Secret Codes
An Introduction

Deepak Kumar

Bryn Mawr College

Based on: The Code Book, Simon Singh, Anchor Books 1999.

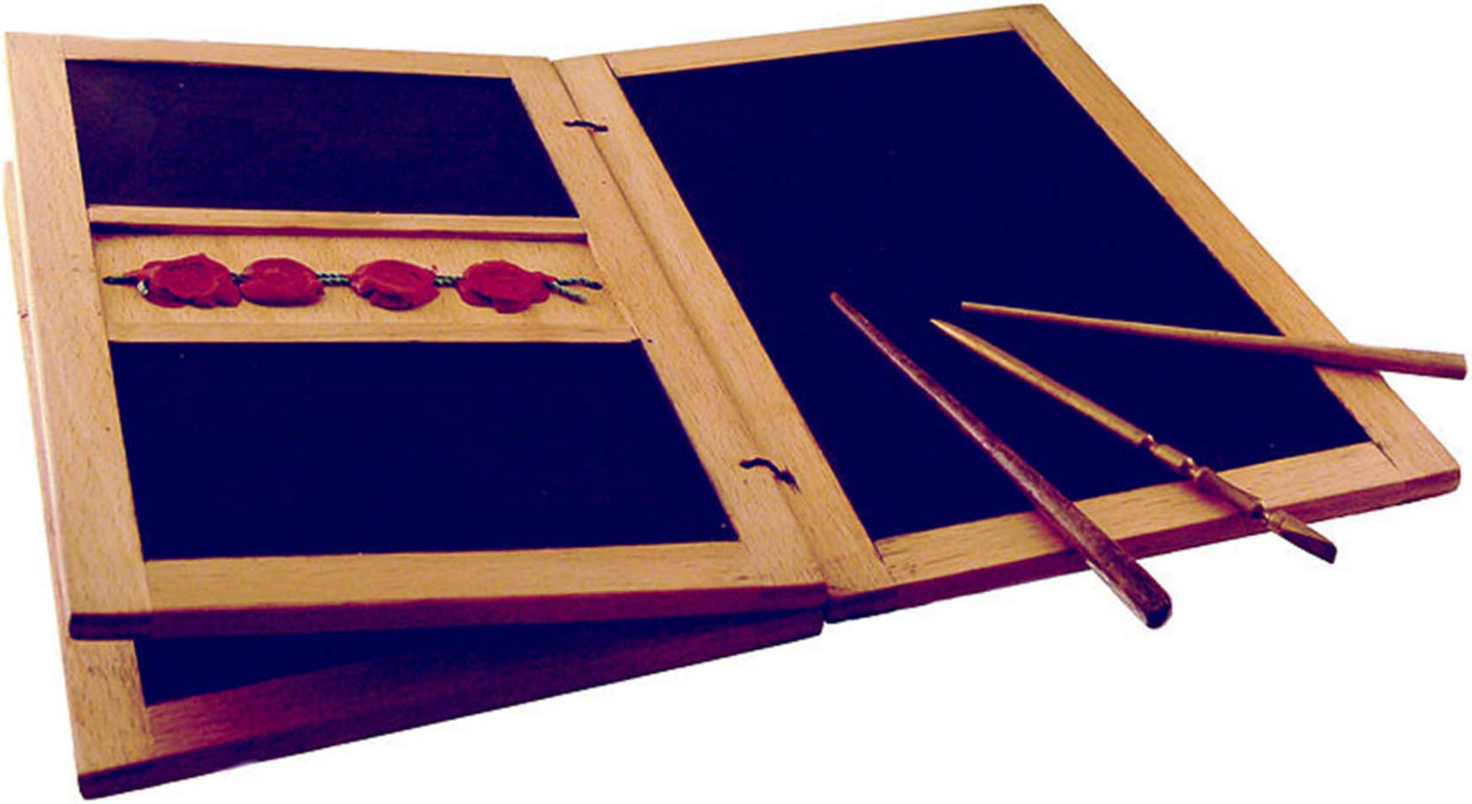
Secret Communication
Essential Elements

- Sender
- Receiver
- Messenger/Medium
- Message

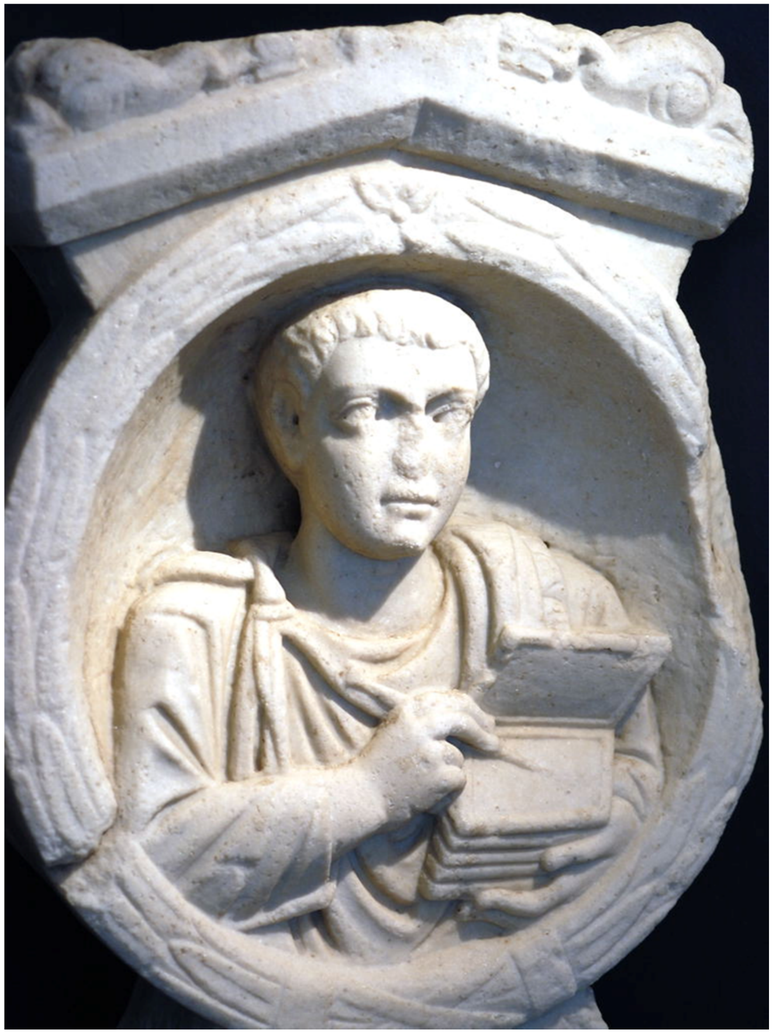
Steganography

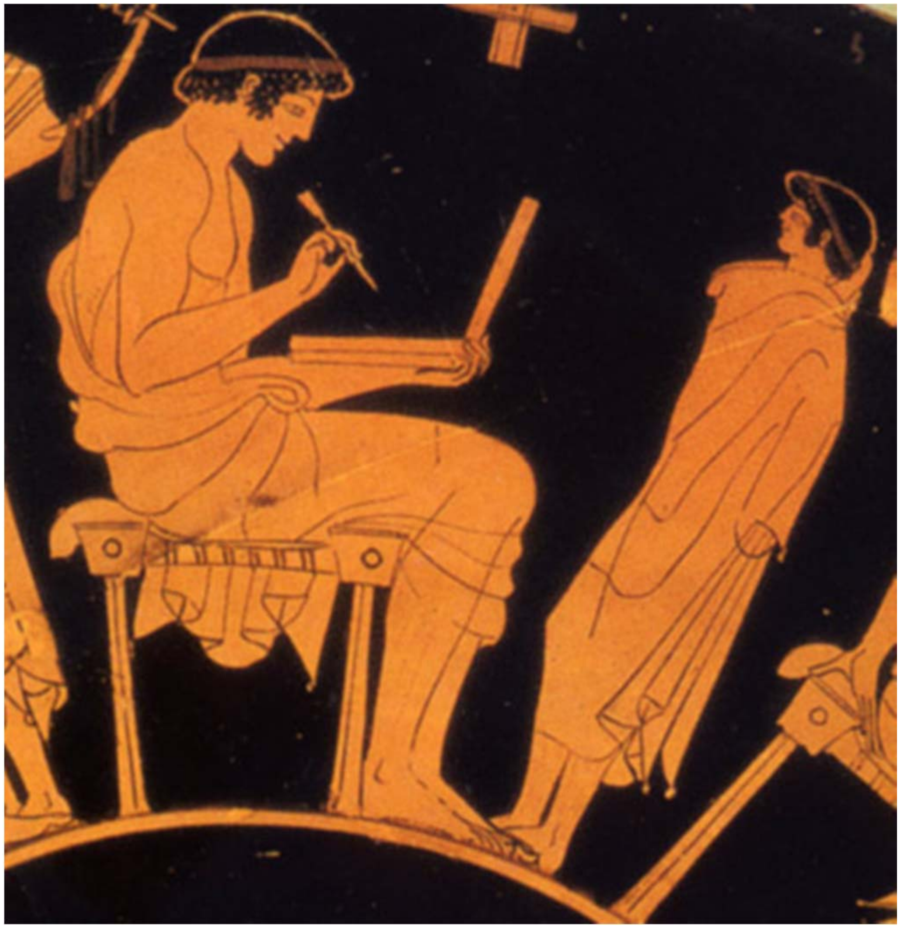
- “concealed writing” from the Greek words *steganos* (στεγανός) meaning "covered or protected", and *graphei* (γραφή) meaning "writing“
- Secret messages were hidden or memorized by runners.
- Demaratus tells Athens of Persia’splans for attack by writing message under the wax on a tablet (5th century B.C.)

Replica of a Wax Tablet



Tablets…





Other Means of Hiding messages

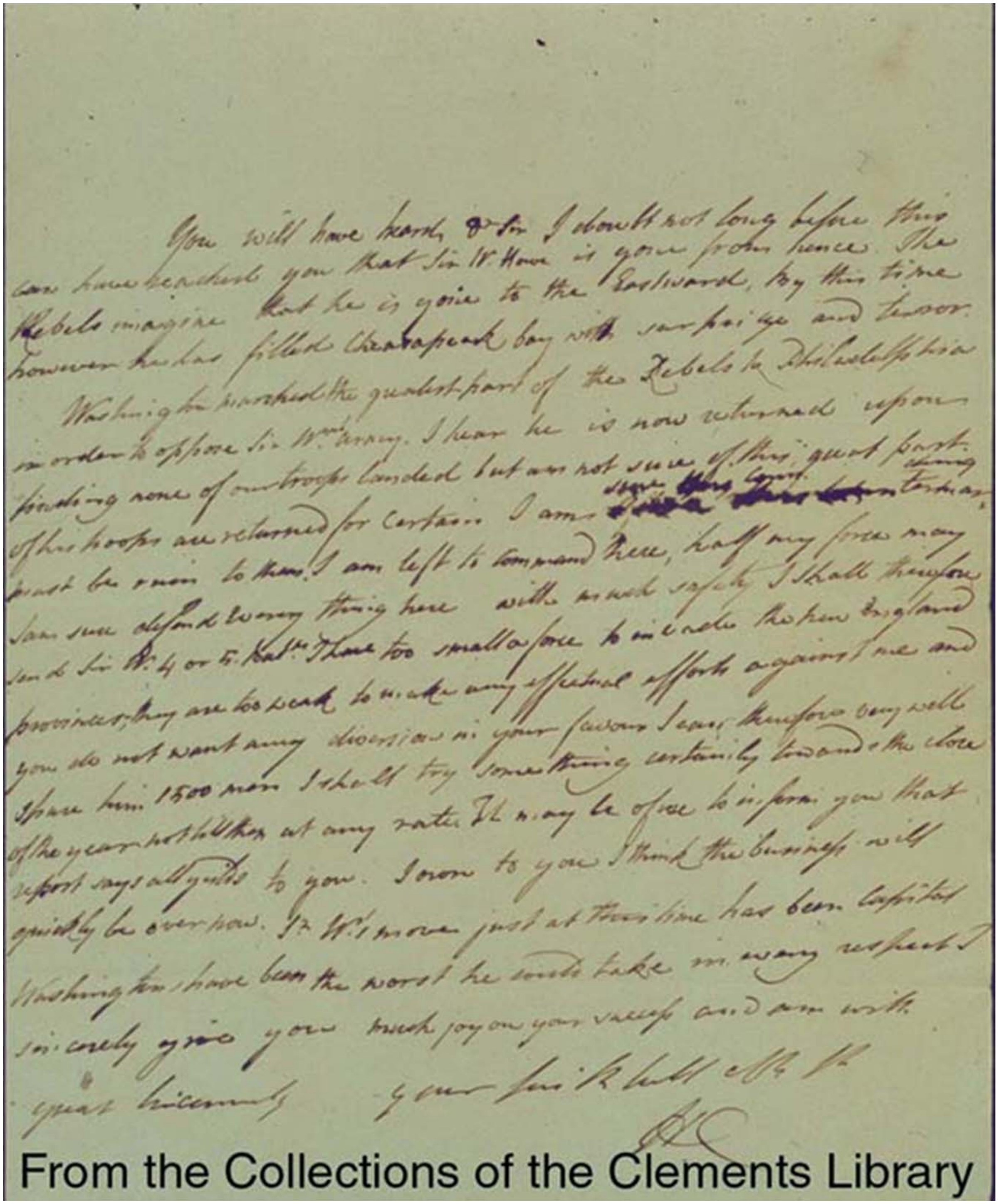
- Greek Histaiaeus encouraged Aristagoras of Miletus to revolt against the Persian King. Writes message on the shaved head of the messenger, and sends him after his hair grew.

- Ancient Chinese silk balls.

- Pliny the Elder's use of invisible ink (1st century A.D.).

- Giovanni Porta's secret message in a hard boiled egg (16th century).

- Writing inside writing. Masking.
  E.g. Spy Letters of the American revolution



You will have heard, Dr Sir I doubt not long before this
can have reached you that Sir W. Howe is gone from hence. The
Rebels imagine that he is gone to the Eastward, by this time
however he has filled Chesapeak bay with surprize and terror.
Washington marched the greatest part of the Rebels to Philadelphia
in order to oppose Sir Wm's army. I hear he is now returned upon
finding none of our troops landed but am not sure of this, great part
of his troops are returned for certain. I am ~~[illegible]~~ sure this count ~~[illegible]~~ termarching
must be ruin to them. I am left to command here, half my force may
I am sure defend every thing here with much safety. I shall therefore
send Sir W. 4 or 5 Batns. I have too small a force to invade the New England
provinces, they are too weak to make any effectual efforts against me and
you do not want any diversion in your favour. I can, therefore very well
spare him 1500 men. I shall try something certainly towards the close
of the year, not till then at any rate. It may be of use to inform you that
report says all yields to you. I own to you I think the business will
quickly be over now. Sr. W's move just at this time has been capital.
Washington's have been the worst he could take in every respect. I
sincerely give you much joy on your success and am with
great Sincerity your faithfull [illegible]

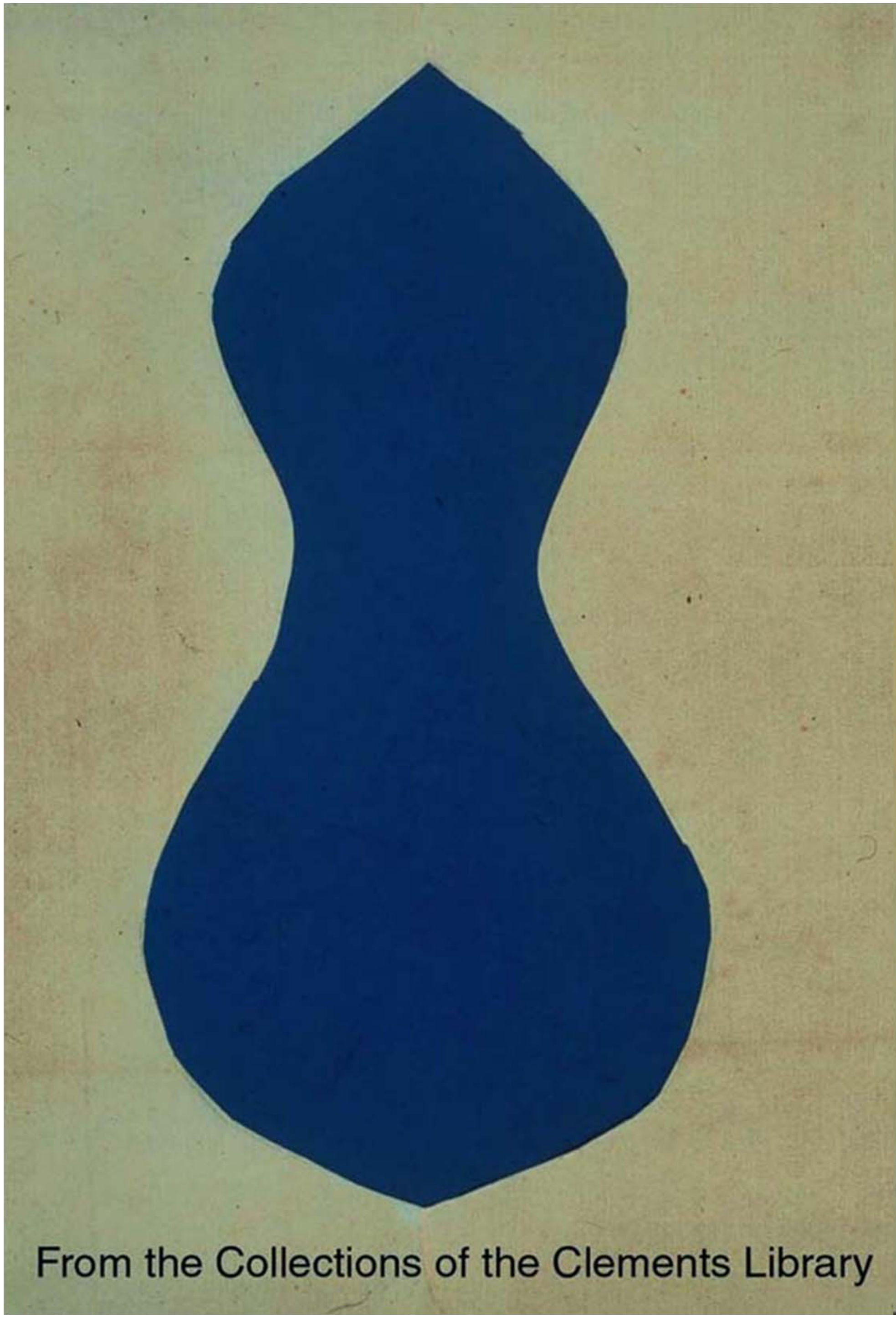
HC

From the Collections of the Clements Library

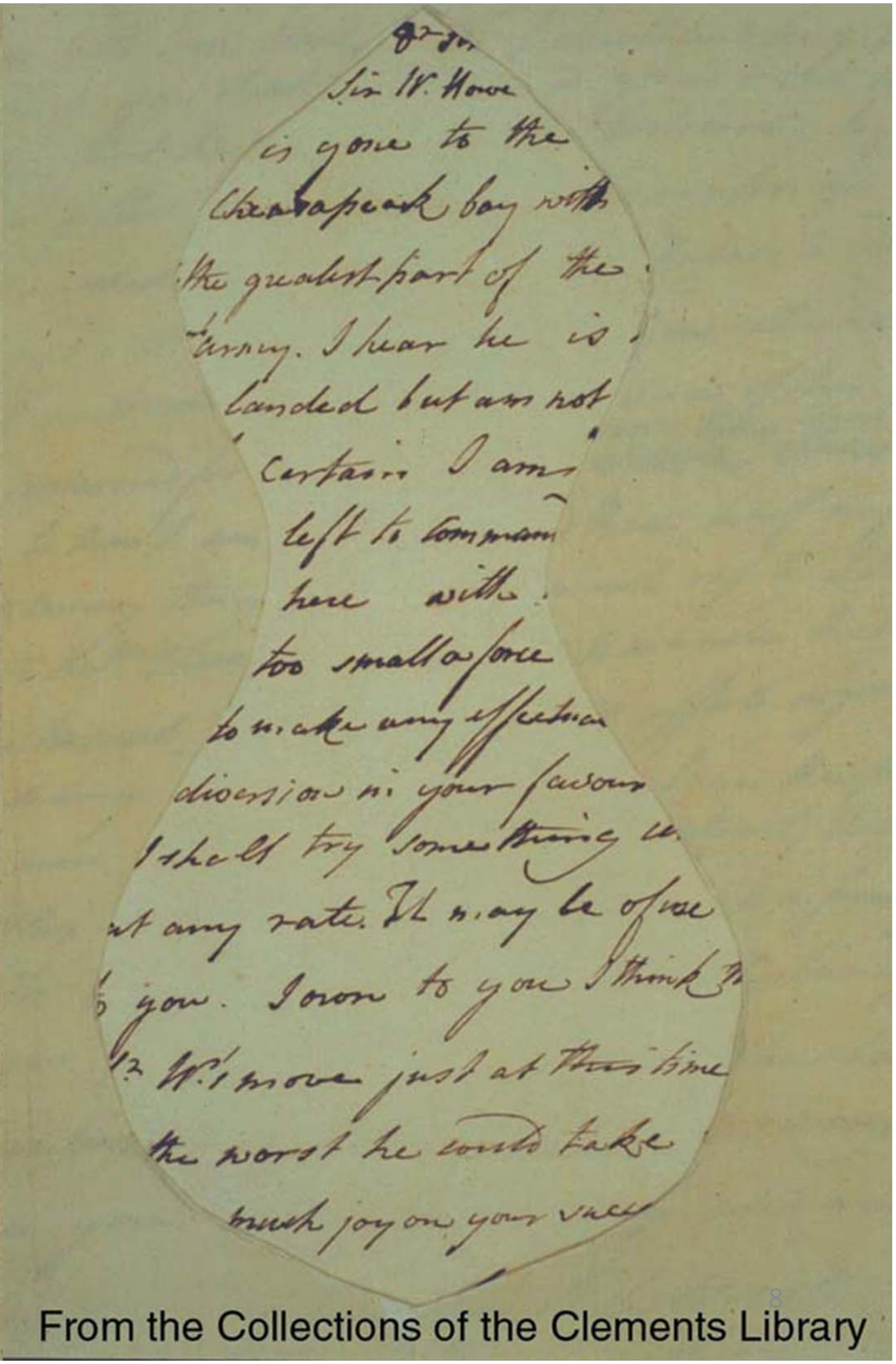
August 10, 1777 -- Henry Clinton to John Burgoyne
From the Gold Star Collection

You will have heard, Dr Sir I doubt not long before this / can have reached you that Sir W. Howe is gone from hence. The / Rebels imagine that he is gone to the Eastward. By this time / however he has filled Chesapeak bay with surprize and terror.

Washington marched the greater part of the Rebels to Philadelphia / in order to oppose Sir Wm's. army. I hear he is now returned upon / finding none of our troops landed but am not sure of this, great part / of his troops are returned for certain. I am sure this countermarching / must be ruin to them. I am left to command here, half of my force may / I am sure defend everything here with much safety. I shall therefore / send Sir W. 4 or 5 Bat [talio] ns. I have too small a force to invade the New England / provinces; they are too weak to make any effectual efforts against me and / you do not want any diversion in your favour. I can, therefore very well / spare him 1500 men. I shall try some thing certainly towards the close / of the year, not till then at any rate. It may be of use to inform you that / report says all yields to you. I own to you that I think the business will / quickly be over now. Sr. W's move just at this time has been capital. / Wahingtons have been the worst he could take in every respect. / sincerely give you much joy on your success and am with / great Sincerity your [ ] / HC

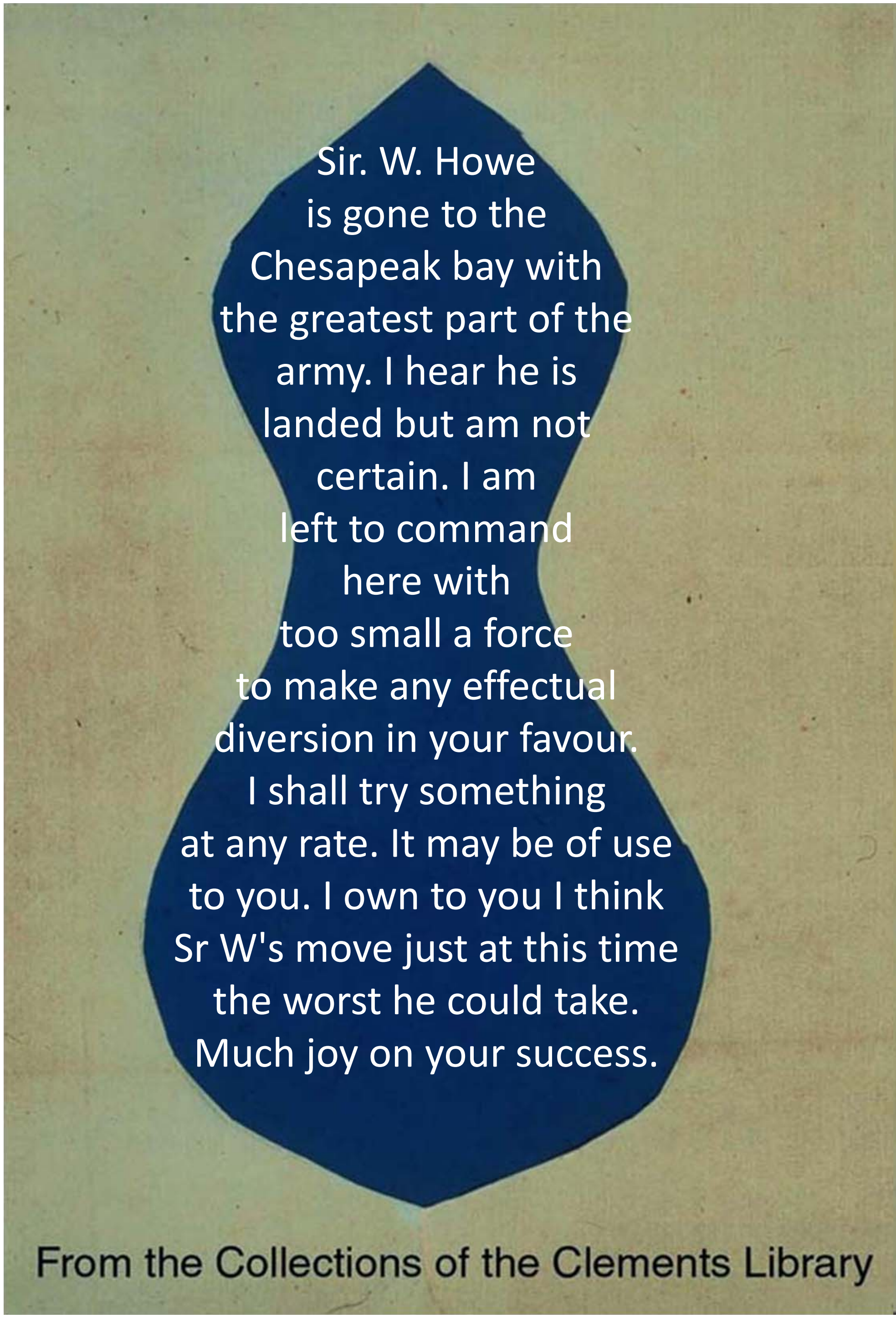


From the Collections of the Clements Library



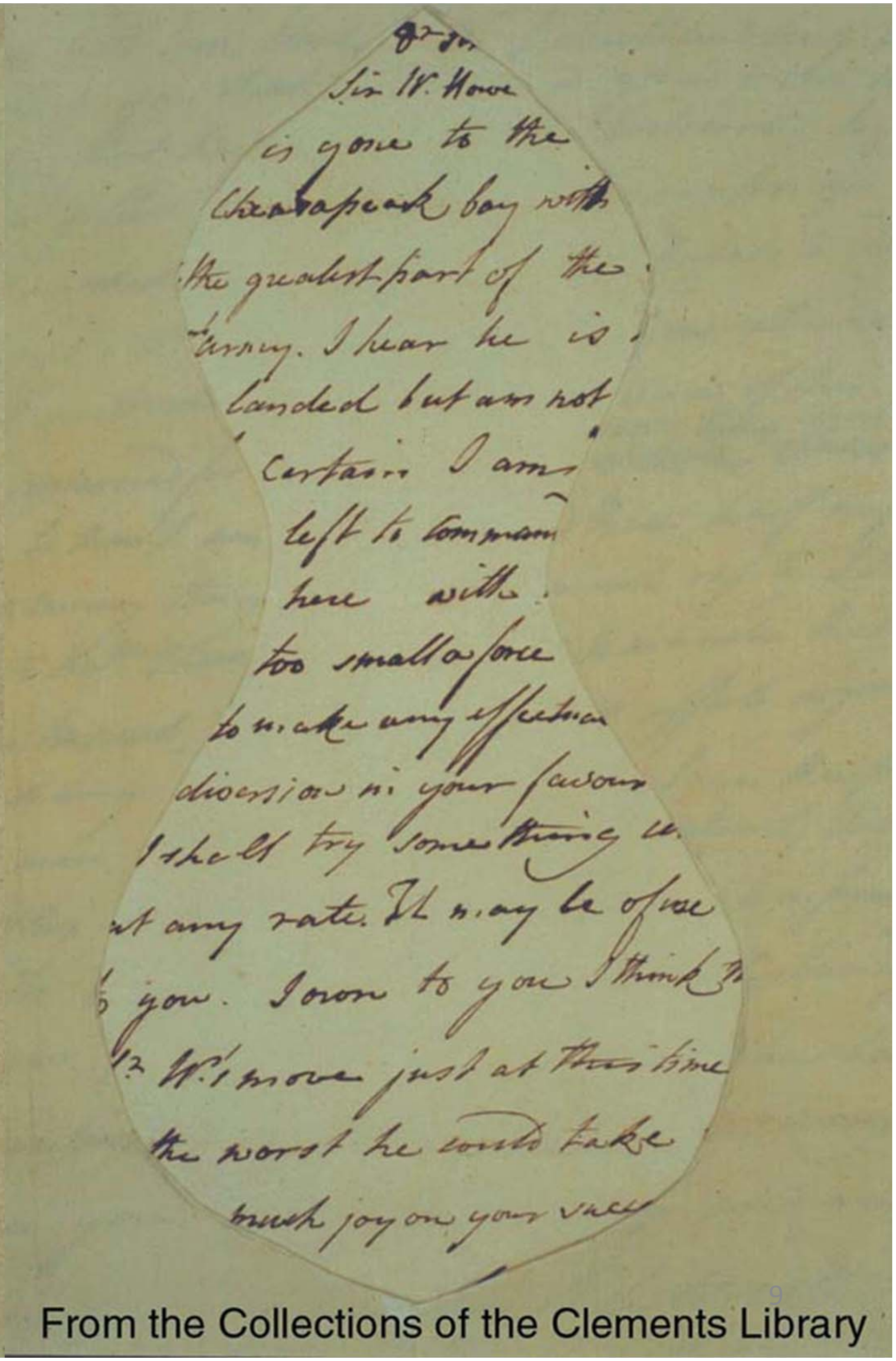
Dr Sir
Sir W. Howe
is gone to the
Cheasapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain I am
left to command
here with
too small a force
to make any effectual
diversion in your favour
I shall try something at
at any rate. It may be of use
to you. I own to you I think
Sr W's move just at this time
the worst he could take
much joy on your succ

From the Collections of the Clements Library



Sir. W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain. I am
left to command
here with
too small a force
to make any effectual
diversion in your favour.
I shall try something
at any rate. It may be of use
to you. I own to you I think
Sr W's move just at this time
the worst he could take.
Much joy on your success.

From the Collections of the Clements Library



Sir W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain I am
left to command
here with
too small a force
to make any effectua
diversion in your favour
I shall try something a
at any rate. It may be of use
you. I own to you I think th
r W's move just at this time
the worst he could take
much joy on your succ

From the Collections of the Clements Library

Cryptography

- from Greek κρυπτός, “hidden, secret”; and *graphei* (γραφή) meaning “writing”

- Involves hiding the *meaning* of the message using *encryption*.
    - Transposition
    - Substitution Cipher

Transposition

- Letters in the message are rearranged.
- No new letters are introduced.
- Encrypted message is an *anagram*.

Tom Marvolo Riddle

Mr. Mojo Risin’

Paul Sernine

Transposition

- Letters in the message are rearranged.
- No new letters are introduced.
- Encrypted message is an *anagram*.

Tom Marvolo Riddle I am Lord Voldemort

Mr. Mojo Risin’

Paul Sernine

Transposition

- Letters in the message are rearranged.
- No new letters are introduced.
- Encrypted message is an *anagram*.

Tom Marvolo Riddle	I am Lord Voldemort
Mr. Mojo Risin’	Jim Morrison
Paul Sernine	

Transposition

- Letters in the message are rearranged.
- No new letters are introduced.
- Encrypted message is an *anagram*.

Tom Marvolo Riddle	I am Lord Voldemort
Mr. Mojo Risin’	Jim Morrison
Paul Sernine	Arsene Lupin

How many transpositions??

- Given a message with N letters

- There are N! transpositions

  tom
  TOM, TMO, MOT, MTO, OMT, OTM
  3! = 3x2x1 = 6

  Lord Voldemort
  has 13! = 6,227,020,800 transpositions!

Transposition: Two Rails

```
BRYN MAWR COLLEGE
```

```
B   Y   M   W   C   L   E   E
  R   N   A   R   O   L   G
```

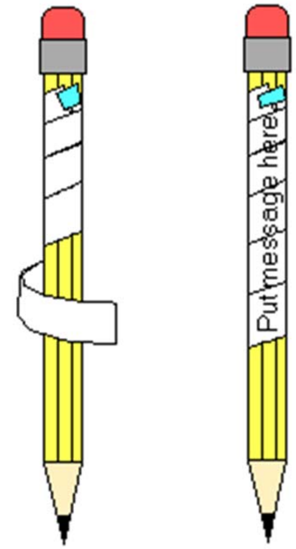
Transposition: Two Rails

BRYN MAWR COLLEGE

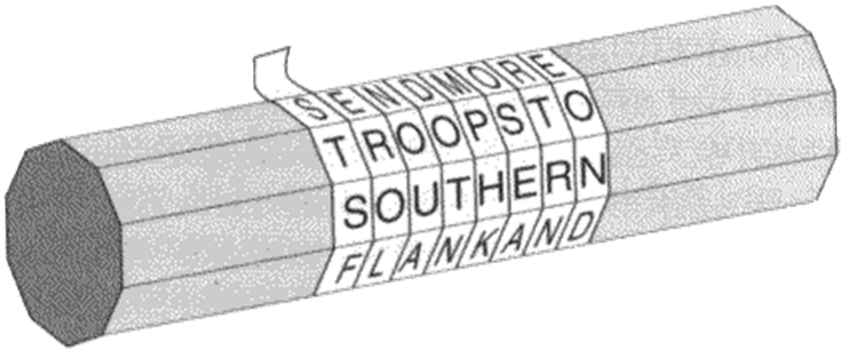
```
B   Y   M   W   C   L   E   E
  R   N   A   R   O   L   G
```

BYMWCLEERNAROLG

Transposition: Scytale (404 B.C.)



KILLKING
TOMORROW
MIDNIGHT



Cryptography

- from Greek κρυπτός, “hidden, secret”; and *graphei* (γραφή) meaning “writing”

- Involves hiding the *meaning* of the message using *encryption*.
  - Transposition
  - Substitution Cipher

Substitution Ciphers

- **Plain alphabet**
  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

- **Cipher alphabet**
  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

- **Monoalphabetic Substitution Cipher**:
  When the cipher alphabet consists of letters (or symbols), or a mix of both.

Substitution Ciphers

- **Caesar Cipher**

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	A	B	C

bryn mawr college
EUBQ PDZU FROOHJH

- **Random Pairing**

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

bryn mawr college
HLPC CVFL MQRRUIU

Substitution Ciphers

- **Atbash (Hebrew)**

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

bryn mawr college
YIBM NZDI XLOOVTV

- **ROT13**

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

bryn mawr college
OELA ZNJR PBYYRTR

Substitution Ciphers

- **Caesar Cipher**

Only 25 distinct ciphers possible.

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	A	B	C

bryn mawr college
EUBQ PDZU FROOHJH

- **Random Pairing**

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

25! = over 400 Septillion (10^{24}) distinct ciphers possible!

bryn mawr college
HLPC CVFL MQRRUIU

Substitution Ciphers

- **Using Keyphrase/Keyword**
  From: BARACK OBAMA
  You get: BARCKOM

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

bryn mawr college
AYIU TBGY RVSSKMK

Substitution Ciphers

- **Using Keyphrase/Keyword**

  From: BARACK OBAMA

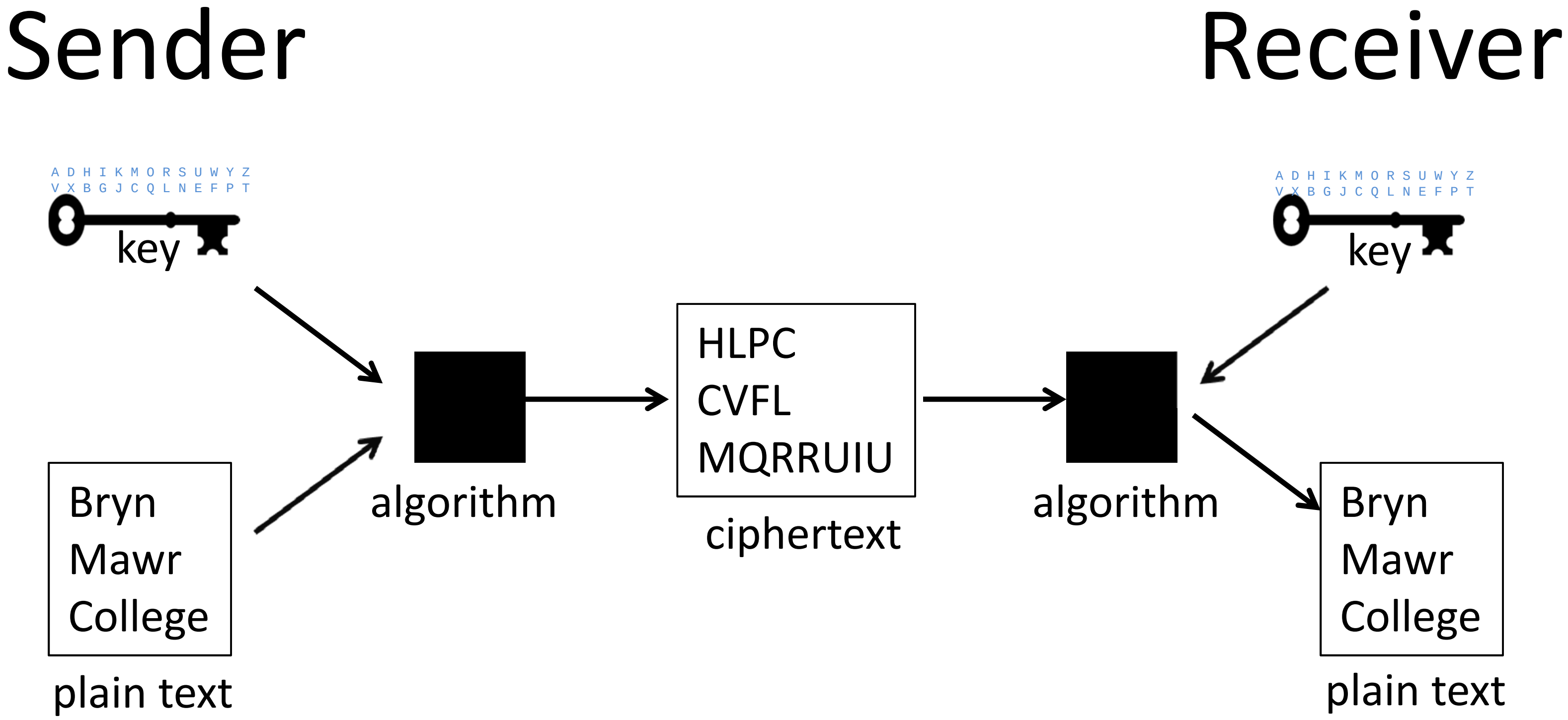
  You get: BARCKOM

Fewer than 25! Ciphers.
But still quite large.
Easier to remember the key.

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

bryn mawr college
AYIU TBGY RVSSKMK

Cryptography: Basic Terminology



Sender

Receiver

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

Bryn Mawr College

plain text

algorithm

HLPC CVFL MQRRUIU

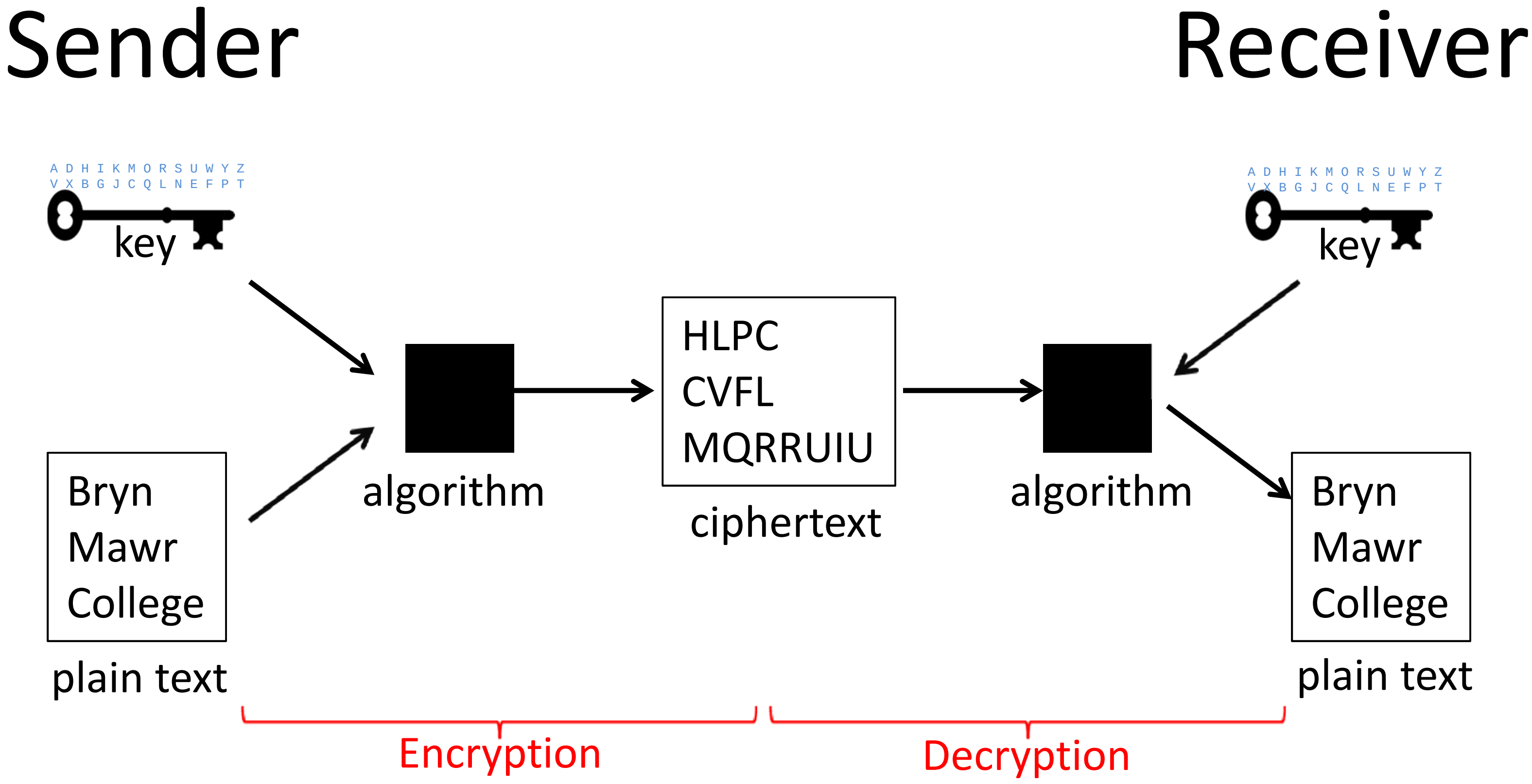
ciphertext

algorithm

Bryn Mawr College

plain text

Cryptography: Basic Terminology



Sender

Receiver

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

key

algorithm

HLPC
CVFL
MQRRUIU

ciphertext

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

key

algorithm

Bryn
Mawr
College

plain text

Bryn
Mawr
College

plain text

Encryption

Decryption

Cryptanalysis

- The science (and art?) of unscrambling a message without knowledge of the key.

- **Frequency Analysis:** Pioneered by al Kindi in 9th century C.E. at Bait al-Hikmah (House of Wisdom) in Baghdad.

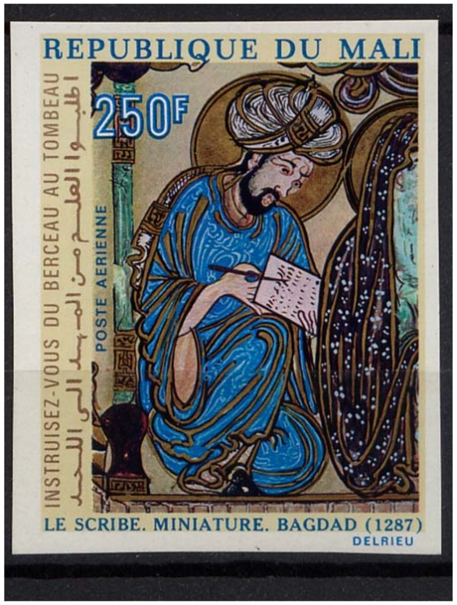
- Still widely used…

al Kindi

SYRIA
الجمهورية العربية السورية
1150 YRS COMMEMORATION OF THE ARAB PHILOS. AL KINDI
10 ليرة
1994
POSTAGE

AR EGYPT
POSTAGE
1975
جمهورية مصر العربية
١٣٩٥
بريد
20M
الكندى
٨٠١-٨٦٥
٢٠م
L. EL SAWAF
P.P.H. CAIRO

الجمهورية العراقية
REPUBLIC OF IRAQ
POSTAGE
6
FILS
١٩٦٢م ١٣٨٢هـ
بريد
٦
فلوس


REPUBLIQUE DU MALI
250F
POSTE AERIENNE
INSTRUISEZ-VOUS DU BERCEAU AU TOMBEAU
LE SCRIBE. MINIATURE. BAGDAD (1287)
DELRIEU

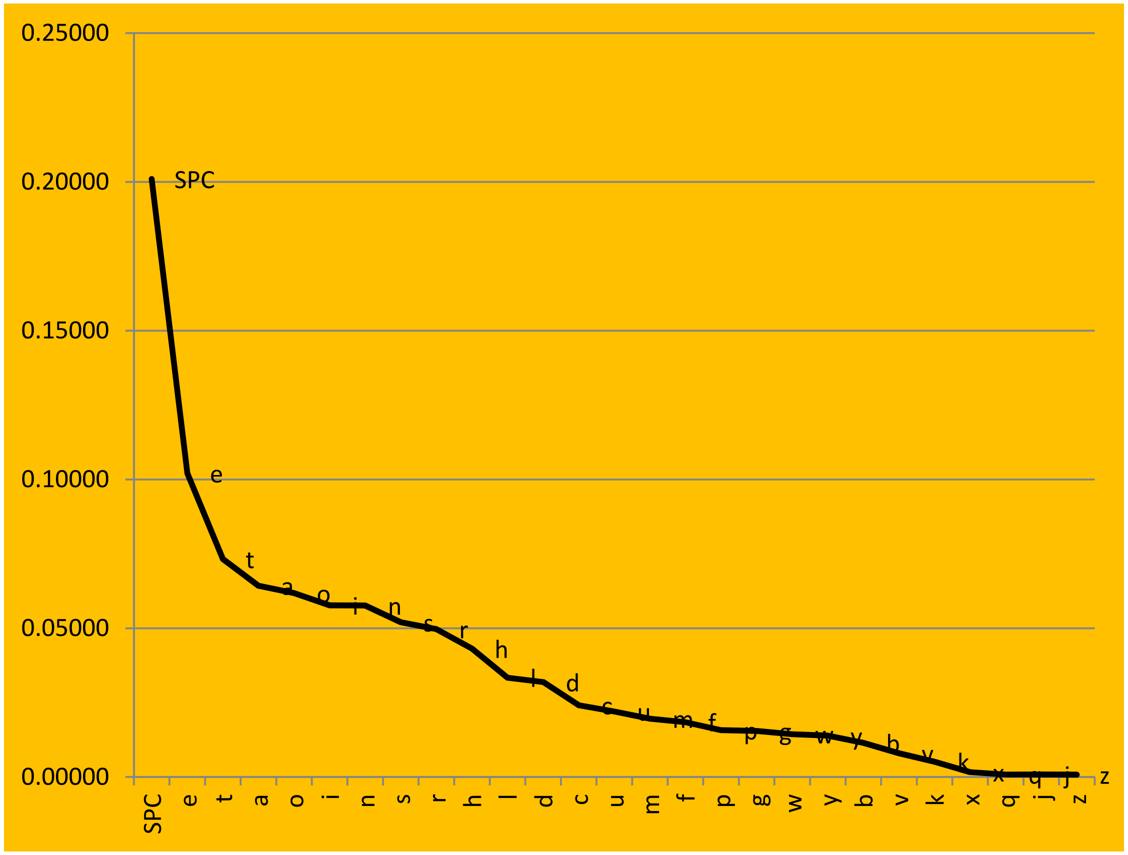
الجمهورية العربية السورية
SYRIA
THE 6TH CONFERENCE OF THE ARAB MINISTERS OF CULTURE
1987
POSTAGE
بريد
330

4 B.
AIR MAIL THE MUTAWAKELITE KINGDOM OF YEMEN
المملكة المتوكلية اليمنية
THE SCRIBE

From: Mathematicians on Stamps: http://jeff560.tripod.com/stamps.html

Text Analysis

a	0.06428
b	0.01147
c	0.02413
d	0.03188
e	0.10210
f	0.01842
g	0.01543
h	0.04313
i	0.05767
j	0.00082
k	0.00514
l	0.03338
m	0.01959
n	0.05761
o	0.06179
p	0.01571
q	0.00084
r	0.04973
s	0.05199
t	0.07327
u	0.02201
v	0.00800
w	0.01439
x	0.00162
y	0.01387
z	0.00077
SPC	0.20096



Cryptanalyzing Text

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X
LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM
LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK.
SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Ciphertext Frequency Analysis

Letter	Frequency		Letter	Frequency	
	Occurences	Percentage		Occurrences	Percentage
A	3	0.9	N	3	0.9
B	25	7.4	O	38	11.2
C	27	8.0	P	31	9.2
D	14	4.1	Q	2	0.6
E	5	1.5	R	6	1.8
F	2	0.6	S	7	2.1
G	1	0.3	T	0	0.0
H	0	0.0	U	6	1.8
I	11	3.3	V	18	5.3
J	18	5.3	W	1	0.3
K	26	7.7	X	34	10.1
L	25	7.4	Y	19	5.6
M	11	3.3	Z	5	1.5

Counting D’s

PCQ VMJYP**D** LBYK LYSO KBXBJXWXV BXV ZCJPO EYP**D** KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PY**D**BL, QBOP KBO BXV OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV EYKKOV LBO **D**JCMPV ZOICJO BYS, KXUYP**D**: “**D**JOXL EYP**D**, ICJ X LBCMKXPV XPV CPO PY**D**BLK Y BXNO ZOOP JOACMPLYP**D** LC UCM LBO IXZROK CI FXKL X**D**OK XPV LBO RO**D**OPVK CI XPAYOPL EYP**D**K. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

OFYRC**D**MO, LXROK IJCS LBO LBCMKXPV XPV CPO PY**D**BLK

Ciphertext Frequency Analysis

Letter	Frequency		Letter	Frequency	
	Occurences	Percentage		Occurrences	Percentage
A	3	0.9	N	3	0.9
B	25	7.4	O	38	11.2
C	27	8.0	P	31	9.2
D	14	4.1	Q	2	0.6
E	5	1.5	R	6	1.8
F	2	0.6	S	7	2.1
G	1	0.3	T	0	0.0
H	0	0.0	U	6	1.8
I	11	3.3	V	18	5.3
J	18	5.3	W	1	0.3
K	26	7.7	X	34	10.1
L	25	7.4	Y	19	5.6
M	11	3.3	Z	5	1.5

O=e,t or a, X=e,t or a, P=e,t or a

Letter	Frequency		Letter	Frequency	
	Occurences	Percentage		Occurrences	Percentage
A	3	0.9	N	3	0.9
B	25	7.4	O	38	11.2
C	27	8.0	P	31	9.2
D	14	4.1	Q	2	0.6
E	5	1.5	R	6	1.8
F	2	0.6	S	7	2.1
G	1	0.3	T	0	0.0
H	0	0.0	U	6	1.8
I	11	3.3	V	18	5.3
J	18	5.3	W	1	0.3
K	26	7.7	X	34	10.1
L	25	7.4	Y	19	5.6
M	11	3.3	Z	5	1.5

Identifying Vowels (O, X, or P?)

	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
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

PCQ VMJYPD LBYK LYS**O** KBXBJXWXV BXV ZCJP**O** EYPD
KBXBJYUXJ LBJ**OO** KCPK. CP LB**O** LBCMKXPV XPV IYJKL PYDBL,
QB**O**P KB**O** BXV **O**PV**O**V LB**O** LXR**O** CI SX’XJMI, KB**O** JCK**O** XPV
EYKK**O**V LB**O** DJCMPV Z**O**ICJ**O** BYS, KXUYPD: “DJ**O**XL EYPD, ICJ X
LBCMKXPV XPV CP**O** PYDBLK Y BXN**O** Z**OO**P J**O**ACMPLYPD LC UCM
LB**O** IXZR**O**K CI FXKL XD**O**K XPV LB**O** R**O**D**O**PVK CI XPAY**O**PL EYPDK.
SXU Y SXE**O** KC ZCRV XK LC AJXN**O** X IXNCMJ CI UCMJ SXG**O**KLU?

OFYRCDM**O**, LXR**O**K IJCS LB**O** LBCMKXPV XPV CP**O** PYDBLK

Identifying Vowels (O, X, or P?)

	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
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

- O and X appear next to most other letters, except 7 or 8 of them).
- P does not appear next to 15 letters.
- Therefore, O and X are vowels (either e or a). P is a consonant!

But is O = e or a? X = e or a?
Take another look at ciphertext…

O = e or a? X = e or a?

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJ**OO** KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X
LBCMKXPV XPV CPO PYDBLK Y BXNO Z**OO**P JOACMPLYPD LC UCM
LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK.
SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

- OO appears twice, but XX never appears.
- In normal text, likely to see ee than aa
- Further, X appears by itself
- Therefore, perhaps X = a and O = e.
- And, since Y appears by itself, it must be that Y = i

Since O = e
Spotting the letter h (the, they, …)

	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
after O	1	**0**	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
before O	0	**9**	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

PCQ VMJYPD LBYK LYS**O** KBXBJXWXV BXV ZCJP**O** EYPD
KBXBJYUXJ LBJ**OO** KCPK. CP LB**O** LBCMKXPV XPV IYJKL PYDBL,
QB**O**P KB**O** BXV **O**PV**O**V LB**O** LXR**O** CI SX’XJMI, KB**O** JCK**O** XPV
EYKK**O**V LB**O** DJCMPV Z**O**ICJ**O** BYS, KXUYPD: “DJ**O**XL EYPD, ICJ X
LBCMKXPV XPV CP**O** PYDBLK Y BXN**O** Z**OO**P J**O**ACMPLYPD LC UCM
LB**O** IXZR**O**K CI FXKL XD**O**K XPV LB**O** R**O**D**O**PVK CI XPAY**O**PL EYPDK.
SXU Y SXE**O** KC ZCRV XK LC AJXN**O** X IXNCMJ CI UCMJ SXG**O**KLU?”

OFYRCDM**O**, LXR**O**K IJCS LB**O** LBCMKXPV XPV CP**O** PYDBLK

Since O = e
Spotting the letter h (the, they, …)

	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
after O	1	**0**	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
before O	0	**9**	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPO: “DJOXL EYPD, ICJ X
LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM
LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK.
SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

Therefore, B = h

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Since O = e, X = a, Y = I, B = h

PCQ VMJ**i**PD L**hi**K L**Y**S**e** K**hah**J**a**W**a**V **ha**V ZCJP**e** E**i**PD
K**hah**J**i**U**a**J L**h**J**ee** KCPK. CP L**he** L**h**CMK**a**PV **a**PV I**i**JKL P**i**D**h**L,
Q**he**P K**he** **ha**V **e**PV**e**V L**he** L**a**R**e** CI S**a**’**a**JMI, K**he** JCK**e** **a**PV
E**i**KK**e**V L**he** DJCMPV Z**e**ICJ**e** **hi**S, K**a**U**i**PD: “DJ**ea**L E**i**PD, ICJ **a**
L**h**CMK**a**PV **a**PV CP**e** P**i**D**h**LK **i** **ha**N**e** Z**ee**P J**e**ACMPL**i**PD LC UCM
L**he** I**a**ZR**e**K CI F**a**KL **a**D**e**K **a**PV L**he** R**e**D**e**PVK CI **a**PA**ie**PL E**i**PDK.
S**a**U **i** S**a**E**e** KC ZCRV **a**K LC AJ**a**N**e** **a** I**a**NCMJ CI UCMJ S**a**G**e**KLU?”

eF**i**RCDM**e**, L**a**R**e**K IJCS L**he** L**h**CMK**a**PV **a**PV CP**e** P**i**D**h**LK

This makes up for over 1/3rd of all characters already!

Since O = e, X = a, Y = I, B = h
Further, look for ‘and’ and ‘the’

PCQ VMJ**i**PD L**hi**K L**i**S**e** K**hah**J**a**W**a**V **ha**V ZCJP**e** E**i**PD
K**hah**J**i**U**a**J L**h**J**ee** KCPK. CP L**he** L**h**CMK**a**PV **a**PV I**i**JKL P**i**D**h**L,
Q**he**P K**he** **ha**V **e**PV**e**V L**he** L**a**R**e** CI S**a**’**a**JMI, K**he** JCK**e** **a**PV
E**i**KK**e**V L**he** DJCMPV Z**e**ICJ**e** **hi**S, K**a**U**i**PD: “DJ**ea**L E**i**PD, ICJ **a**
L**h**CMK**a**PV **a**PV CP**e** P**i**D**h**LK **i** **ha**N**e** Z**ee**P J**e**ACMPL**i**PD LC UCM
L**he** I**a**ZR**e**K CI F**a**KL **a**D**e**K **a**PV L**he** R**e**D**e**PVK CI **a**PA**ie**PL E**i**PDK.
S**a**U **i** S**a**E**e** KC ZCRV **a**K LC AJ**a**N**e** **a** I**a**NCMJ CI UCMJ S**a**G**e**KLU?”

eF**i**RCDM**e**, L**a**R**e**K IJCS L**he** L**h**CMK**a**PV **a**PV CP**e** P**i**D**h**LK

Perhaps, L=t, P=n, V=d

O = e, X = a, Y = I, B = h,
L=t, P=n, V=d

nCQ **d**MJ**in**D **thi**K **ti**S**e** K**hah**J**a**W**ad** **had** ZCJ**ne** E**in**D
K**hah**J**i**U**a**J **th**J**ee** KC**n**K. C**n** **the** **th**CMK**and** **and** I**i**JK**t** **ni**D**ht**,
Q**hen** K**he** **had** **ended** **the** **ta**R**e** CI S**a**’**a**JMI, K**he** JCK**e** **and**
E**i**KK**ed** **the** DJCM**nd** Z**e**ICJ**e** **hi**S, K**a**U**in**D: “DJ**eat** E**in**D, ICJ **a**
thCMK**and** **and** C**ne** **ni**D**ht**K **i** **ha**N**e** Z**een** J**e**ACM**ntin**D **t**C UCM
the I**a**ZR**e**K CI F**a**K**t** **a**D**e**K **and** **the** R**e**D**end**K CI **an**A**ient** E**in**DK.
S**a**U **i** S**a**E**e** KC ZCR**d** **a**K **t**C AJ**a**N**e** **a** I**a**NCMJ CI UCMJ S**a**G**e**K**t**U?”

eF**i**RCDM**e**, **ta**R**e**K IJCS **the** **th**CMK**and** **and** C**ne** **ni**D**ht**K

O = e, X = a, Y = I, B = h,
L=t, P=n, V=d

nCQ **d**MJ**in**D **thi**K **ti**Se K**hah**J**a**W**ad** **had** ZCJ**ne** E**in**D
K**hah**J**i**U**a**J **th**J**ee** KC**n**K. C**n** **the** **th**CMK**and** **and** I**i**JK**t** **ni**D**ht**,
Q**hen** K**he** **had** **ended** **the** **ta**R**e** CI S**a**’**a**JMI, K**he** JCK**e** **and**
E**i**KK**ed** **the** DJCM**nd** Z**e**ICJ**e** **hi**S, K**a**U**in**D: “DJ**eat** E**in**D, ICJ **a**
thCMK**and** **and** C**ne** **ni**D**ht**K **i** **ha**N**e** Z**een** J**e**ACM**ntin**D **t**C UCM
the I**a**ZR**e**K CI F**a**K**t** **a**D**e**K **and** **the** R**e**D**end**K CI **an**A**ient** E**in**DK.
S**a**U **i** S**a**E**e** KC ZCR**d** **a**K **t**C AJ**a**N**e** **a** I**a**NCMJ CI UCMJ S**a**G**e**K**t**U?”

eF**i**RCDM**e**, **ta**R**e**K IJCS **the** **th**CMK**and** **and** C**ne** **ni**D**ht**K

Next, C=o, K=s, I=f

O = e, X = a, Y = l, B = h,
L=t, P=n, V=d, C=o, K=s, I=f

noQ dMJinD this tiSe shahJaWad had ZoJne EinD
shahJiUaJ thJee sons. on the thoMsand and fiJst niDht,
Qhen she had ended the taRe of Sa’aJMf, she Jose and
Eissed the DJoMnd ZefoJe hiS, saUinD: “DJeat EinD, foJ a
thoMsand and one niDhts i haNe Zeen JeAoMntinD to UoM
the faZRes of Fast aDes and the ReDends of anAient EinDs.
SaU i SaEe so ZoRd as to AJaNe a faNoMJ of UoMJ SaGestU?”

eFiRoDMe, taRes fJoS the thoMsand and one niDhts

Next, M=u, J=r, D=g, R=l, S=m

Plain Text	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
Cipher Text	X	-	-	V	O	I	D	B	Y	-	-	R	S	P	C	-	-	J	K	L	M	-	-	-	-	-

noQ during this time shahraWad had Zorne Eing
shahriUar three sons. on the thousand and first night,
Qhen she had ended the tale of ma’aruf, she rose and
Eissed the ground Zefore him, saUing: “great Eing, for a
thousand and one nights i haNe Zeen reAounting to Uou
the faZles of Fast ages and the legends of anAient Eings.
maU i maEe so Zold as to AraNe a faNour of UouJ maGestU?

eFilogue, tales from the thousand and one nights

Plain Text	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
Cipher Text	X	-	-	V	O	I	D	B	Y	-	-	R	S	P	C	-	-	J	K	L	M	-	-	-	-	-

Key Phrase: A VOID BY GEORGES PEREC = AVOIDBYGERSPC

noQ during this time shahraWad had Zorne Eing
shahriUar three sons. on the thousand and first night,
Qhen she had ended the tale of ma’aruf, she rose and
Eissed the ground Zefore him, saUing: “great Eing, for a
thousand and one nights i haNe Zeen reAounting to Uou
the faZles of Fast ages and the legends of anAient Eings.
maU i maEe so Zold as to AraNe a faNour of UouJ maGestU?

eFilogue, tales from the thousand and one nights

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

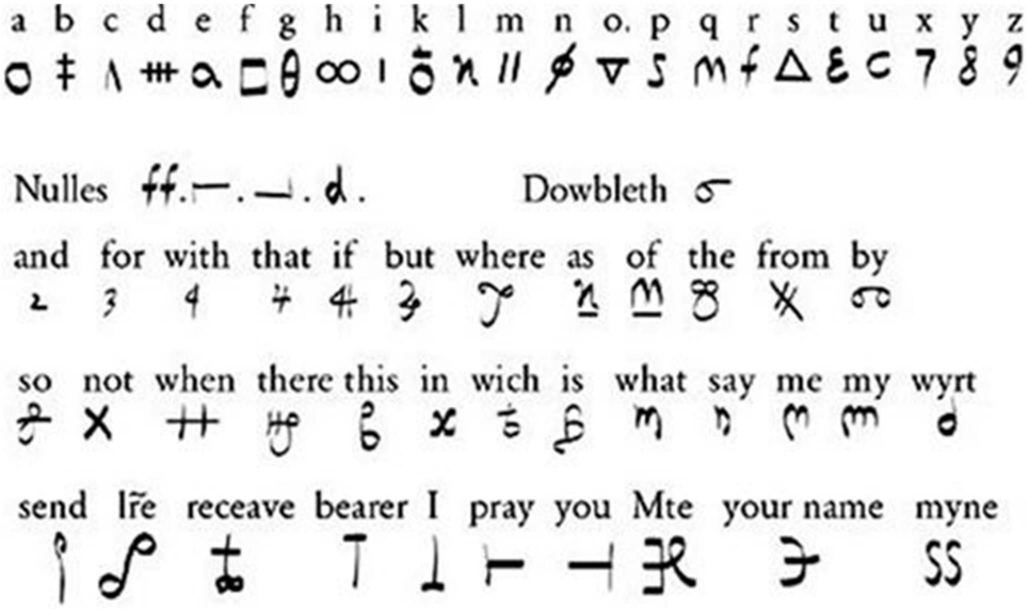
Plain Text	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**I**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Cipher Text	**X**	**Z**	**A**	**V**	**O**	**I**	**D**	**B**	**Y**	**G**	**E**	**R**	**S**	**P**	**C**	**F**	**H**	**J**	**K**	**L**	**M**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

Key Phrase: A VOID BY GEORGES PEREC = AVOIDBYGERSPC

now during this time shahrazad had borne king shahriyar three sons. on the thousand and first night, when she had ended the tale of ma'aruf, she rose and kissed the ground before him, saying: "great king, for a thousand and one nights i have been recounting to you the fables of past ages and the legends of ancient kings. may i make so bold as to crave a favour of your majesty?"

epilogue, tales from the thousand and one nights

Nomenclators: Symbols + Codes


a b c d e f g h i k l m n o. p q r s t u x y z
7 8 9
Nulles
Dowbleth
and for with that if but where as of the from by
2 3 4 4 4
so not when there this in wich is what say me my wyrt
send lr̃e receave bearer I pray you Mte your name myne
SS

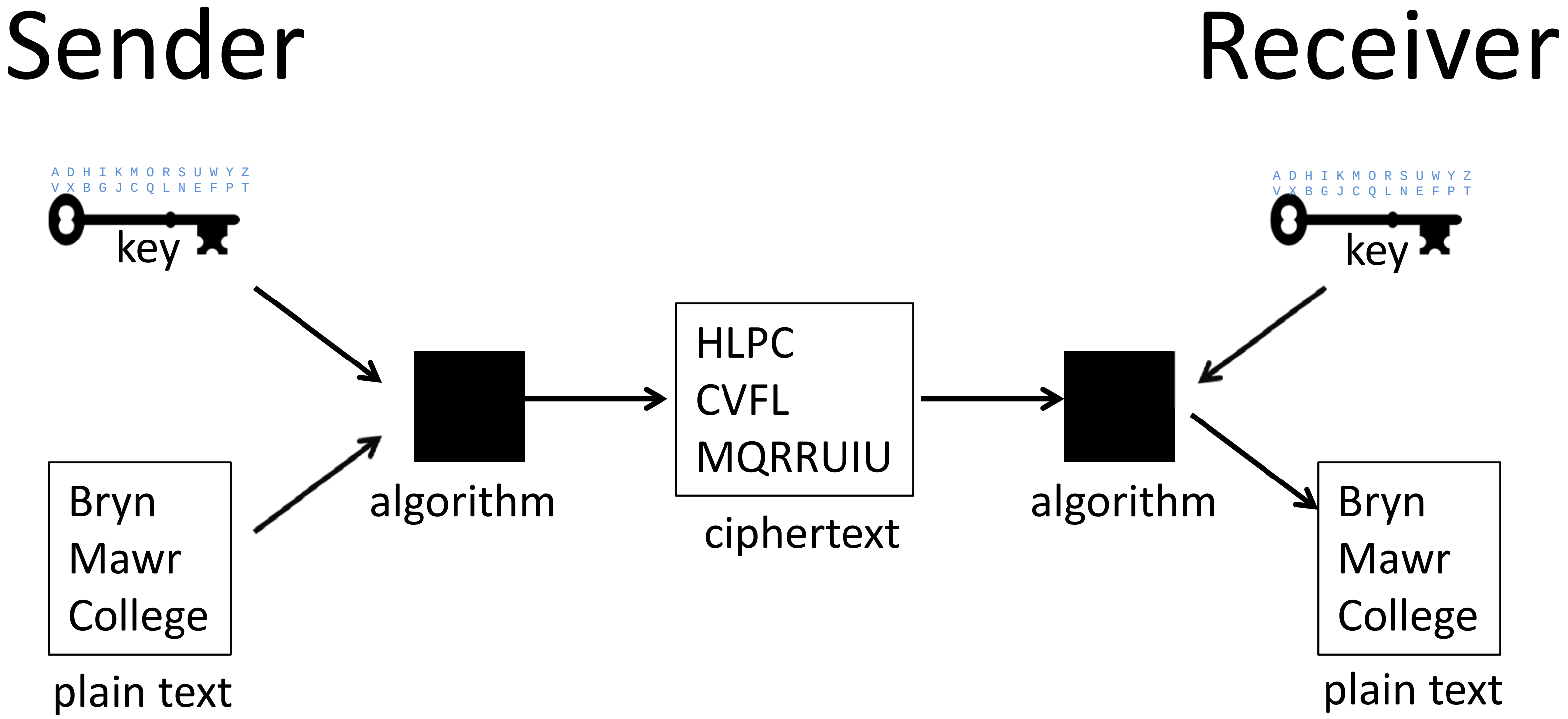
Summary: Secret Codes

- Steganography (hidden)
- Cryptography (scrambled)
  - Transposition
  - Substitution
    - Code (replace words)
    - Cipher (replace letters)
    - Nomenclators (codes+ciphers)

Summary: Secret Codes

- Steganography (hidden)
- Cryptography (scrambled)
  - Transposition
  - Substitution
    - Code (replace words)
    - Cipher (replace letters)
    - Nomenclators (codes+ciphers)
- Cryptanalysis (codebreaking)
  - Frequency Analysis

Cryptography: Basic Terminology



Sender

Receiver

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

key

Bryn
Mawr
College

plain text

algorithm

HLPC
CVFL
MQRRUIU

ciphertext

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

key

algorithm

Bryn
Mawr
College

plain text