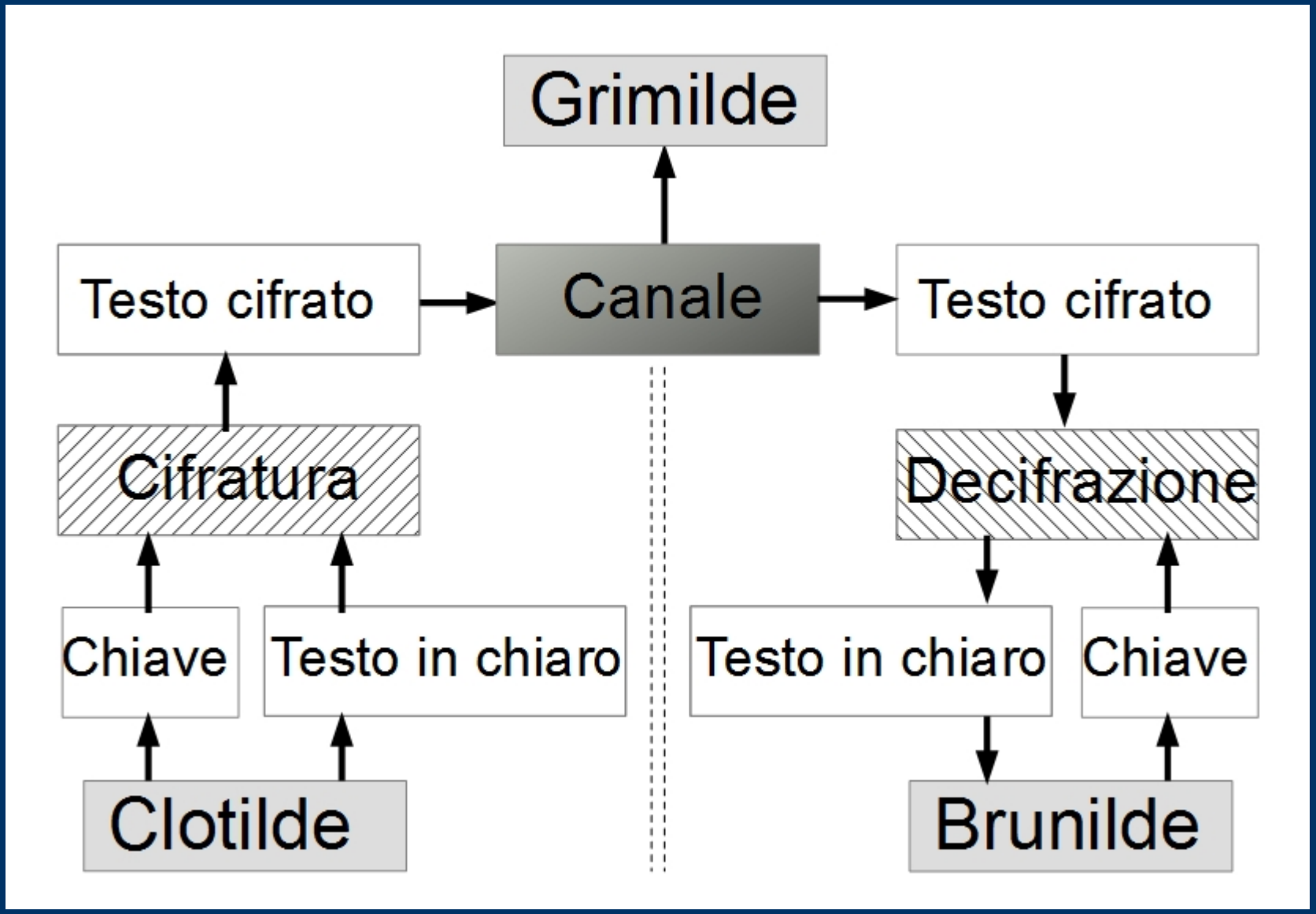
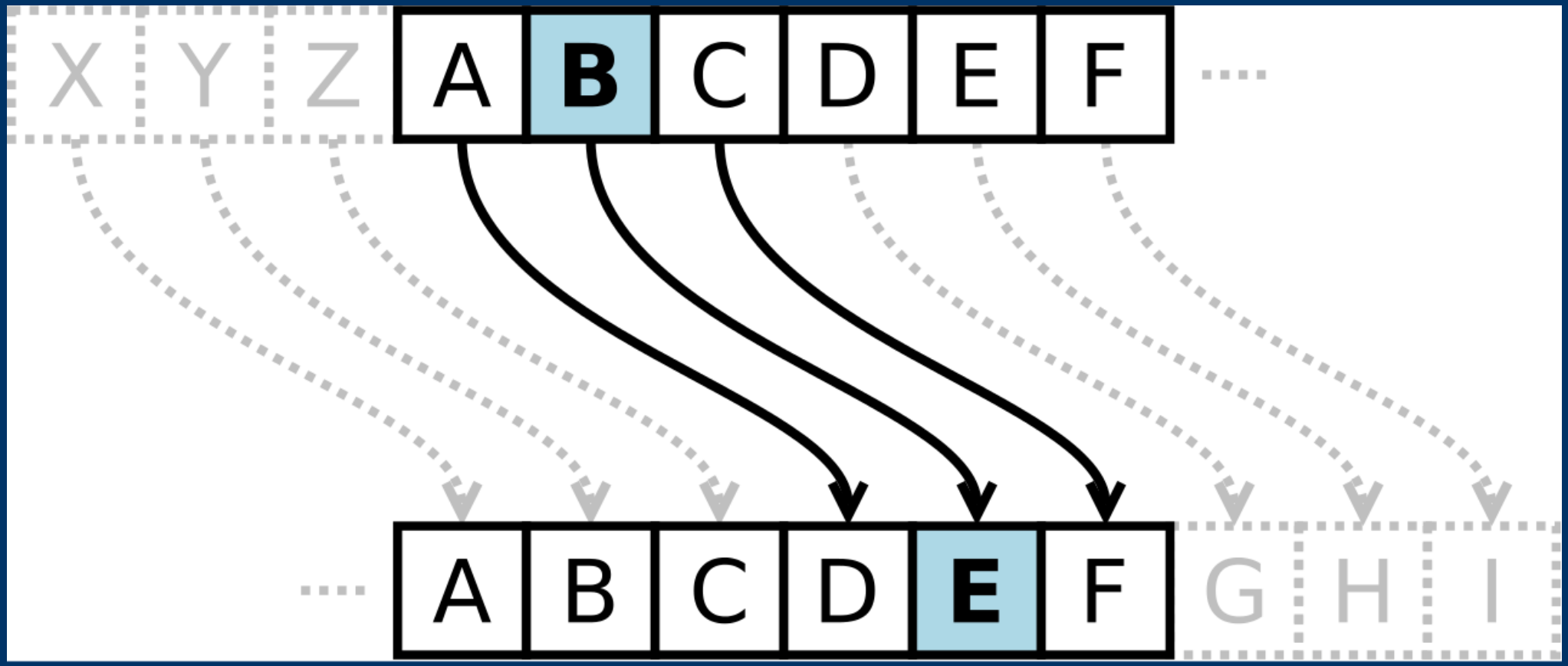
Messaggi segreti

La crittografia
da Cesare
ai moderni
computer

Conferenza di
Giorgio Chinnici

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


Grimilde
Testo cifrato
Canale
Testo cifrato
Cifratura
Decifrazione
Chiave
Testo in chiaro
Testo in chiaro
Chiave
Clotilde
Brunilde

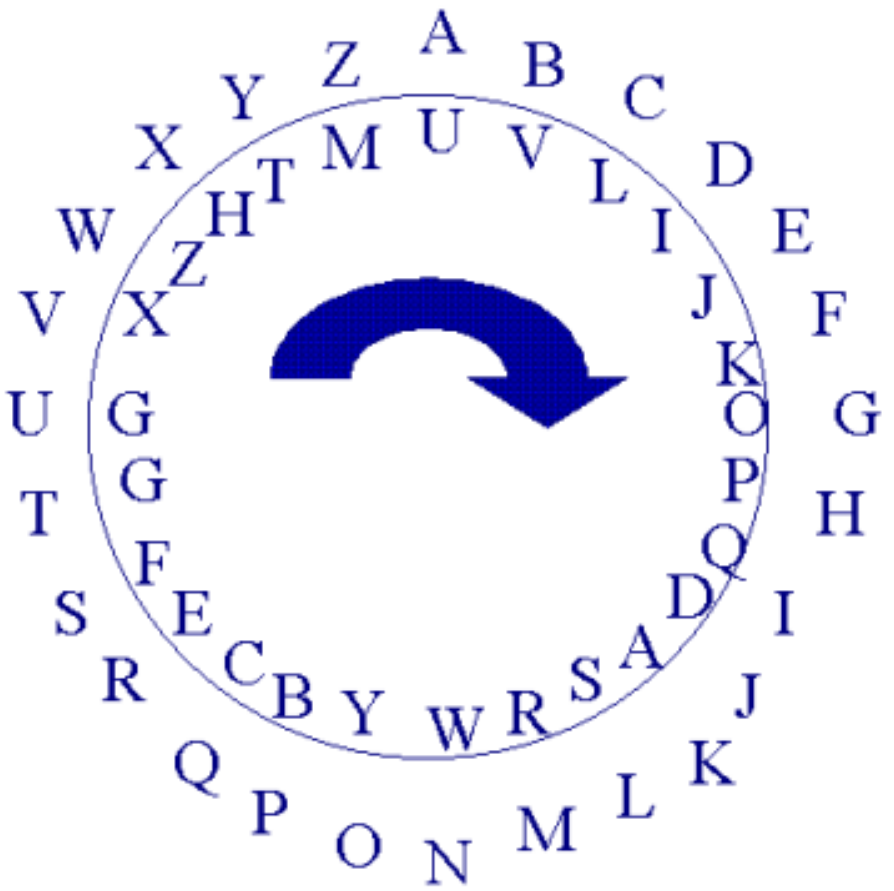

X Y Z
A B C D E F
....
.... A B C D E F G H I

Cifrario di Cesare

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
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	q	r	s
gallia est omnis divisa in partes tres																									
jdoold hvw rpqlv glylvd lq sduwhv wuhv																									

Disco dell'Alberti

Leon Battista Alberti, architetto italiano, XV secolo

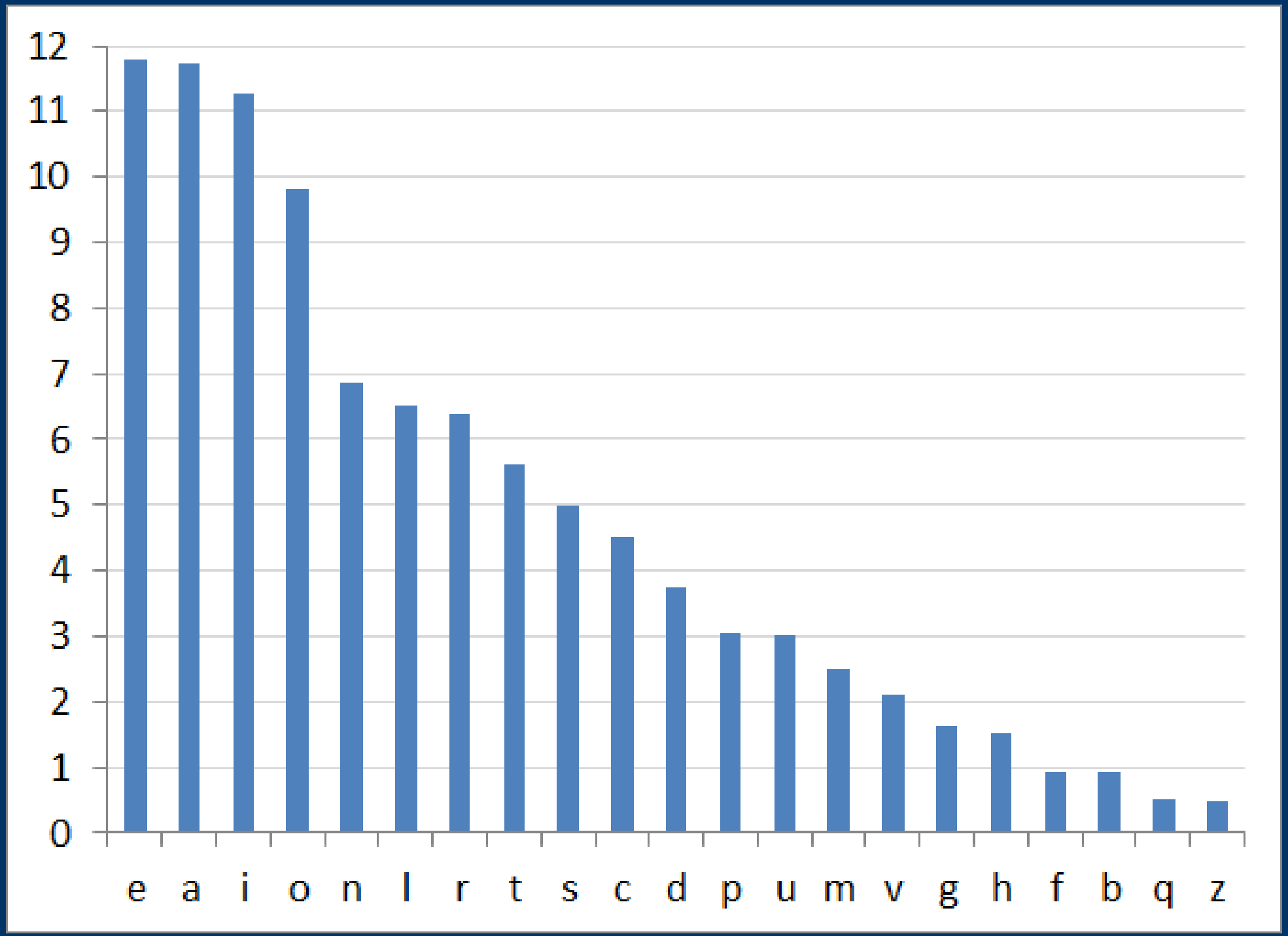


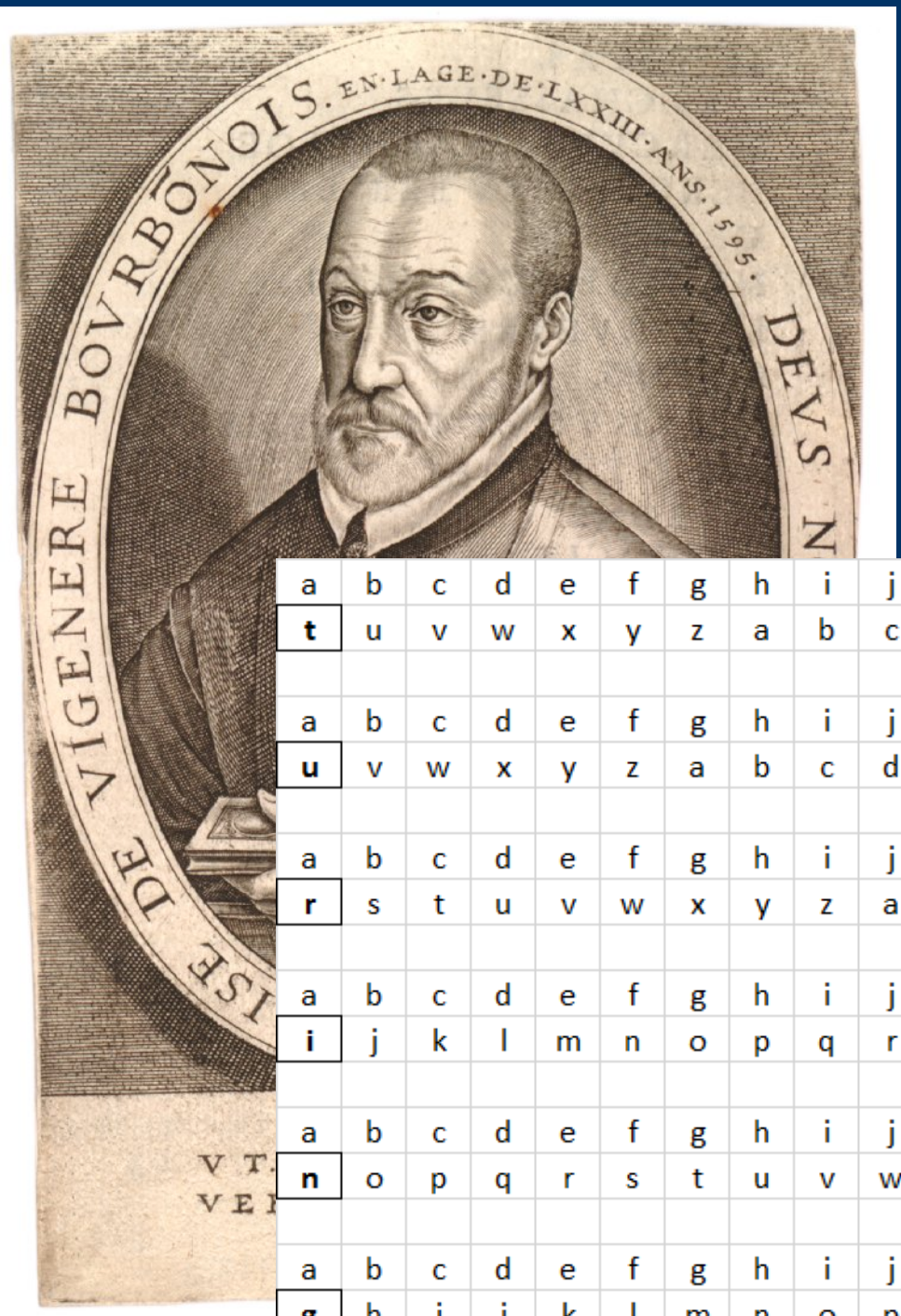
testo in chiaro

D I S C O

I Q F L Y

testo cifrato


12
11
10
9
8
7
6
5
4
3
2
1
0
e a i o n l r t s c d p u m v g h f b q z



Cifrario di Vigenère

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
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
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
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
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
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
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
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
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
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
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
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

gallia est omnis divisa in partes tres

zuctvg xmk wztbm uqiolu zv cgknva gxxm


CONFEDERATE
TWENTY DOLLAR
Well pay
on demand
Richmond
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
C S A

CLASS OF SERVICE DESIRED

Fast Day Message	X
Day Letter	
Night Message	
Night Letter	

Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8307

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No. MC

Check 3350

Time Filed

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

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

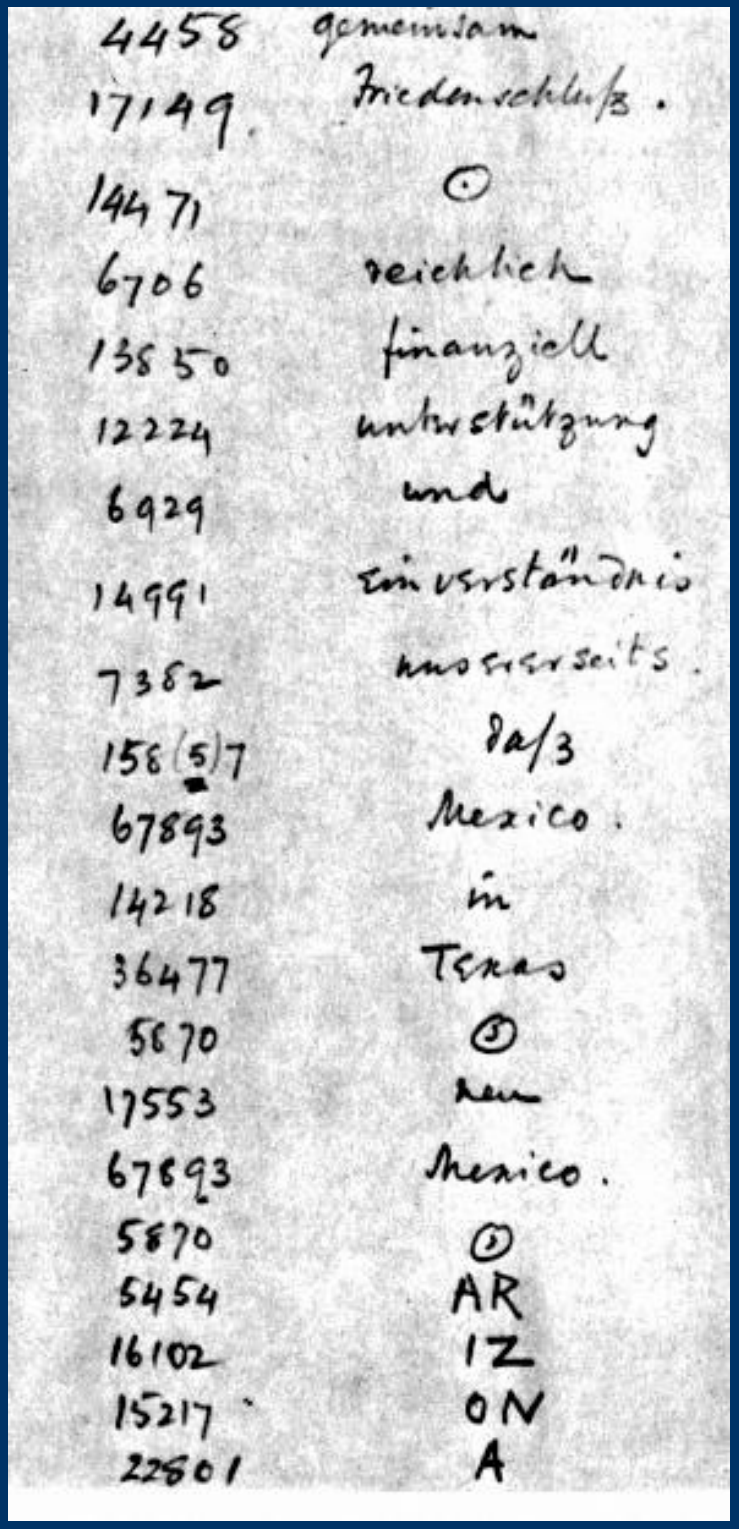
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

INSPECTED

Charge German Embassy.

862.20212/524


4458 gemeinsam
17149. Friedensschluß.
14471 ⊙
6706 reichlich
13850 finanziell
12224 unterstützung
6929 und
14991 einverständnis
7382 unsererseits.
156(5)7 da/3
67893 Mexico.
14218 in
36477 Texas
5870 ⊙
17553 neu
67893 Mexico.
5870 ⊙
5454 AR
16102 IZ
15217 ON
22601 A

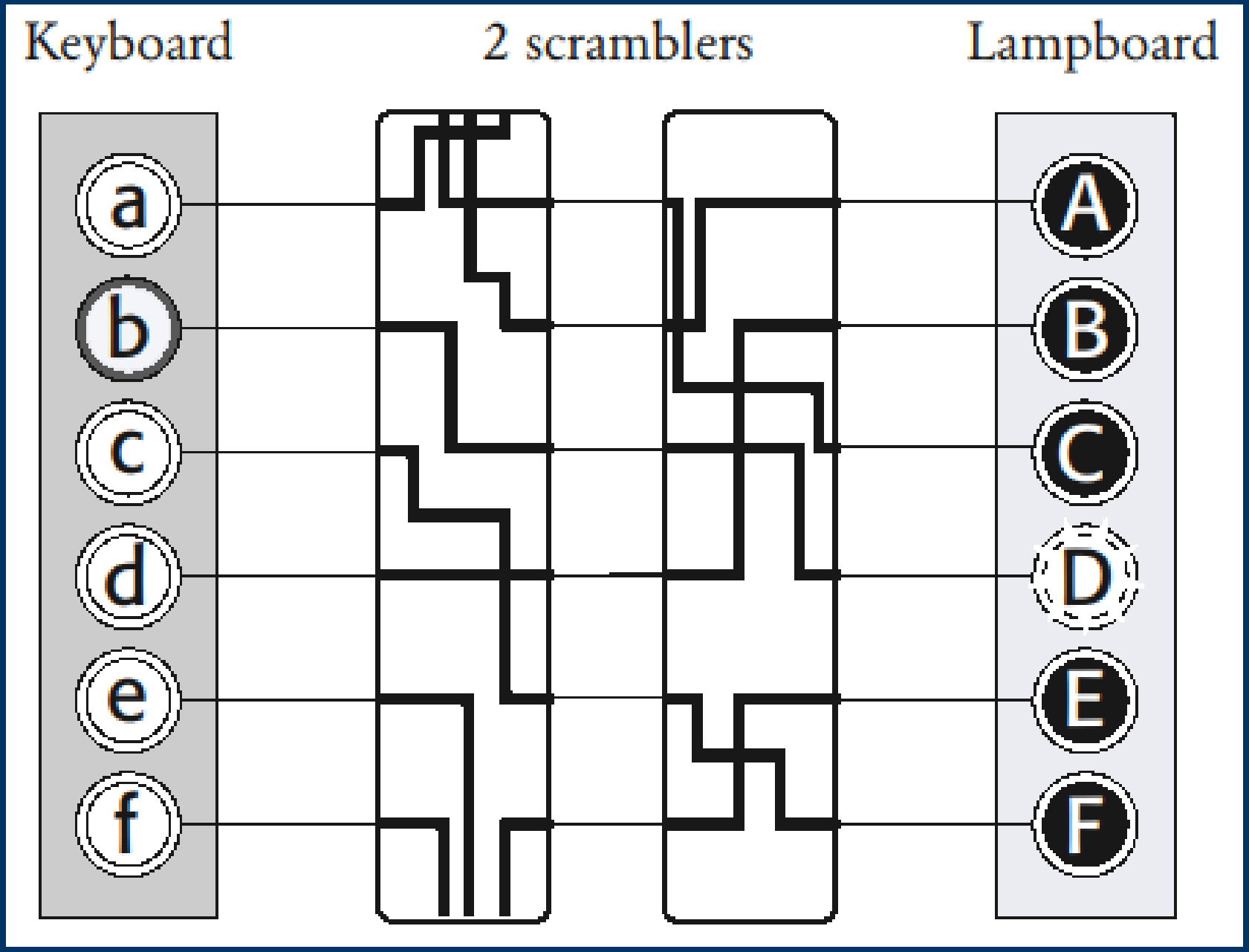
CLAS... ...ANCELED
...ctor 1-8-58
...erson, State Dept.
By *[signature]*
Date *Oct. 22, 1957*

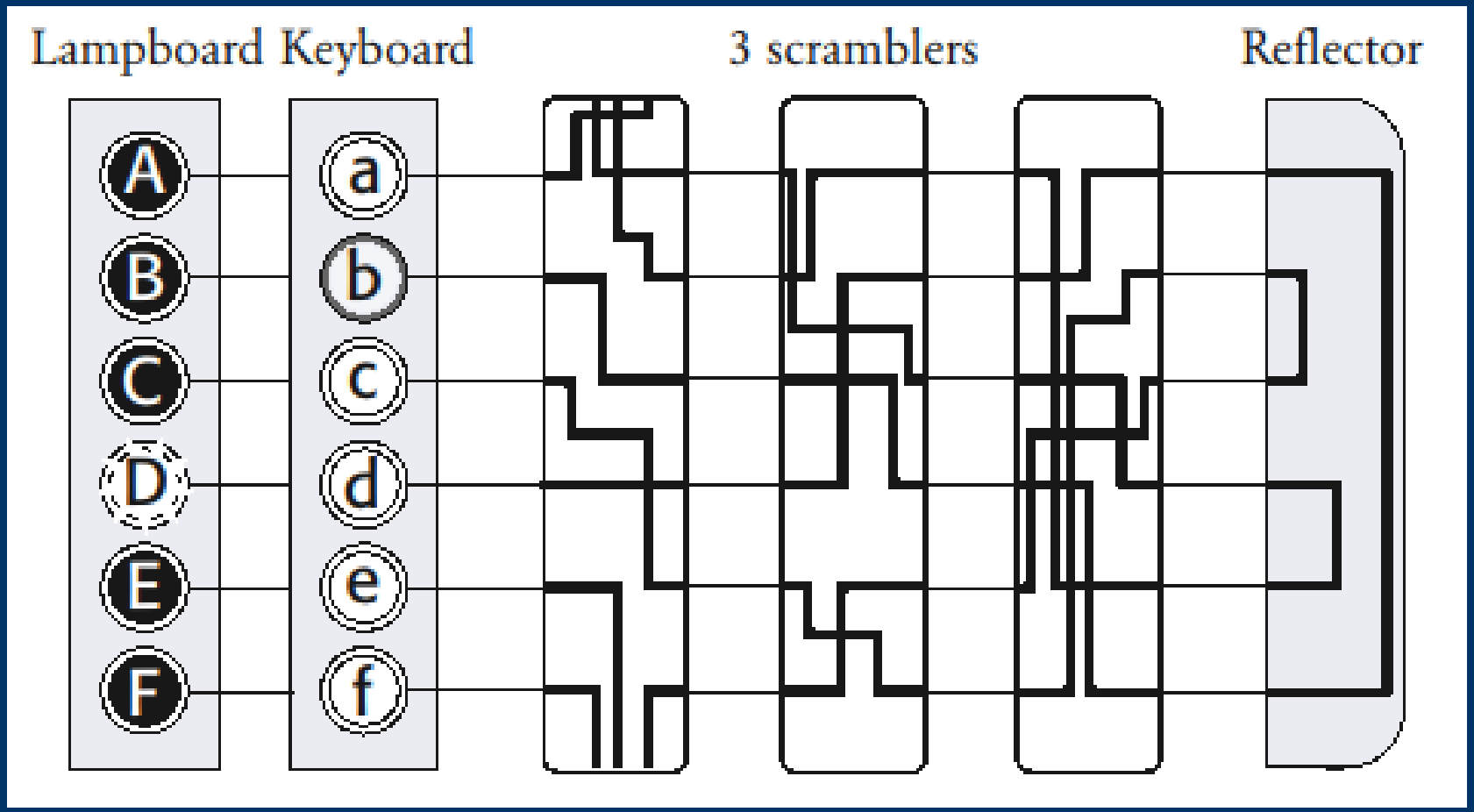
TELEGRAM RECEIVED.

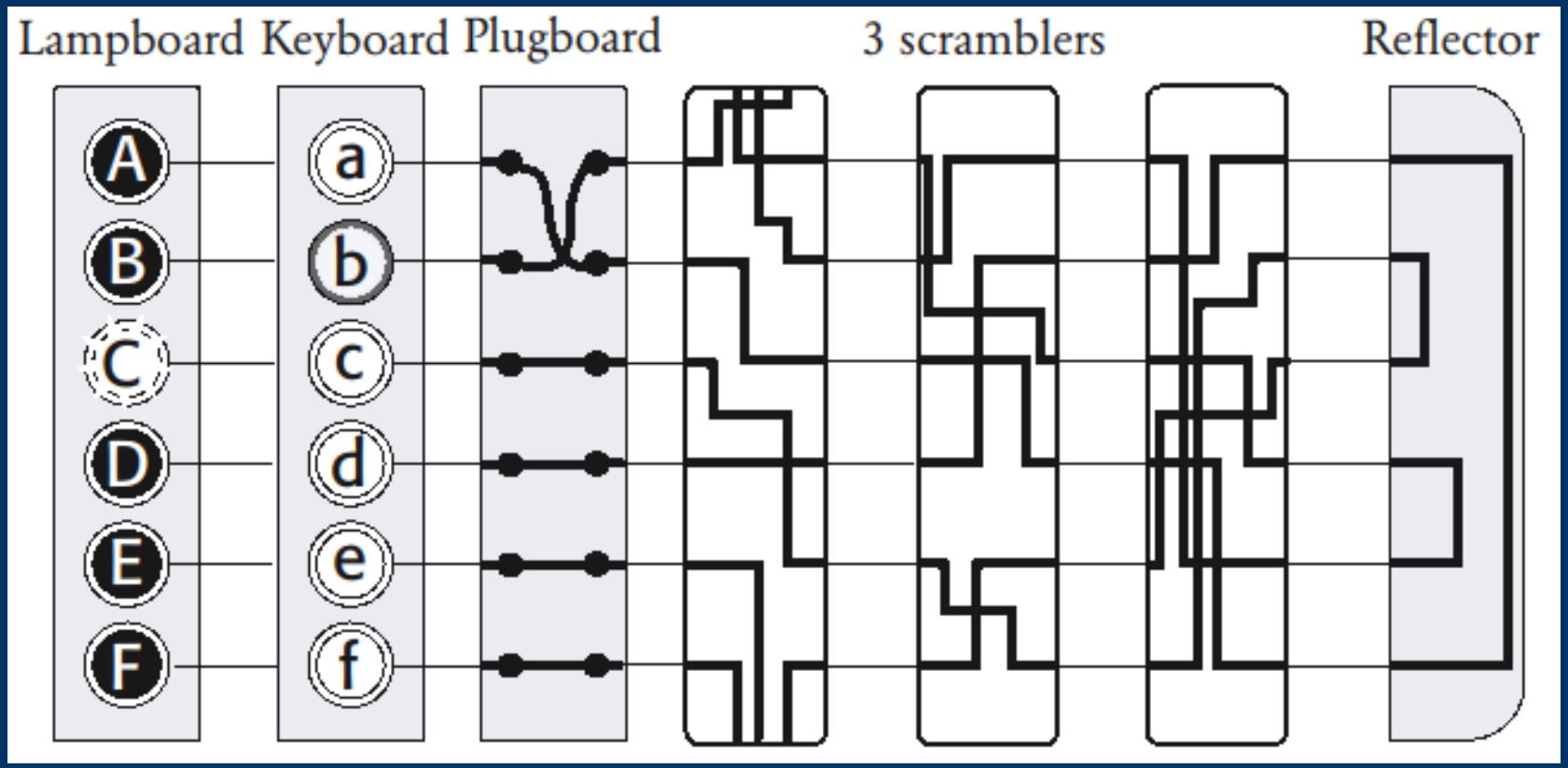
FROM 2nd from London # 5747.

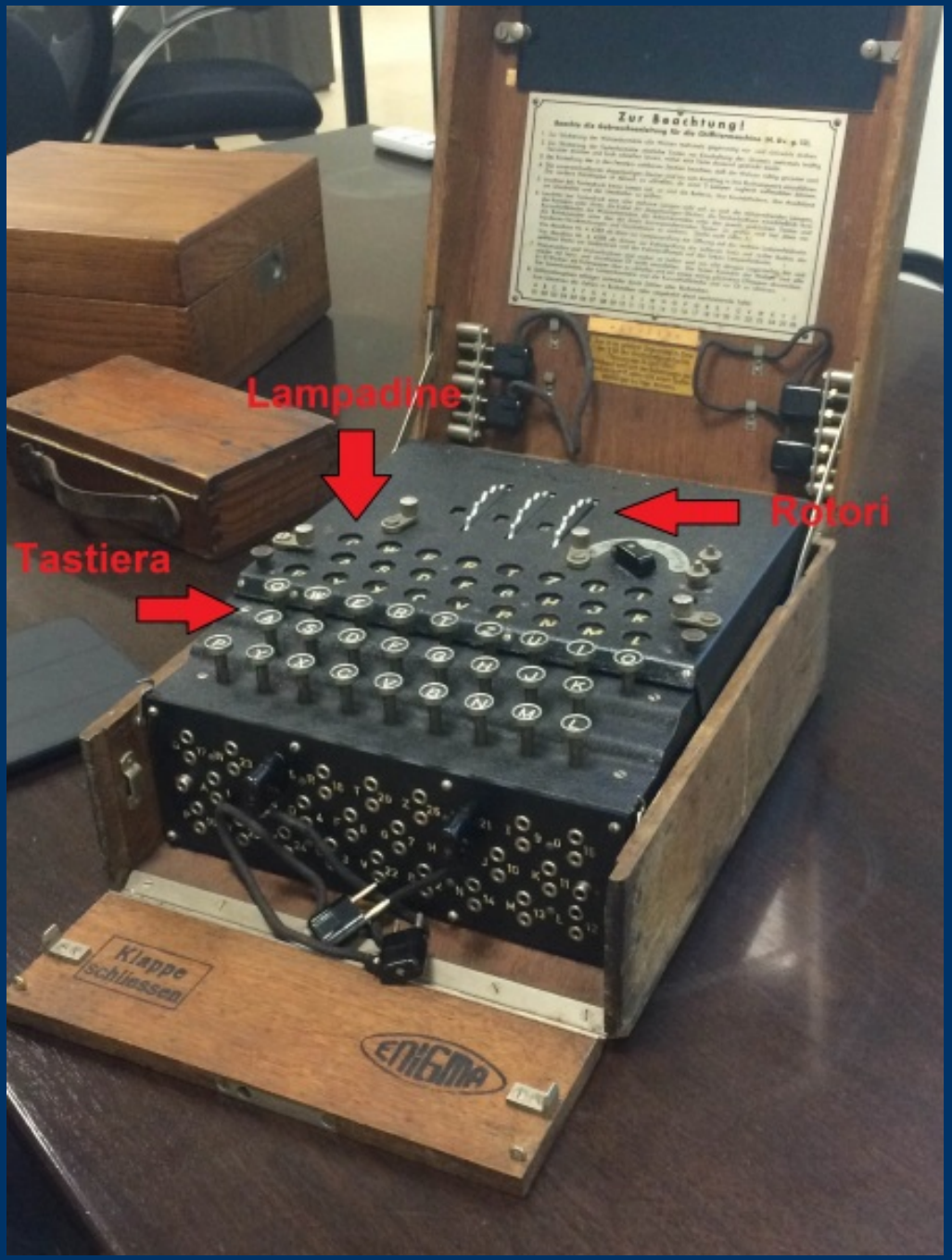
"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous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


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


Keyboard
2 scramblers
Lampboard
a
b
c
d
e
f
A
B
C
D
E
F


Lampboard
Keyboard
3 scramblers
Reflector
A
B
C
D
E
F
a
b
c
d
e
f

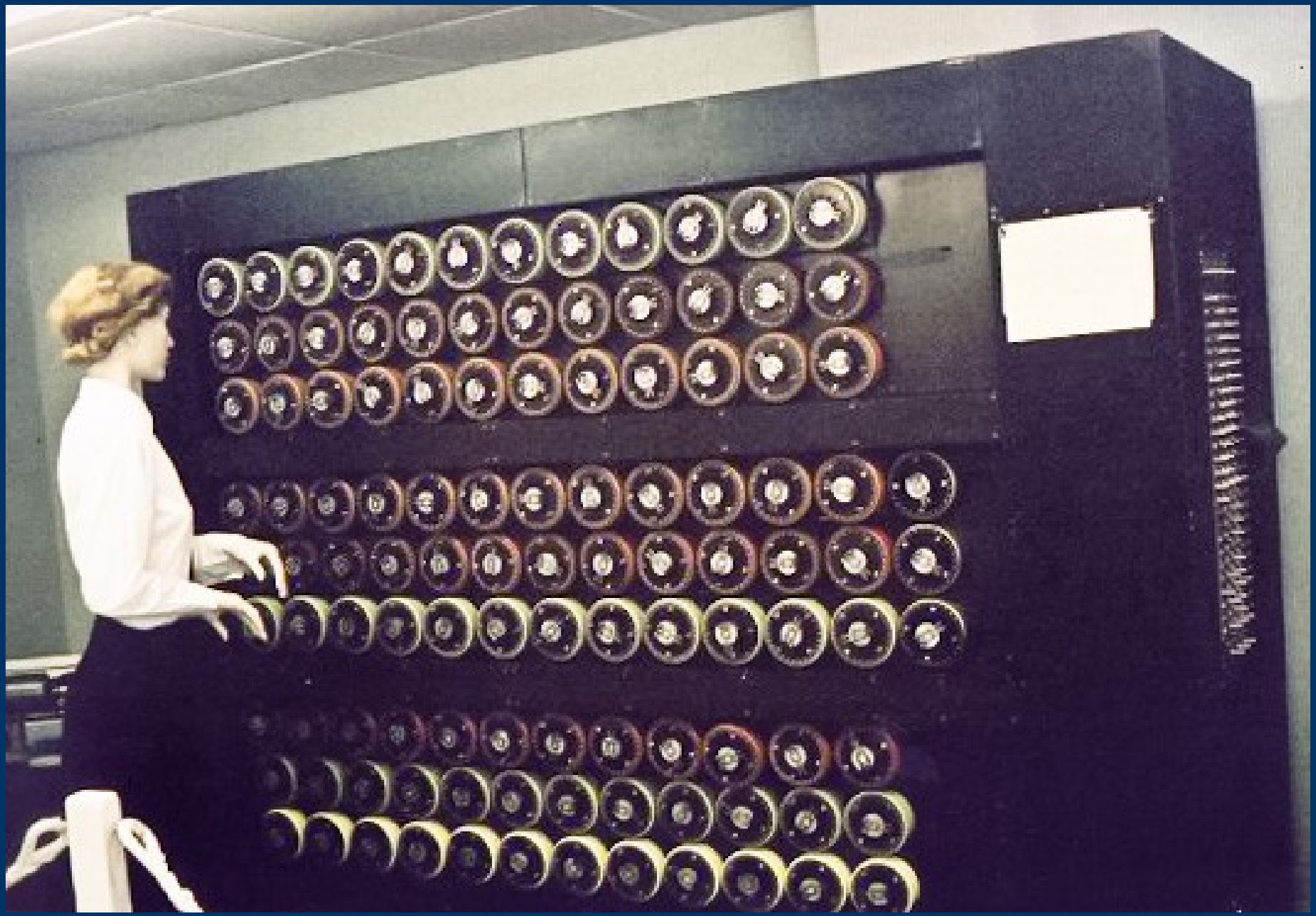

Lampboard
Keyboard
Plugboard
3 scramblers
Reflector
A
B
C
D
E
F
a
b
c
d
e
f


Lampadine
Rotori
Tastiera
Zur Beachtung!
Klappe schliessen
ENIGMA

The ciphertext is **DAEDAQOZSIQMMKBILGMPWHAIV**

The plaintext is **KEINEZUSAETZEZUMVORBERIQT**

(keine Zusätze zum Vorbericht)



U.S. Marine Corps

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

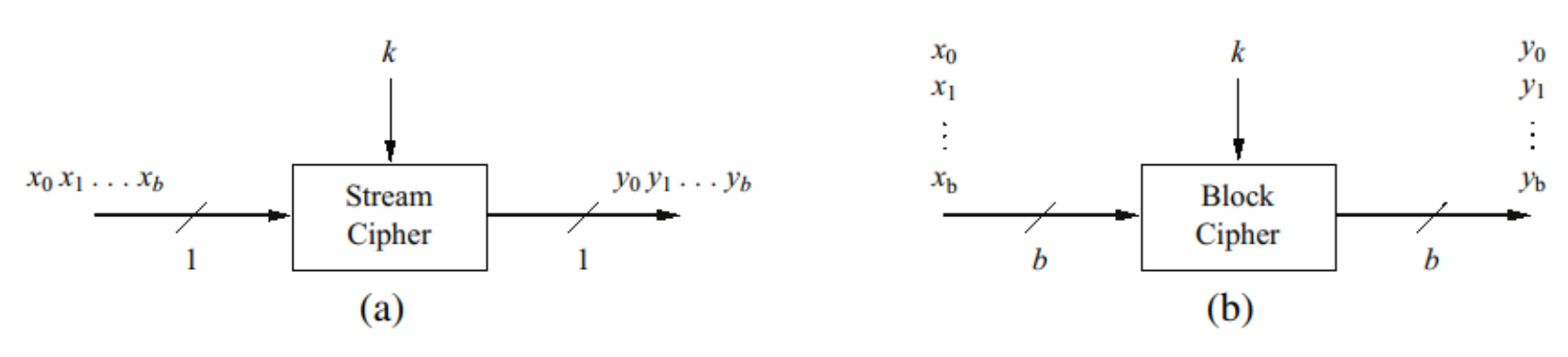
x_1	x_2	AND
0	0	0
0	1	0
1	0	0
1	1	1

x_1	x_2	OR
0	0	0
0	1	1
1	0	1
1	1	1

x_1	x_2	XOR
0	0	0
0	1	1
1	0	1
1	1	0

x_i	s_i	y_i
0	**0**	**0**
0	**1**	**1**
1	0	1
1	1	0

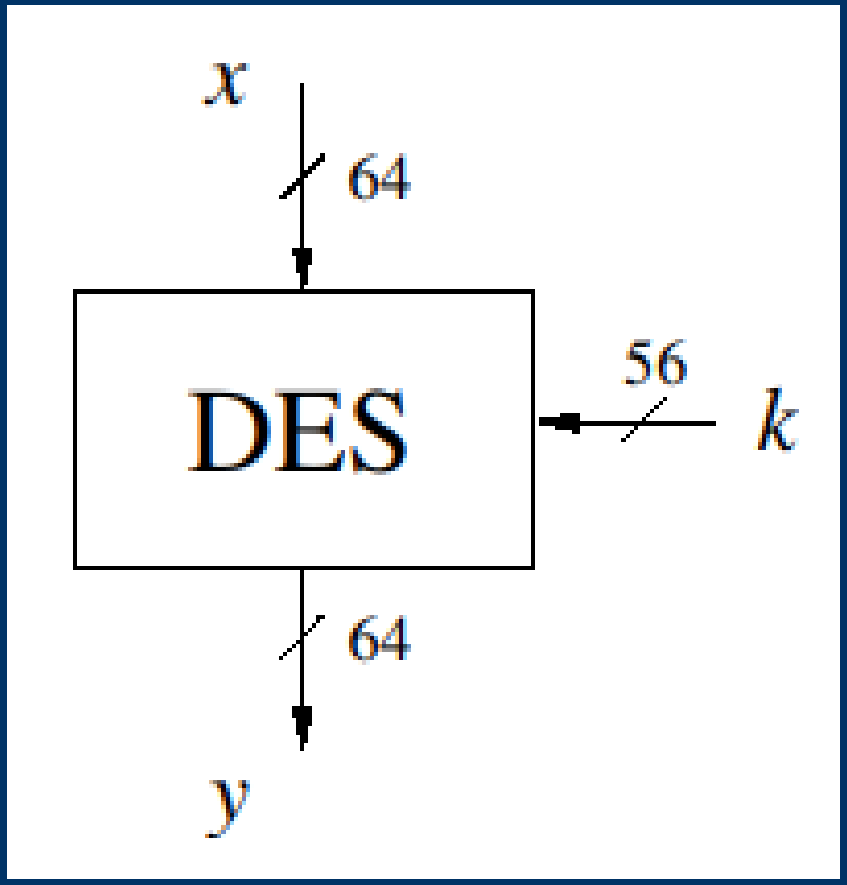
Message	**HELLO**
Message in ASCII	**01001000010001011001100100110010011111**
Key = **DAVID**	**10001001000001101011010010011000100**
Ciphertext	**00011000000100001101000001010001011**


k
$x_0\, x_1 \ldots x_b$
Stream Cipher
$y_0\, y_1 \ldots y_b$
1
1
(a)
x_0
x_1
x_b
k
y_0
y_1
y_b
Block Cipher
b
b
(b)

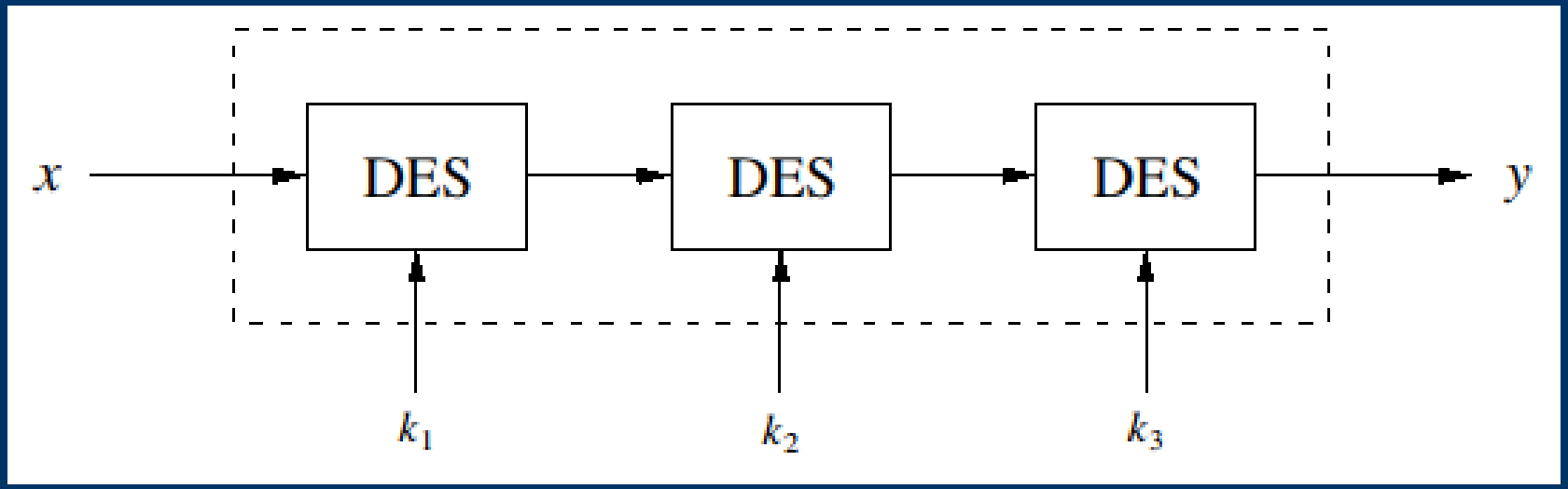
$$
\begin{aligned}
x_0, \ldots, x_6 &= 1000001 = \mathtt{A} \\
&\quad \oplus \\
s_0, \ldots, s_6 &= 0101100 \\
y_0, \ldots, y_6 &= 1101101 = \mathtt{m}
\end{aligned}
$$

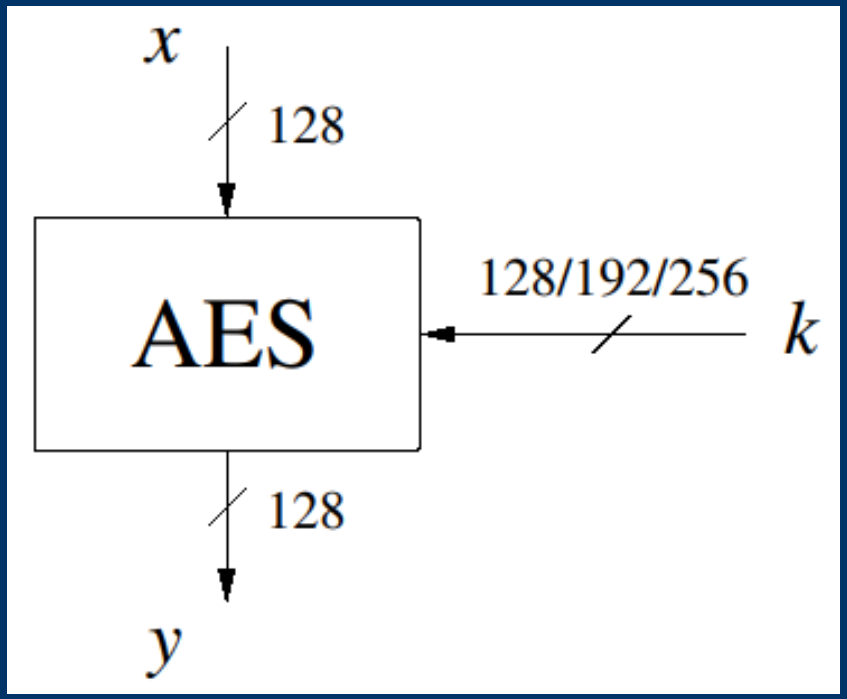
$$
\xrightarrow{\mathtt{m}=1\dot{1}01101}
$$

$$
\begin{aligned}
y_0, \ldots, y_6 &= 1101101 \\
&\quad \oplus \\
s_0, \ldots, s_6 &= 0101100 \\
x_0, \ldots, x_6 &= 1000001 = \mathtt{A}
\end{aligned}
$$

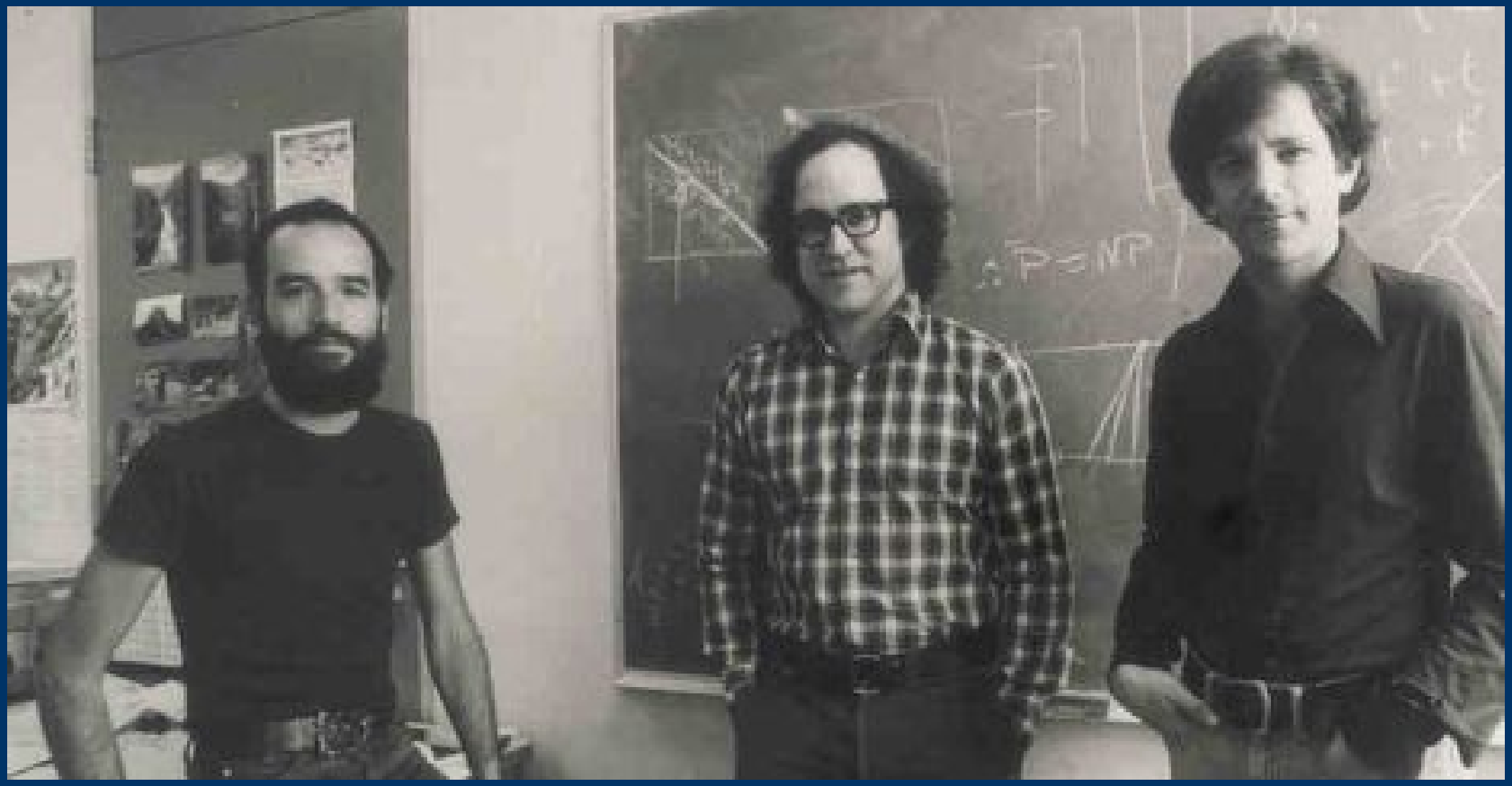

x
64
DES
56
k
64
y

Jun. 1997	DES Challenge I broken through brute-force; distributed effort on the Internet took 4.5 months
Feb. 1998	DES Challenge II–1 broken through brute-force; distributed effort on the Internet took 39 days
Jul. 1998	DES Challenge II–2 broken through brute-force; Electronic Frontier Foundation built the Deep Crack key-search machine for about $250,000. The attack took 56 h (15 days average)
Jan. 1999	DES Challenge III broken through brute-force by distributed Internet effort combined with Deep Crack and a total search time of 22 hours
Apr. 2006	Universities of Bochum and Kiel built COPACOBANA key-search machine based on low-cost FPGAs for approximately $10,000. Average search time is 7 days

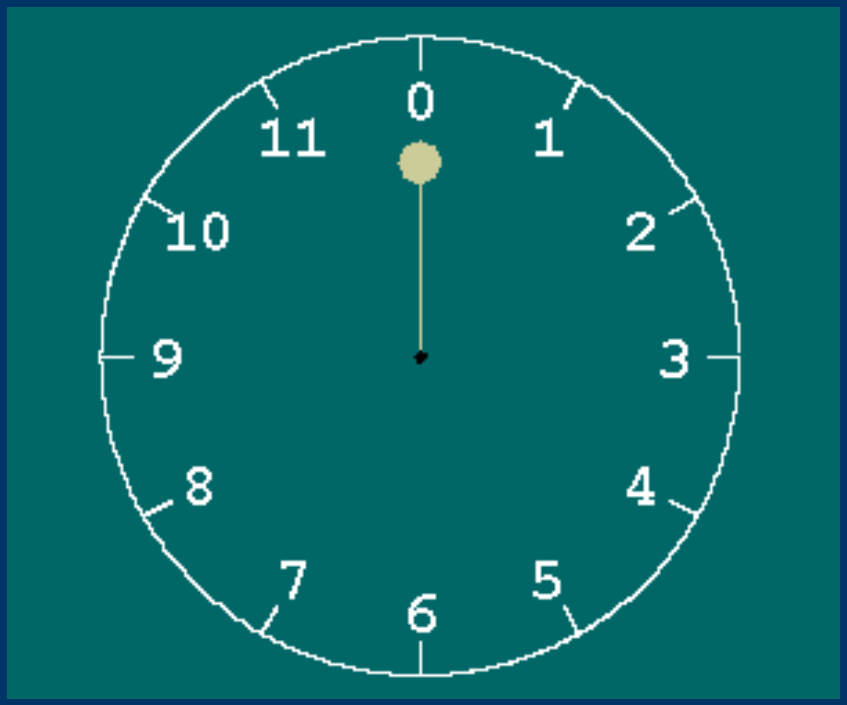

x
DES
DES
DES
y
k_1
k_2
k_3


x
128
AES
128/192/256
k
128
y


Alice
Bob


∴P=NP

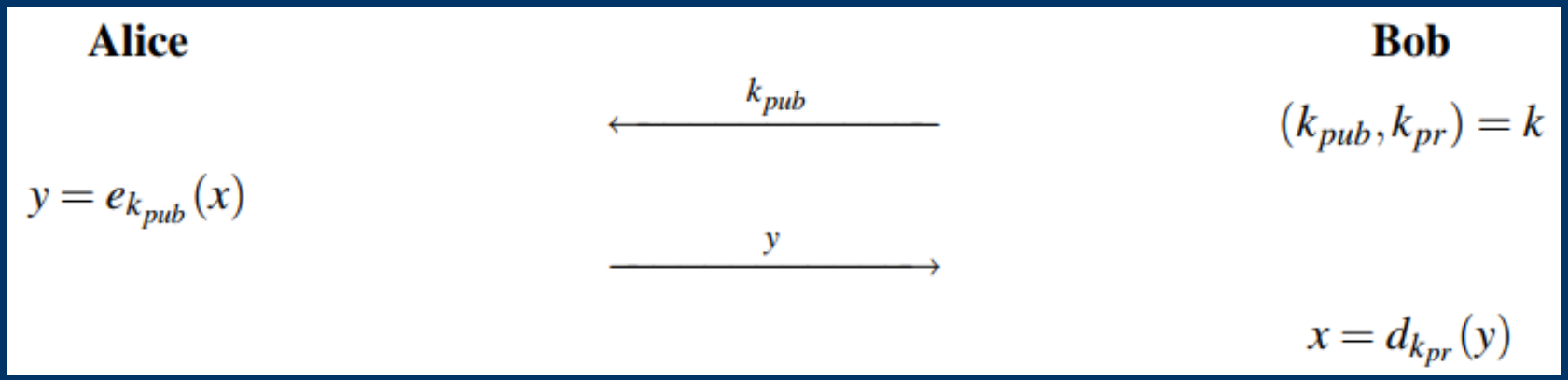

RON RIVEST, ADI SHAMIR & LEN ADLEMAN
acm
RSA public-key cryptography
A.M. TURING AWARD
2002

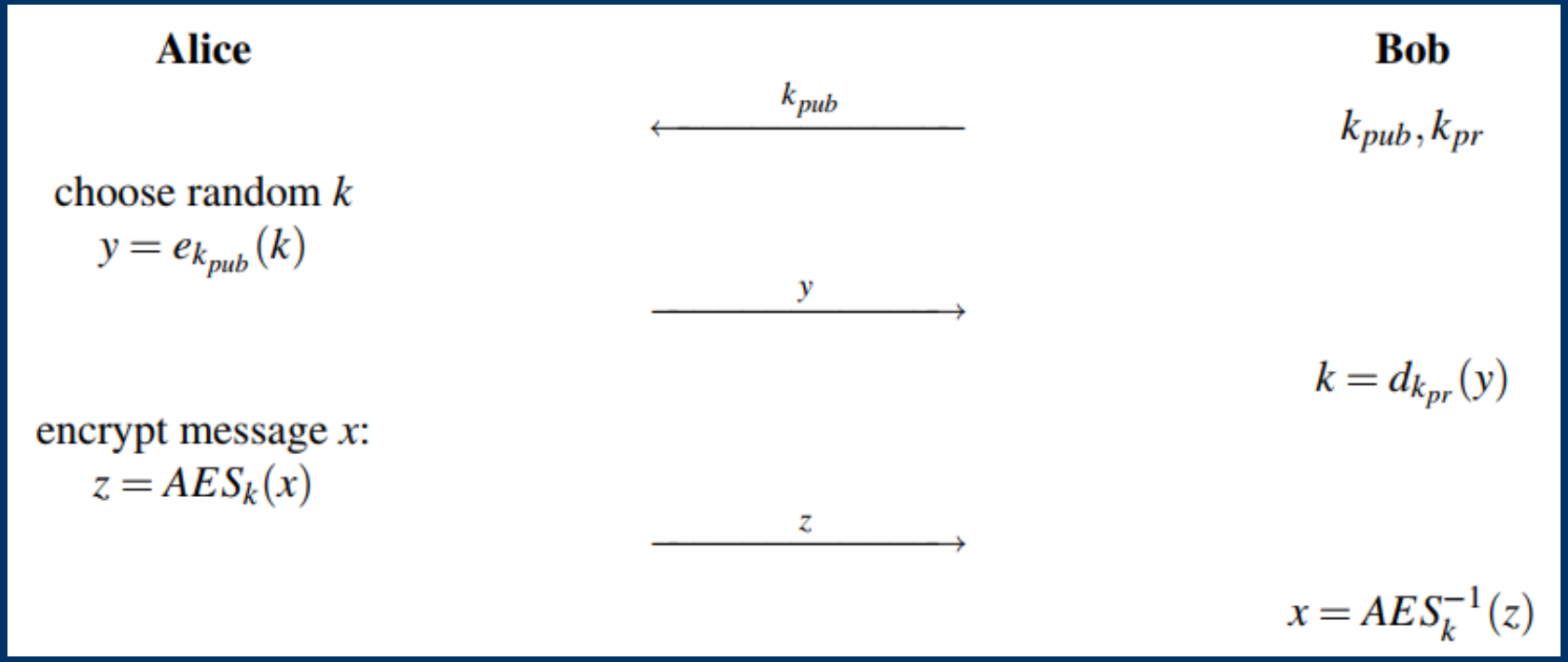

0
1
2
3
4
5
6
7
8
9
10
11

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

$p = 17159 \quad q = 10247$

$N = pq = 175828273$


Alice
Bob
k_{pub}
$(k_{pub}, k_{pr}) = k$
$y = e_{k_{pub}}(x)$
y
$x = d_{k_{pr}}(y)$


Alice
Bob
k_{pub}
k_{pub}, k_{pr}
choose random k
$y = e_{k_{pub}}(k)$
y
$k = d_{k_{pr}}(y)$
encrypt message x:
$z = AES_k(x)$
z
$x = AES_k^{-1}(z)$

Alice		Bob
message $x = 4$		1. choose $p = 3$ and $q = 11$ 2. $n = p \cdot q = 33$ 3. $\Phi(n) = (3-1)(11-1) = 20$ 4. choose $e = 3$ 5. $d \equiv e^{-1} \equiv 7 \bmod 20$
	$\xleftarrow{k_{pub}=(33,3)}$	
$y = x^e \equiv 4^3 \equiv 31 \bmod 33$		
	$\xrightarrow{y=31}$	
		$y^d = 31^7 \equiv 4 = x \bmod 33$


GIORGIO CHINNICI
Assoluto e relativo
La relatività da Galilei
ad Einsteln e oltre
HOEPLI


GIORGIO CHINNICI
Il labirinto
del continuo
Numeri, strutture, infiniti
HOEPLI


Giorgio Chinnici
Turing
L'Enigma di un genio
MICROSCOPI
HOEPLI


Giorgio Chinnici
Guarda caso
I meccanismi segreti
del mondo quantistico
MICROSCOPI
HOEPLI


Giorgio Chinnici
La stella
danzante
Sei versioni del caos
MICROSCOPI
HOEPLI