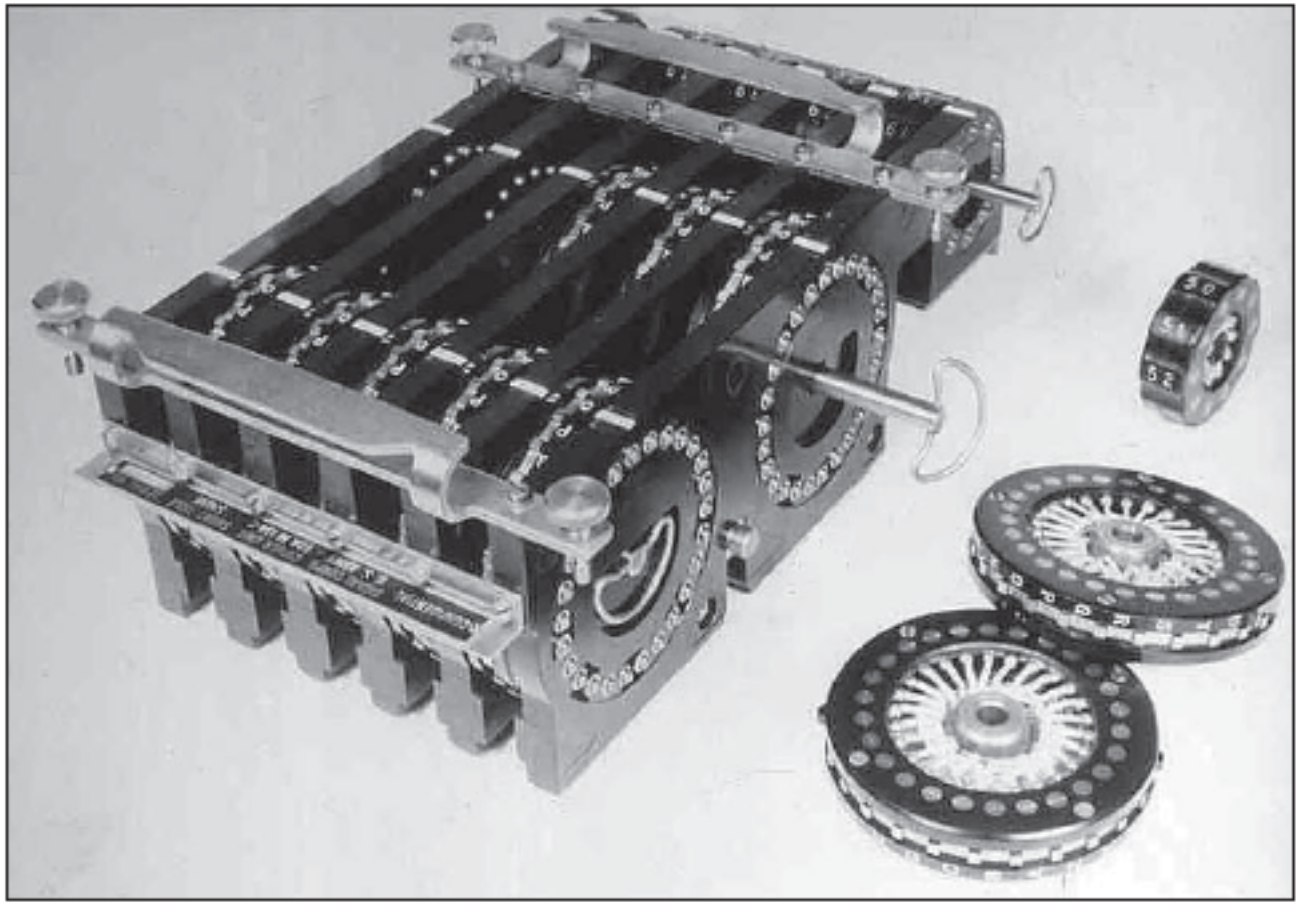


Five-group punched hole paper telegraphic tape

An electrical impulse beginning with, say, the letter A on one side might connect to H on the other side and so on around the wheel in random fashion. Several cylinders serially juxtaposed on a spindle sideby-side could further scramble impulses. (Image courtesy the online Crypto Museum, www.cryptomuseum.com)

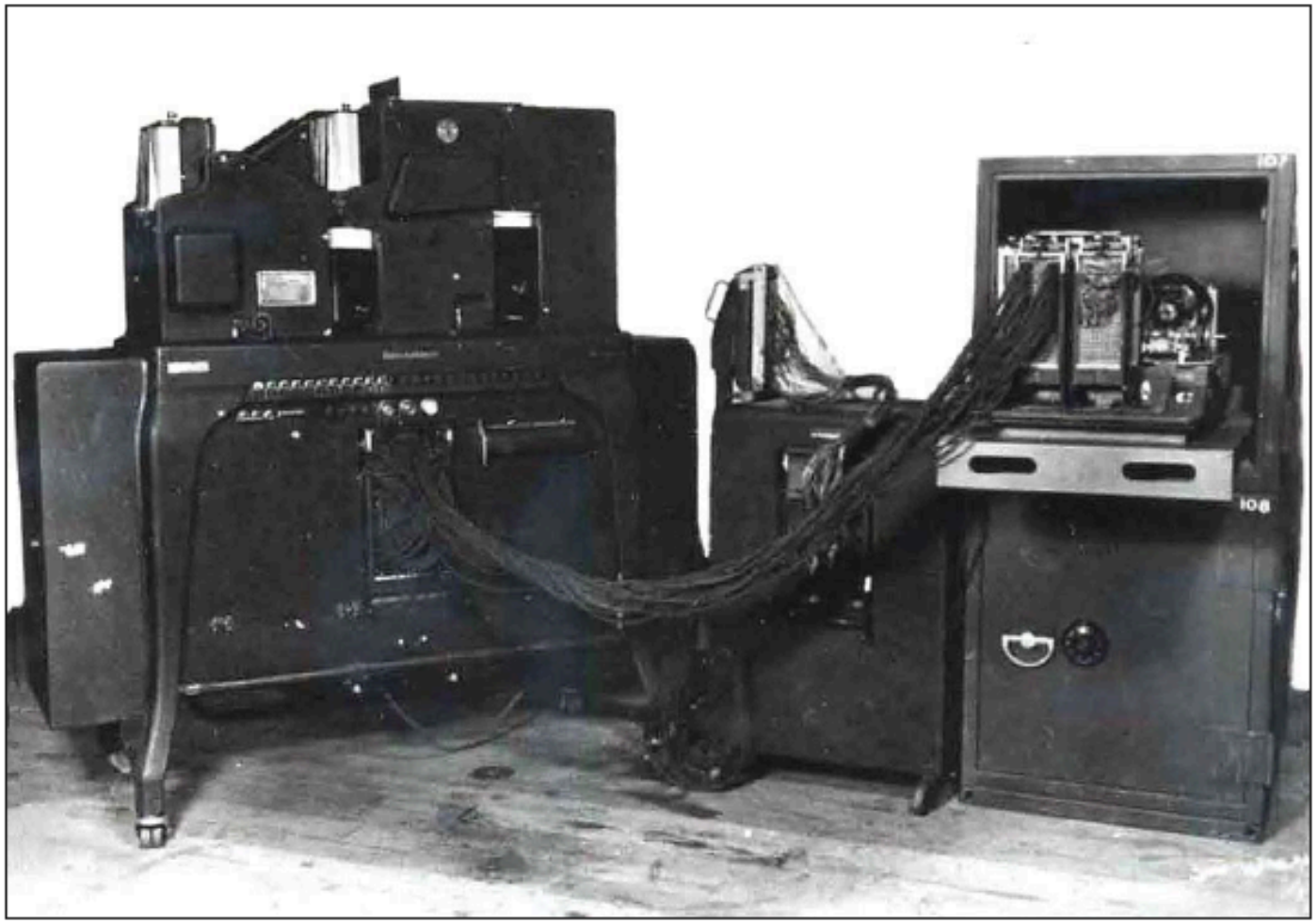


A sketch of the wheel control unit, the "control rotor bank," separate from the cipher unit, called the "cipher rotor bank." Note at bottom reads, "Wheel control unit and cipher wheel unit are identical in design and interchangeable. Wiring to be arranged as indicated." It is similar to the diagrams Friedman showed the Navy during 1935. (Friedman Collection, NSA/CSS accession #47270, box 10, folder 5)



SIGABA rotor maze. Note the five small ten-pin wheels that replaced the Army's original plugboard.

Women assembling SIGABA crypto rotor wheels



IBM SIGABA key generator used at headquarters to produce daily key settings[55]

In 1956 a grateful Congress awarded $100,000 to William Friedman for his contribution to SIGABA and for other cryptologic achievements.

The SIGABA/ECM II

United Colonies' Cipher

General George Washington's Tradecraft

The Church Cryptogram: Birth of Our Nation's Cryptology

General George Washington's Tradecraft

The Jefferson-Patterson Ciphers

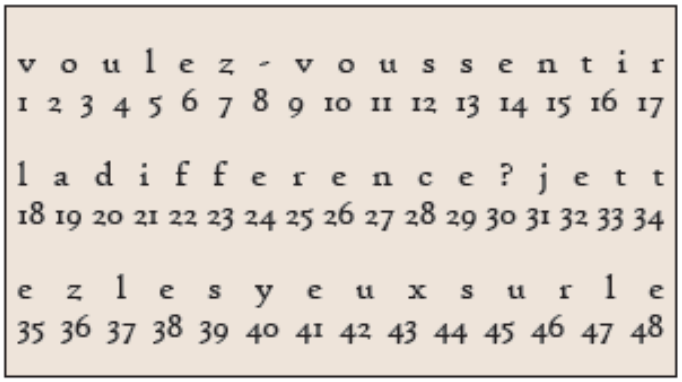
Jefferson's Cipher Cylinder

John Quincy Adams's Sliding Cipher

Aaron Burr's "Cipher Letter"

The First U.S. Government Manual on Cryptography

Seward's Other Folly: America's First Encrypted Cable



The Dumas cipher (partial)

Dear Sir,

We have News here that your Fleet has behaved bravely; I congratulate you upon it most cordially.

I have just received a 14. 5 .3. 10. 28 .2. 76. 202. 66. 11. 12. 273. 50. 14. joining 76. 5. 42. 45. 16. 15. 424. 235. 19. 20. 69, 580. 11. 150. 27. 56. 35. 104. 652. 28. 675. 85. 79. 50. 63. 44. 22. 219. 17. 60. 29. 147. 136. 41. but this is not likely to afford 202. 55. 580. 10. 227. 613. 176. 373. 309. 4. 108. 40. 19. 97. 309 17. 35. 90. 201. 100. 677.

By our last Advices our Affairs were in a pretty good train. I hope we shall have advice of the Expulsion of the English from Virginia.

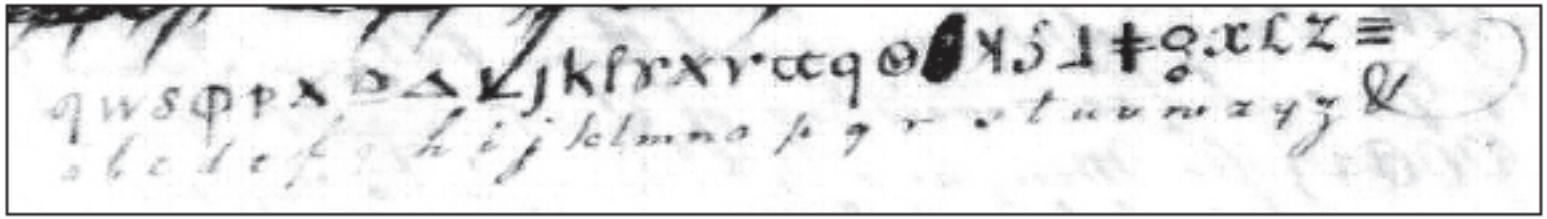
I am ever, Dear Sir,
Your most obedient & most humble Servant

B. Franklin[1]

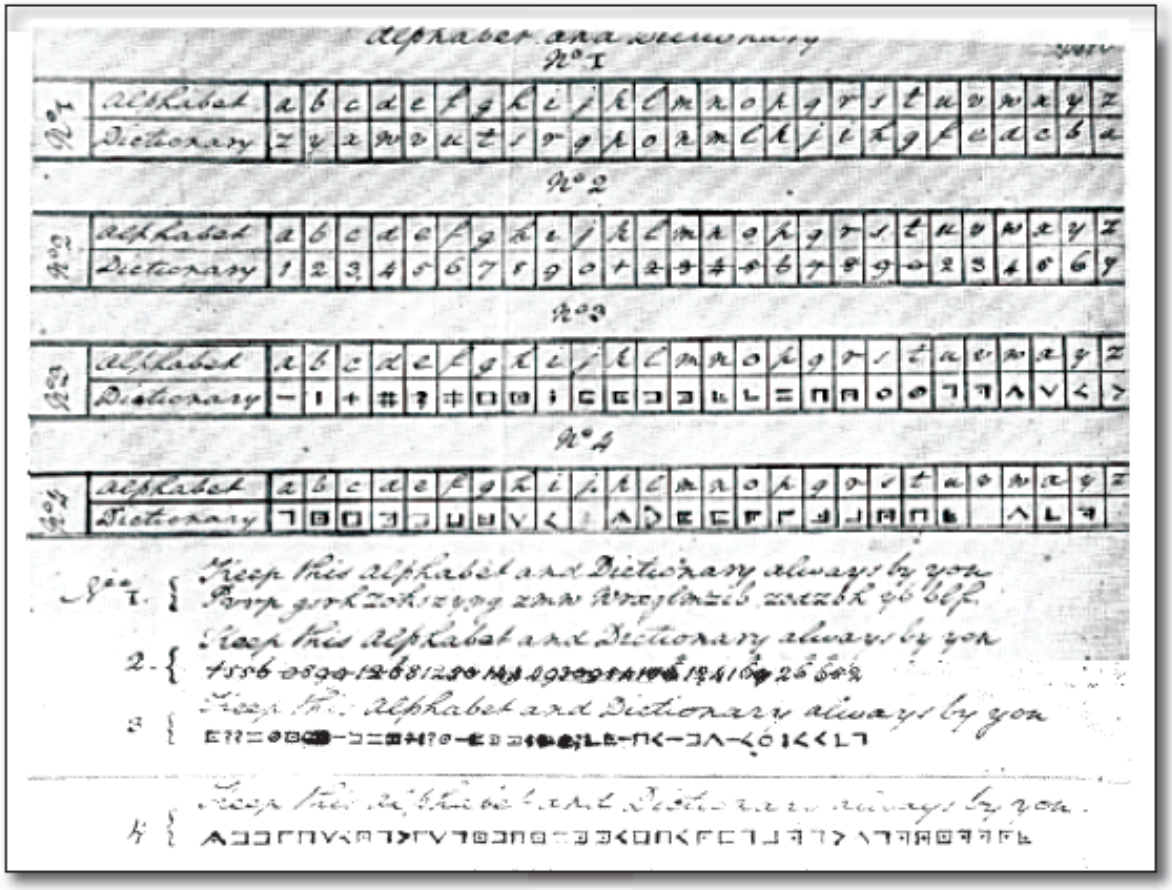
Letter from Benjamin Franklin to Charles Dumas, 1781

					b	a	n	k	r	u	p	t			
I can only say that we are					27.	11.	12.	21.	16.	4.	14.	3.			
w	i	t	h	a	m	u	t	i	n	o	u	s			
21.	19.	18.	18.	26.	23.	19.	3.	7.	24.	13.	19.	2.			
a	r	m	y							d	e	l	a	y	
26.	1.	11.	8.	the latter owing very much to the						2.	15.	10.	11.	23.	
o	f	c	l	o	a	t	h	i	n	g					
25	4.	13.	10.	25.	26.	3.	6.	19.	12.	17.[3]					

Letter from James Lovell to John Adams, 1781

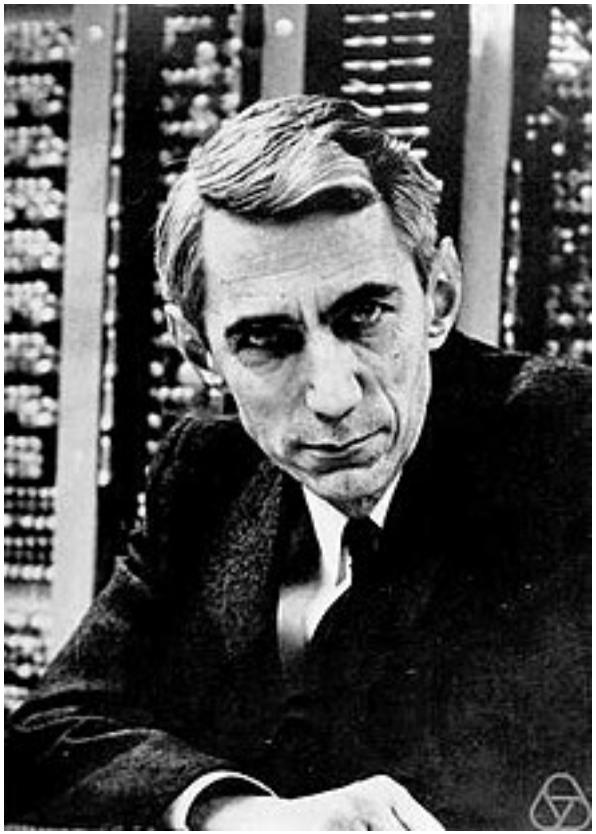


Church cipher system



George Washington's alphabet code sheet, 1783. *Library of Congress*

Cipher cylinder of President Jefferson's design and period. *National Cryptologic Museum*



Claude Elwood Shannon
(April 30, 1916 – February 24, 2001)
was an American mathematician, electrical engineer, and cryptographer known as "the father of information theory"

Shannon formulated a version of Kerckhoffs' principle as "The enemy knows the system". In this form it is known as "Shannon's maxim".

In cryptography, **Kerckhoffs's principle** was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century*:*

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Two methods (other than recourse to ideal systems) suggest themselves for frustrating a statistical analysis. These we may call the methods of ***diffusion*** and ***confusion***.

Communication Theory of Secrecy Systems
By C. E. SHANNON

HOMOMORPHIC ENCRYPTION

Secure computing techniques such as Ring-LWE-based Homomorphic Encryption (HE) offer the possibility of general computing on data while the data remains encrypted.

Practical and usable homomorphic encryption would lead to a sea change in outsourced (cloud) computation on privacy-critical data, and enable a number of application scenarios that are currently either impossible due to technical or legal reasons, or are possible but rely on costly and time-consuming legal processes.

Although homomorphic encryption is still at an early point in its life cycle, there has been consistent, substantive, and rapid progress in making it practical from a performance standpoint.

NIST Post-Quantum

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sized needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Tarantula Technology

blockchain solutions

Uses of cryptographic techniques

- Commitment schemes
- Secure multiparty computation
- Electronic voting
- Authentication
- Digital signatures
- Crypto systems
- Dining cryptographers problem
- Anonymous remailer
- Pseudonymity
- Anonymous internet banking
- Onion routing
- Digital currency
- Secret sharing

Tarantula Technology
blockchain solutions

Branches of cryptography

- Cryptographic engineering
- Multivariate cryptography
- Post-quantum cryptography
- Quantum cryptography
- Steganography
- Visual cryptography

Ciphers

Substitution

- Monoalphabetic substitution
  - Caesar cipher
    - ROT13
  - Affine cipher
  - Atbash cipher
  - Keyword cipher
- Polyalphabetic substitution
  - Vigenère cipher
  - Autokey cipher
  - Homophonic substitution cipher
- Polygraphic substitution
  - Playfair cipher
  - Hill cipher

Ciphers

Transposition

- Scytale
- Grille
- Permutation cipher
- VIC cipher – complex hand cypher time

Ciphers

Modern symmetric-key algorithms

Stream ciphers

- A5/1 & A5/2 – ciphers specified for the GSM cellular telephone standard
- BMGL
- Chameleon
- FISH – by Siemens AG
- WWII 'Fish' cyphers
  - Geheimfernschreiber – WWII mechanical onetime pad by Siemens AG, called STURGEON by Bletchley Park
  - Pike – improvement on FISH by Ross Anderson
  - Schlusselzusatz – WWII mechanical onetime pad by Lorenz, called *tunny* by Bletchley Park
- HELIX
- ISAAC – intended as a PRNG
- Leviathan
- LILI-128
- MUGI – CRYPTREC recommendation
- MULTI-S01 - CRYPTREC recommendation
- One-time pad – Vernam and Mauborgne, patented 1919; an extreme stream cypher
- Panama
- RC4 (ARCFOUR) – one of a series by Professor Ron Rivest of MIT; CRYPTREC recommended limited to 128-bit key
  - CipherSaber – (RC4 variant with 10 byte random IV, easy to implement
- Salsa20 – an eSTREAM recommended cipher
  - ChaCha20 – A Salsa20 variant.

Tarantula Technology

blockchain solutions

Ciphers

Block ciphers

- Product cipher
- Feistel cipher – pattern by Horst Feistel
- Advanced Encryption Standard (Rijndael) – 128-bit block; NIST selection for the AES, FIPS 197; Created 2001—by Joan Daemen and Vincent Rijmen; NESSIE selection; CRYPTREC recommendation.
- Anubis – 128-bit block
- BEAR – built from a stream cypher and hash function, by Ross Anderson
- Blowfish – 64-bit block; by Bruce Schneier *et al.*
- Camellia – 128-bit block; NESSIE selection (NTT & Mitsubishi Electric); CRYPTREC recommendation
- CAST-128 (CAST5) – 64-bit block; one of a series of algorithms by Carlisle Adams and Stafford Tavares, insistent that the name is not due to their initials
  - CAST-256 (CAST6) – 128-bit block; the successor to CAST-128 and a candidate for the AES competition
- CIPHERUNICORN-A – 128-bit block; CRYPTREC recommendation
- CIPHERUNICORN-E – 64-bit block; CRYPTREC recommendation (limited)
- CMEA – cipher used in US cellphones, found to have weaknesses.
- CS-Cipher – 64-bit block
- Data Encryption Standard (DES) – 64-bit block; FIPS 46-3, 1976
- DEAL – an AES candidate derived from DES
- DES-X – a variant of DES to increase the key size.
- FEAL
- GDES – a DES variant designed to speed up encryption
- Grand Cru – 128-bit block
- Hierocrypt-3 – 128-bit block; CRYPTREC recommendation
- Hierocrypt-L1 – 64-bit block; CRYPTREC recommendation (limited)
- IDEA NXT – project name FOX, 64-bit and 128-bit block family; Mediacrypt (Switzerland); by Pascal Junod & Serge Vaudenay of Swiss Institute of Technology Lausanne
- International Data Encryption Algorithm (IDEA) – 64-bit block;James Massey & X Lai of ETH Zurich
- Iraqi Block Cipher (IBC)
- KASUMI – 64-bit block; based on MISTY1, adopted for next generation W-CDMA cellular phone security
- KHAZAD – 64-bit block designed by Barretto and Rijmen
- Khufu and Khafre – 64-bit block ciphers
- Kuznyechik – Russian 128-bit block cipher, defined in GOST R 34.12-2015 and RFC 7801.
- LION – block cypher built from stream cypher and hash function, by Ross Anderson
- LOKI89/91 – 64-bit block ciphers
- LOKI97 – 128-bit block cipher, AES candidate
- Lucifer – by Tuchman *et al.* of IBM, early 1970s; modified by NSA/NBS and released as DES
- MAGENTA – AES candidate
- Mars – AES finalist, by Don Coppersmith et al.
- MISTY1 – NESSIE selection 64-bit block; Mitsubishi Electric (Japan); CRYPTREC recommendation (limited)

Tarantula Technology
blockchain solutions

Ciphers

Modern asymmetric-key algorithms

Asymmetric key algorithm

- ACE-KEM – NESSIE selection asymmetric encryption scheme; IBM Zurich Research
  - ACE Encrypt
- Chor-Rivest
- Diffie-Hellman – key agreement; CRYPTREC recommendation
- El Gamal – discrete logarithm
- Elliptic curve cryptography – (discrete logarithm variant)
- PSEC-KEM – NESSIE selection asymmetric encryption scheme; NTT (Japan); CRYPTREC recommendation only in DEM construction w/SEC1 parameters
  - ECIES – *Elliptic Curve Integrated Encryption System*, Certicom Corporation
    - ECIES-KEM
    - ECDH – *Elliptic Curve Diffie-Hellman key agreement*, CRYPTREC recommendation
- EPOC
- Merkle–Hellman knapsack cryptosystem – knapsack scheme
- McEliece
- Niederreiter cryptosystem
- NTRUEncrypt
- RSA – factoring
  - RSA-KEM – NESSIE selection asymmetric encryption scheme; ISO/IEC 18033-2 draft
  - RSA-OAEP – CRYPTREC recommendation

Cryptographic hash functions

- Message authentication code
- Keyed-hash message authentication code
  - Encrypted CBC-MAC (EMAC) – NESSIE selection MAC
  - HMAC – NESSIE selection MAC; ISO/IEC 9797-1, FIPS PUB 113 and IETF RFC
  - TTMAC – (Two-Track-MAC) NESSIE selection MAC; K.U.Leuven (Belgium) & debis AG (Germany)
  - UMAC – NESSIE selection MAC; Intel, UNevada Reno, IBM, Technion, & UC Davis
- MD5 – one of a series of message digest algorithms by Prof Ron Rivest of MIT; 128-bit digest
- SHA-1 – developed at NSA 160-bit digest, an FIPS standard; the first released version was defective and replaced by this; NIST/NSA have released several variants with longer 'digest' lengths; CRYPTREC recommendation (limited)
  - SHA-256 – NESSIE selection hash function, FIPS 180-2, 256-bit digest; CRYPTREC recommendation
  - SHA-384 – NESSIE selection hash function, FIPS 180-2, 384-bit digest; CRYPTREC recommendation
  - SHA-512 – NESSIE selection hash function, FIPS 180-2, 512-bit digest; CRYPTREC recommendation
- SHA-3 – originally known as Keccak; was the winner of the NIST hash function competition using sponge function.
- Streebog – Russian algorithm created to replace an obsolete GOST hash function defined in obsolete standard GOST R 34.11-94.
- RIPEMD-160 – developed in Europe for the RIPE project, 160-bit digest; CRYPTREC recommendation (limited)
- RTR0 – one of Retter series; developed by Maciej A. Czyzewski; 160-bit digest
- Tiger – by Ross Anderson *et al.*
- Snefru – NIST hash function competition
- Whirlpool – NESSIE selection hash function, Scopus Tecnologia S.A. (Brazil) & K.U.Leuven (Belgium)

Tarantula Technology

blockchain solutions

Keys

Key authentication

- Public key infrastructure
  - X.509
  - OpenPGP
- Public key certificate
  - Certificate authority
  - Certificate revocation list
- ID-based cryptography
- Certificate-based encryption
- Secure key issuing cryptography
- Certificateless cryptography
- Merkle tree

Tarantula Technology

blockchain solutions

Keys

Transport/exchange

- Diffie–Hellman
- Man-in-the-middle attack
- Needham–Schroeder
- Offline private key
- Otway–Rees
- Trusted paper key
- Wide Mouth Frog

Keys

Weak keys

- Brute force attack
- Dictionary attack
- Related key attack
- Key derivation function
- Key strengthening
- Password
- Password-authenticated key agreement
- Passphrase
- Salt

Cryptanalysis

Classical

- Frequency analysis
- Contact analysis
- Index of coincidence
- Kasiski examination

Cryptanalysis

Modern

- Symmetric algorithms
  - Boomerang attack
  - Brute force attack
  - Davies' attack;
  - Differential cryptanalysis
  - Impossible differential cryptanalysis
  - Integral cryptanalysis
  - Linear cryptanalysis
  - Meet-in-the-middle attack
  - Mod-n cryptanalysis
  - Related-key attack
  - Slide attack
  - XSL attack

Cryptanalysis

Modern

- Hash functions:
  - Birthday attack
- Attack models
  - Chosen-ciphertext
  - Chosen-plaintext
  - Ciphertext-only
  - Known-plaintext
- Side channel attacks
  - Power analysis
  - Timing attack
  - Cold boot attack

Attacks

1. Ciphertext-only attack
2. Known-plaintext attack
3. Chosen-plaintext attack
4. Adaptively-chosen-plaintext attack
5. Chosen and adaptively-chosen-ciphertext attacks

Attacks

Ciphertext-only attack

Eve has the ability to obtain ciphertexts. This is likely to be the case in any encryption situation. An encryption method that cannot resist a ciphertext-only attack is completely insecure.

Known-plaintext attack

Eve has the ability to obtain plaintext–ciphertext pairs. Using the information from these pairs, she attempts to decrypt a ciphertext for which she does not have the plaintext. At first glance, it might appear that such information would not ordinarily be available to an attacker. However, it very often is available. Messages may be sent in standard formats which Eve knows.

Attacks

Chosen-plaintext attack

Eve has the ability to obtain ciphertexts for plaintexts of her choosing.

Then she attempts to decrypt a ciphertext for which she does not have the plaintext. While again this may seem unlikely, there are many cases in which Eve can do just this.

For example, she may send some interesting information to her intended victim which she is confident he will encrypt and send out.

This type of attack assumes that Eve must first obtain whatever plaintext–ciphertext pairs she wants and then do her analysis, without any further interaction. This means that she only needs access to the encrypting device once.

Attacks

Adaptively-chosen-plaintext attack

This is the same as the previous attack, except that now Eve may do some analysis on the plaintext–ciphertext pairs, and subsequently get more pairs.

She may switch between gathering pairs and performing the analysis as often as she likes.

This means that she either has lengthy access to the encrypting device or can somehow make repeated use of it.

Attacks

Chosen and adaptively-chosen-ciphertext attacks

These two attacks are similar to the above plaintext attacks.

Eve can choose ciphertexts and get the corresponding plaintexts.

She has access to the decryption device.

Cryptanalysis

Modern

- Network attacks
  - Man-in-the-middle attack
  - Replay attack
- External attacks
  - Black-bag cryptanalysis
  - Rubber-hose cryptanalysis

Cryptanalysis

Robustness properties

- Provable security
- Random oracle model
- Ciphertext indistinguishability
- Semantic security
- Malleability
- Forward secrecy
- Forward anonymity
- Freshness

Cryptanalysis

Undeciphered historical codes and ciphers

- Beale ciphers
- Chaocipher
- D'Agapeyeff cipher
- Dorabella cipher
- Rongorongo
- Shugborough inscription
- Voynich manuscript

Organizations and selection projects

Cryptography standards

- Federal Information Processing Standards (FIPS) Publication Program – run by NIST to produce standards in many areas to guide operations of the US Federal government; many FIPS publications are ongoing and related to cryptography
- American National Standards Institute (ANSI) – standardization process that produces many standards in many areas; some are cryptography related, ongoing)
- International Organization for Standardization (ISO) – standardization process produces many standards in many areas; some are cryptography related, ongoing
- Institute of Electrical and Electronics Engineers (IEEE) – standardization process produces many standards in many areas; some are cryptography related, ongoing
- Internet Engineering Task Force (IETF) – standardization process that produces many standards called RFCs) in many areas; some are cryptography related, ongoing)

Organizations and selection projects

General cryptographic

- National Security Agency (NSA) – internal evaluation/selections, charged with assisting NIST in its cryptographic responsibilities
- Government Communications Headquarters (GCHQ) – internal evaluation/selections, a division is charged with developing and recommending cryptographic standards for the UK government
- Defence Signals Directorate (DSD) – Australian SIGINT agency, part of ECHELON
- Communications Security Establishment (CSE) – Canadian intelligence agency

Organizations and selection projects

Open efforts

- Data Encryption Standard (DES) – NBS selection process, ended 1976
- RIPE – division of the RACE project sponsored by the European Union, ended mid-1980s
- Advanced Encryption Standard (AES) – a "break-off" competition sponsored by NIST, ended in 2001
- NESSIE Project – an evaluation/selection program sponsored by the European Union, ended in 2002
- eSTREAM– program funded by ECRYPT; motivated by the failure of all of the stream ciphers submitted to NESSIE, ended in 2008
- CRYPTREC – evaluation/recommendation program sponsored by the Japanese government; draft recommendations published 2003
- CrypTool – an e-learning freeware programme in English and German— exhaustive educational tool about cryptography and cryptanalysis

Legal issues

- AACS encryption key controversy
- Free speech
  - *Bernstein v. United States* - Daniel J. Bernstein's challenge to the restrictions on the export of cryptography from the United States.
  - *Junger v. Daley*
  - DeCSS
  - Phil Zimmermann - Arms Export Control Act investigation regarding the PGP software.
- Export of cryptography
- Key escrow and Clipper Chip
- Digital Millennium Copyright Act
- Digital Rights Management (DRM)
- Patents
  - RSA – now public domain
  - David Chaum – and digital cash
- Cryptography and law enforcement
  - Telephone wiretapping
  - Espionage
- Cryptography laws in different nations
  - Official Secrets Act – United Kingdom, India, Ireland, Malaysia, and formerly New Zealand
  - Regulation of Investigatory Powers Act 2000 – United Kingdom

Tarantula Technology

blockchain solutions

Academic and professional publications

- Journal of Cryptology
- Encyclopedia of Cryptography and Security
- Cryptologia – quarterly journal focusing on historical aspects
- Communication Theory of Secrecy Systems – cryptography from the viewpoint of information theory

Tarantula Technology
blockchain solutions

Your partner for …
your blockchain consulting, development, and hosting needs.
-Mark