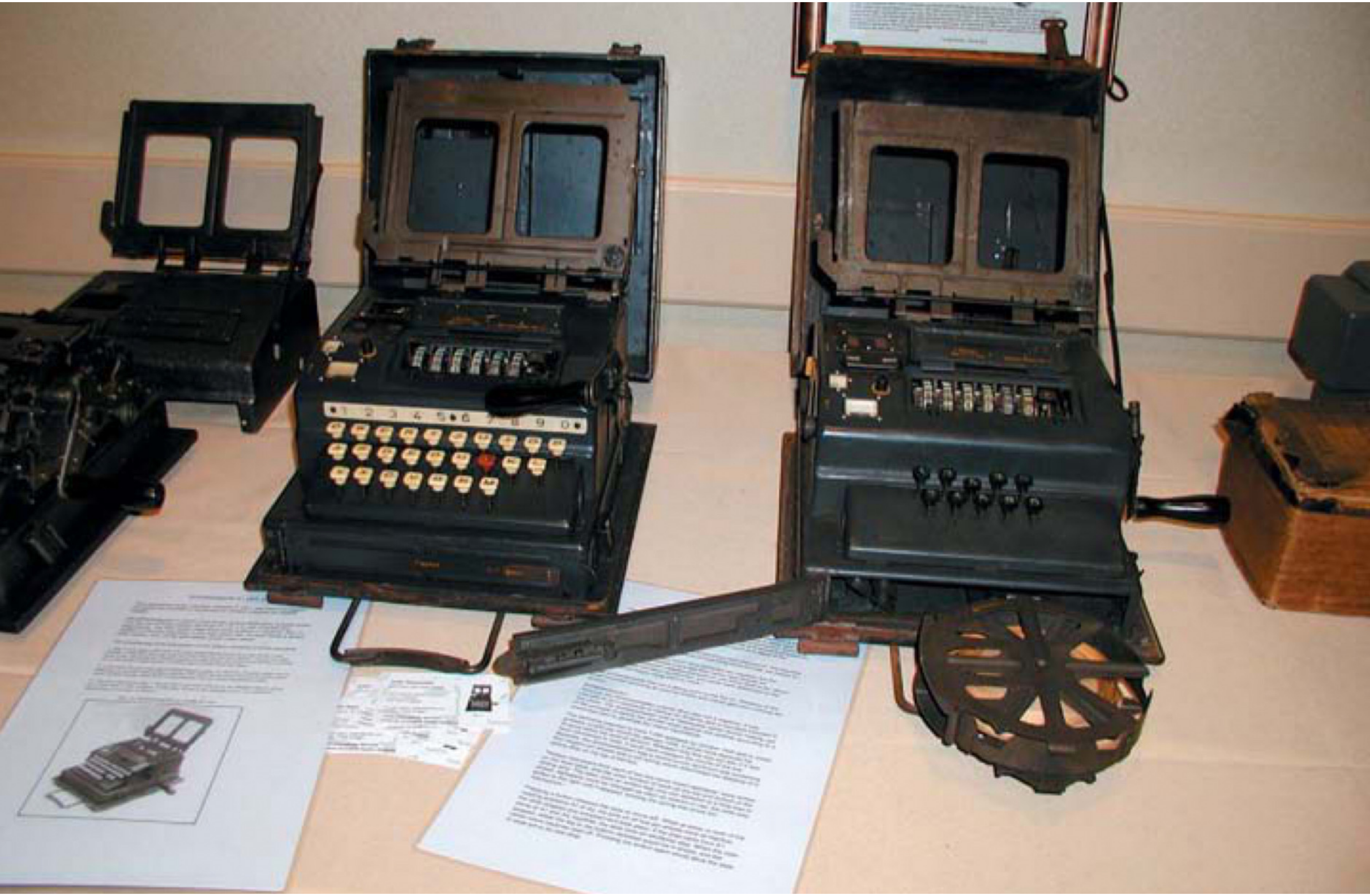
Cryptography

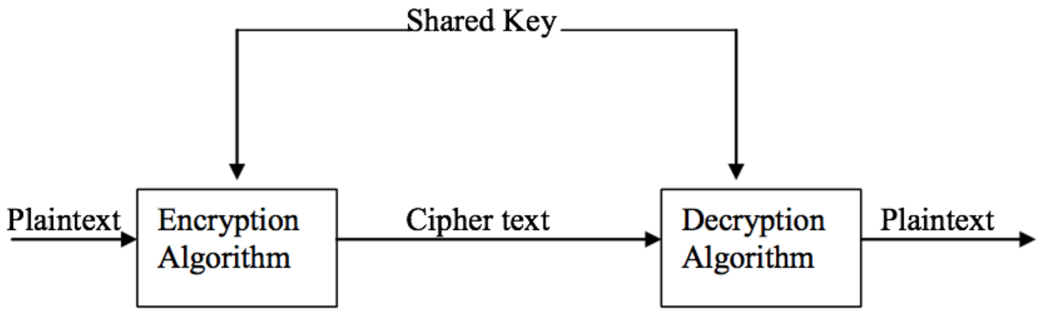
Where Security Meets Mathematics

Talia Q MSc. MA BCIS



1 2 3 4 5 6 7 8 9 0

Simplified Model of Conventional Encryption



Shared Key

Plaintext

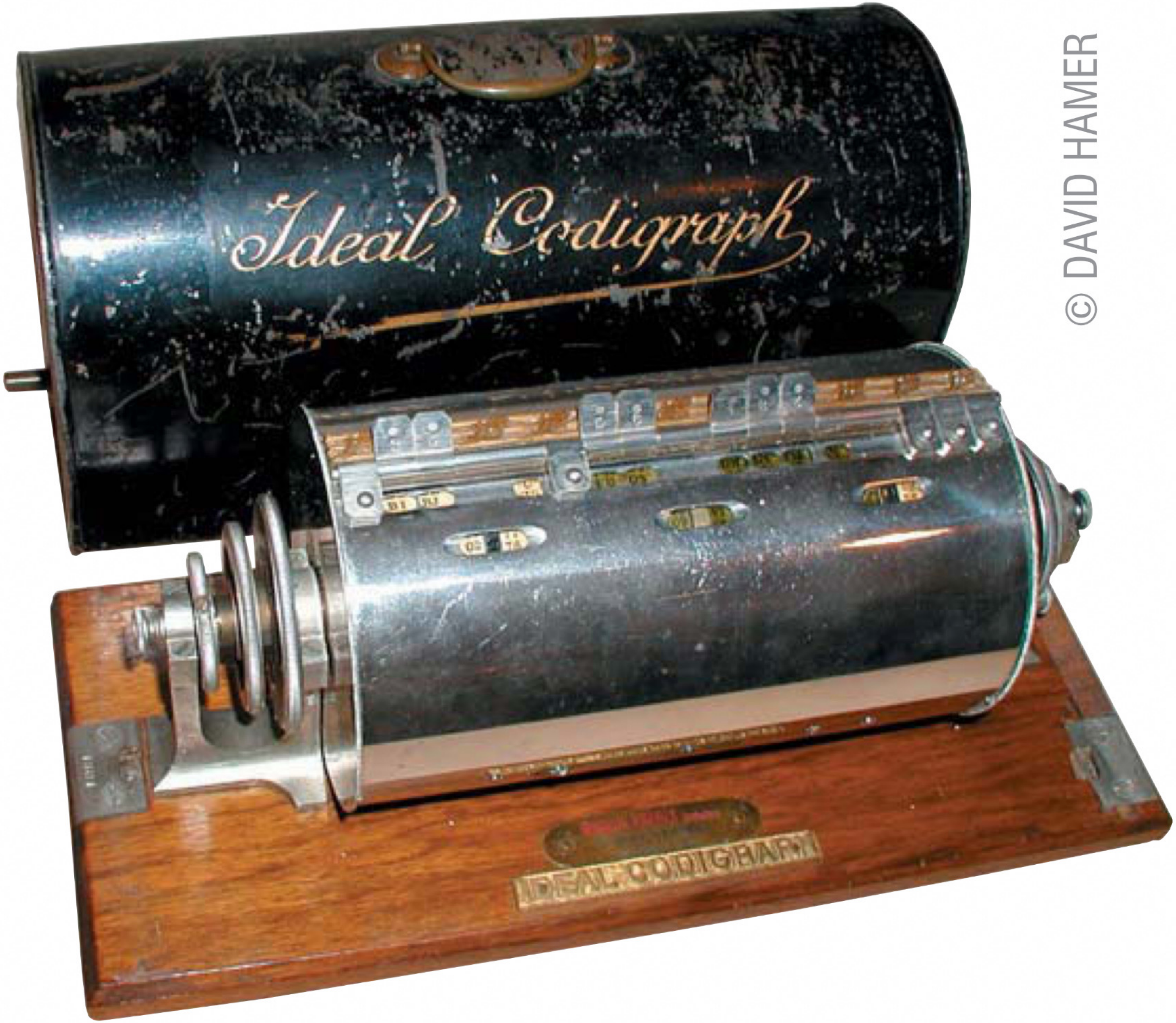
Encryption Algorithm

Cipher text

Decryption Algorithm

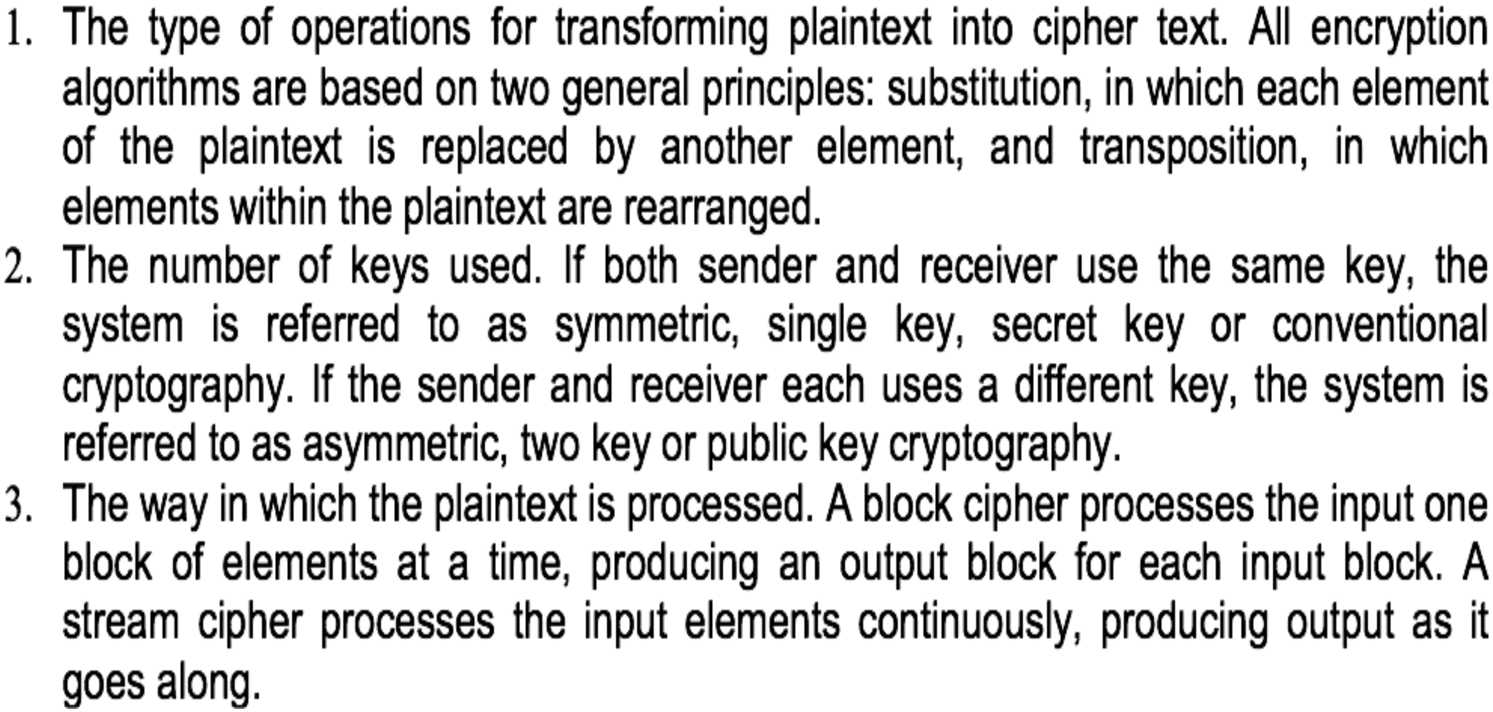
Plaintext

Figure 1. Simplified Model of Conventional Encryption



© DAVID HAMER

Cryptography



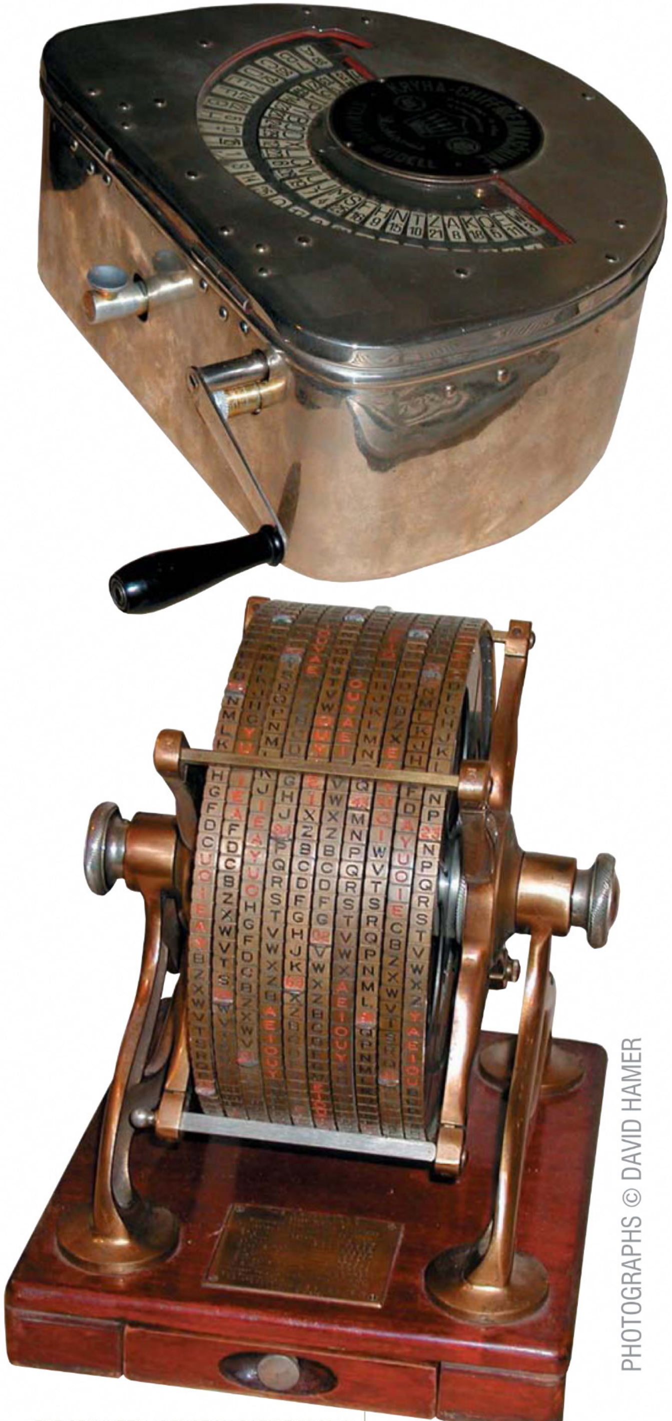
1. The type of operations for transforming plaintext into cipher text. All encryption algorithms are based on two general principles: substitution, in which each element of the plaintext is replaced by another element, and transposition, in which elements within the plaintext are rearranged.
2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single key, secret key or conventional cryptography. If the sender and receiver each uses a different key, the system is referred to as asymmetric, two key or public key cryptography.
3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output as it goes along.

Cryptanalysis

- Cipher text only. The attacker only knows the cipher text and tries to recover the plaintext.
- Known plaintext. The attacker knows the cipher text to be decoded, and several pairs of plaintext and corresponding cipher text.
- Chosen plaintext. The attacker knows the cipher text to be decoded. The attacker can also choose plaintext and ask the sender to output the corresponding cipher text.
- Chosen cipher text. The attacker knows the cipher text to be decoded. The attacker can also choose cipher text (different from the purported cipher text) and ask the receiver to output the corresponding plaintext.
- A combination of 3 and 4.

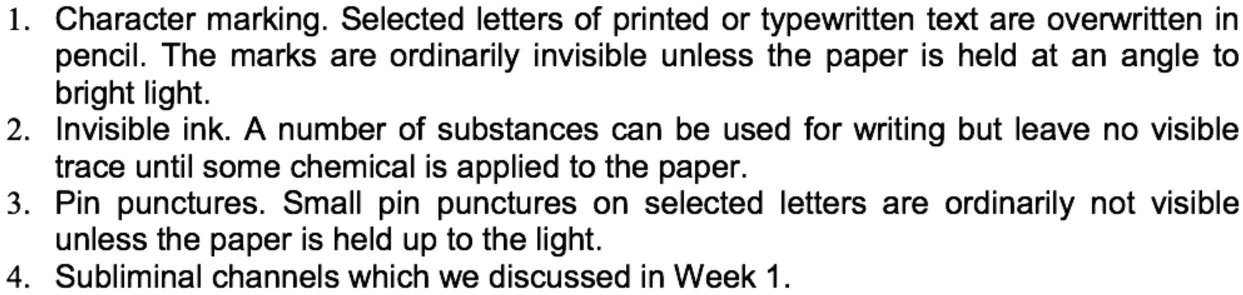
Steganography

- Character marking. Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily invisible unless the paper is held at an angle to bright light.
- Invisible ink. A number of substances can be used for writing but leave no visible trace until some chemical is applied to the paper.
- Pin punctures. Small pin punctures on selected letters are ordinarily not visible unless the paper is held up to the light.
- Subliminal channels which we discussed in Week 1.



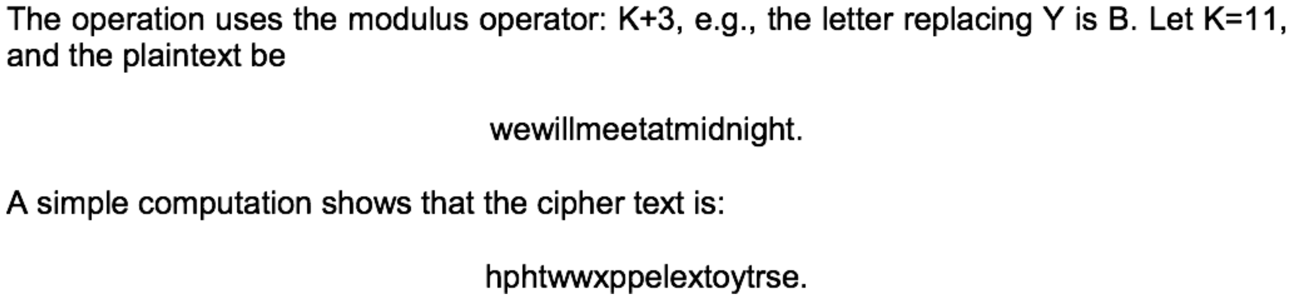
PHOTOGRAPHS © DAVID HAMER

Steganography



1. Character marking. Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily invisible unless the paper is held at an angle to bright light.
2. Invisible ink. A number of substances can be used for writing but leave no visible trace until some chemical is applied to the paper.
3. Pin punctures. Small pin punctures on selected letters are ordinarily not visible unless the paper is held up to the light.
4. Subliminal channels which we discussed in Week 1.

The Shift Cipher (Caesar Cipher)



The operation uses the modulus operator: K+3, e.g., the letter replacing Y is B. Let K=11, and the plaintext be

wewillmeetatmidnight.

A simple computation shows that the cipher text is:

hphtwwxppelextoytrse.

The Substitution Cipher

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

The cipher text is obtained by substituting each letter with another letter according to the above permutation table K. Correspondingly, we have a decryption table:

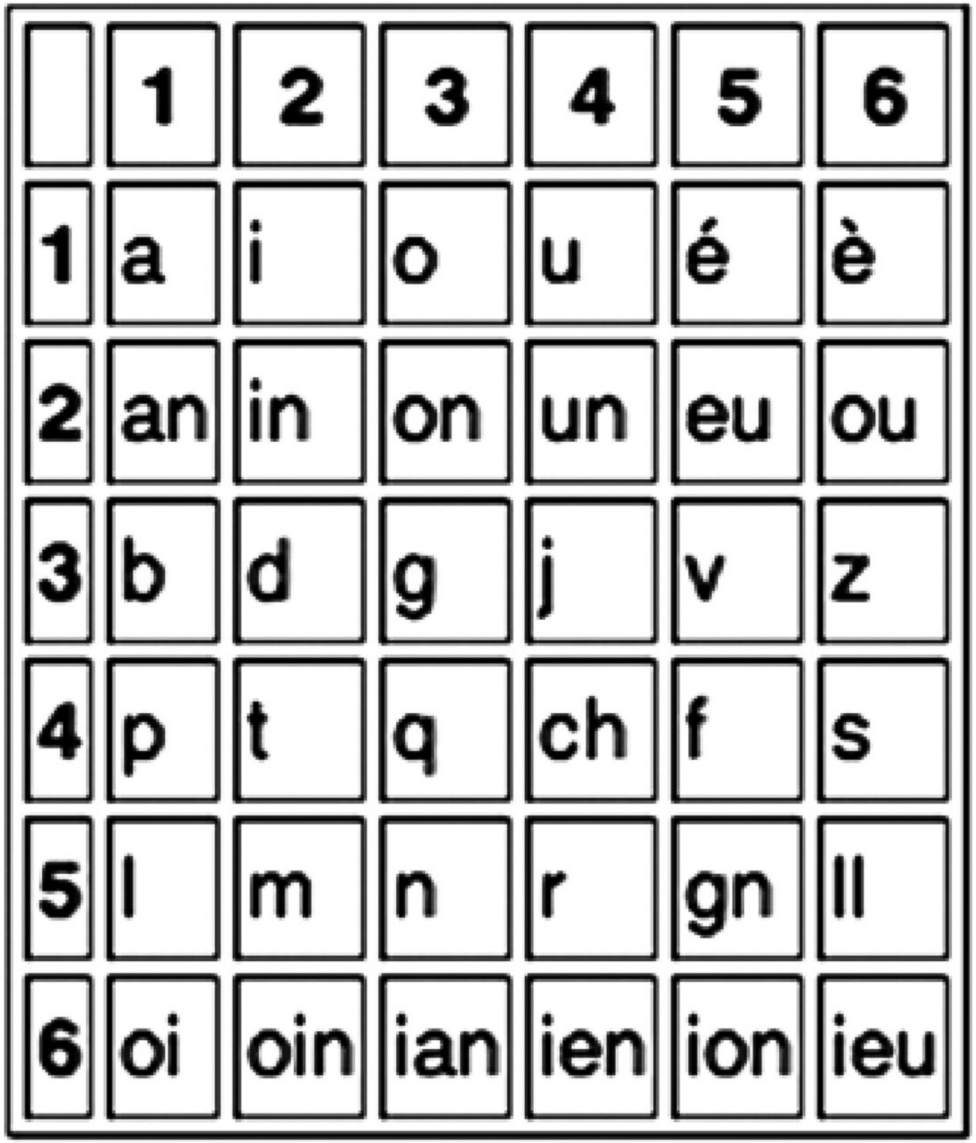
A	B	C	D	E	F	G	H	I	J	K	L	M
D	L	R	Y	V	O	H	E	Z	X	W	P	T
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	G	F	J	Q	N	M	U	S	K	A	C	I

As an exercise decrypt the following cipher text using the above decryption key.

mgzvyzlghcmhjmyxssfmnhahycdlmha

Masonic Cipher

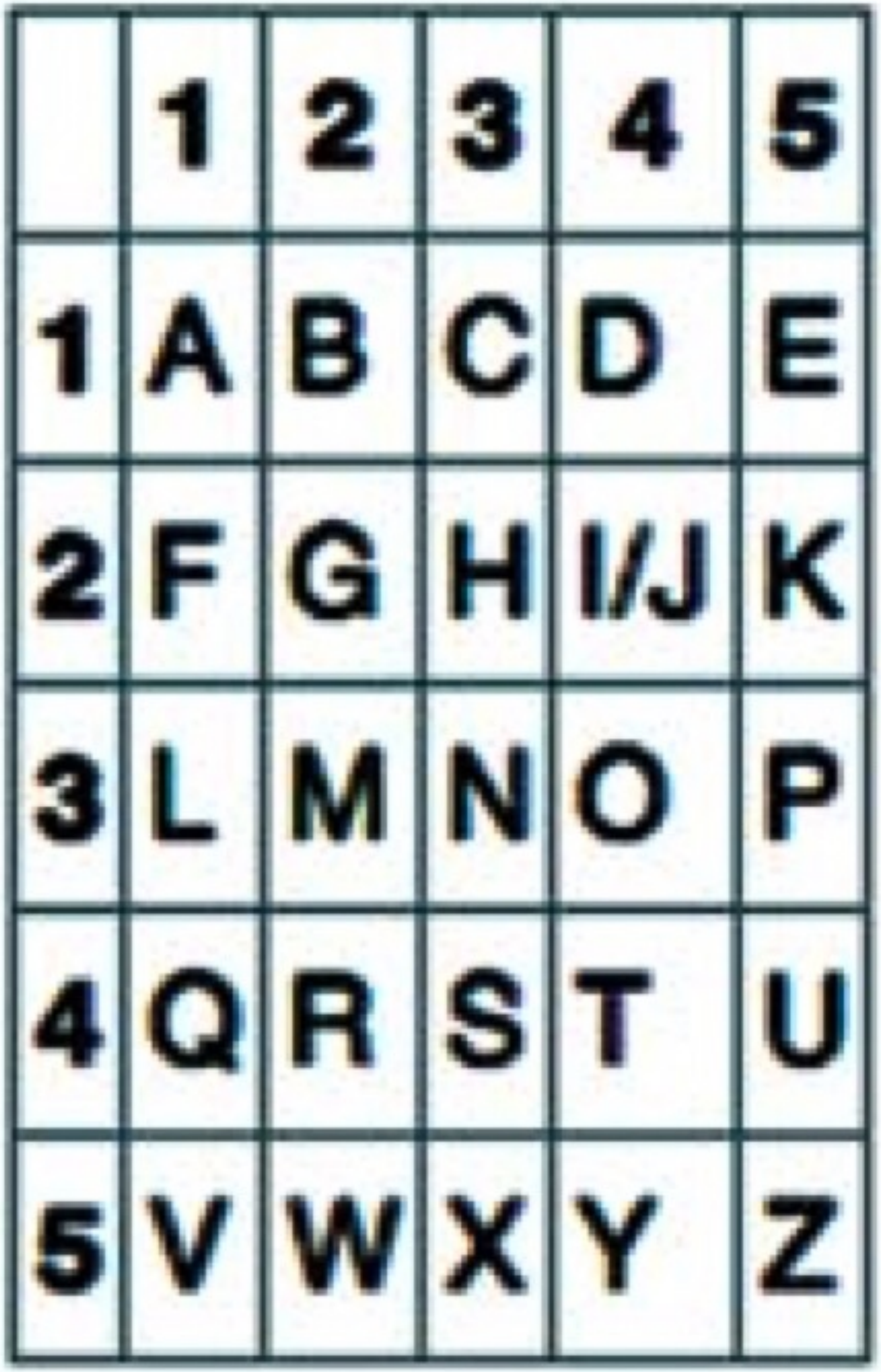
- Geometric simple substitution cipher which exchanges letters for symbols which are fragments of a grid
- The example key shows one way the letters can be assigned to the grid.



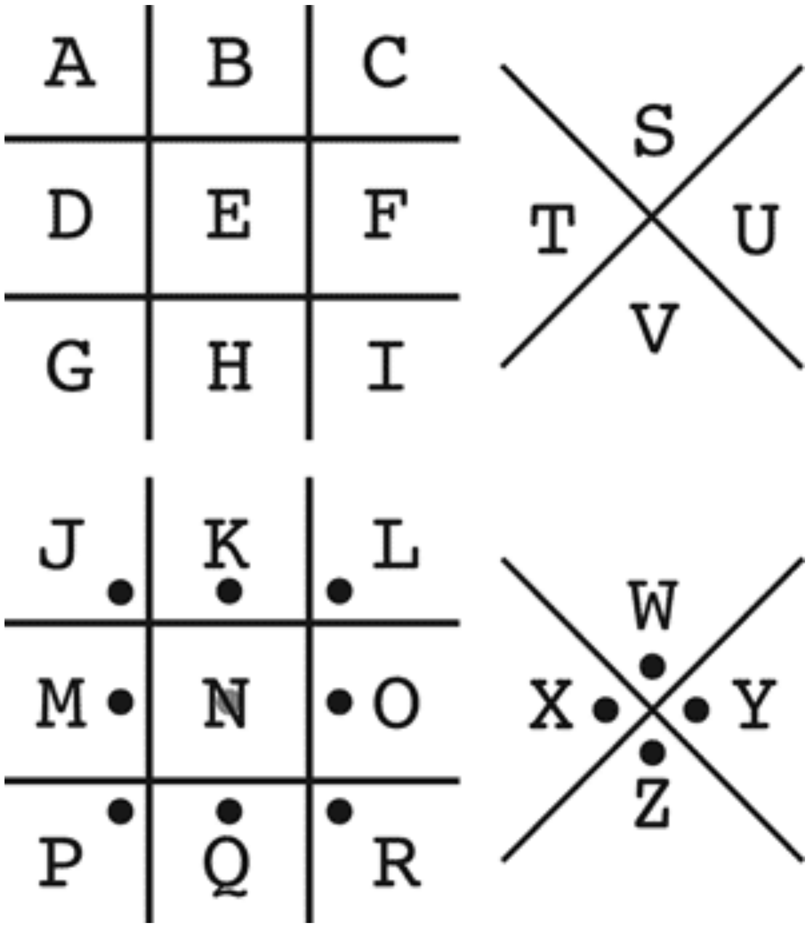
	1	2	3	4	5	6
1	a	i	o	u	é	è
2	an	in	on	un	eu	ou
3	b	d	g	j	v	z
4	p	t	q	ch	f	s
5	l	m	n	r	gn	ll
6	oi	oin	ian	ien	ion	ieu

Captain Charles Barbier de la Serre's Polybius Square was adapted for 'night writing' and later evolved into braille

© DAVID HAMER



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z


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

Solve The Following Cipher

SLAVERY IS A DISEASE, WHOSE SHADOW LIES ALWAYS UPON AMERICA'S THRESHOLD, ORIGINATING IN THE AVARICE AND CRUELTY OF THE SLAVE TRADE. I KNOW IT IS AN EVIL. COMMERCIAL GREED VALUES THE LIFE OF MEN NO MORE THAN IT VALUES THE LIVES OF ANTS.

To be Continued