

Codes and Ciphers

FRANK RUBIN

Marist College CLS
Fall 2017

Outline

The history of cryptography.

Hobbyist ciphers.

Class members create and solve ciphers.

www.ContestCen.com/CLS.htm

How to invent an unbreakable cipher.

Course webpage

www.ContestCen.com/CLS.htm

Useful links.

Crypto tables.

Rules for submitting cryptograms and solutions.

Cryptograms.

Lists of solvers.

Basic terms

Cryptography

is the entire field of secret writing including devising codes and ciphers, encoding and decoding messages, analyzing and evaluating systems, codebreaking, design of cryptographic machines, chemical and photographic methods, intercepting transmissions, planting false messages, etc. In short, every aspect of secret writing.

Codes

- Operate on words and phrases
- Usually commercial
- Used to save on telegraph costs
- Not secret
- Sender and receiver use the same book
- Fixed set of words and phrases

00001 Buy

00002 Deadline

00003 Agree to proposal

Ciphers

- Operate on letters or groups of letters
- Render the message unreadable to outsiders
- Legitimate receivers can unscramble and read the message
- Usually uses a different key for each message

Encryption/Encipherment

Converting a message from **plaintext** into unreadable **ciphertext** by a legitimate sender who know the method and has the key.

Plaintext is the message you wish to keep secret:

THE QUICK BROWN FOX

Ciphertext is the result of the encryption:

KB&4chDnZ\$p+ufG3T=

Decryption/Decipherment

Converting a message from unreadable **ciphertext** back into **plaintext** by a legitimate receiver who knows the method and has the key.

For example, KB&4chDnZ\$P+ufG3T=
back to THE QUICK BROWN FOX

Cryptology/Codebreaking

Reading of encrypted messages by a third party who has not been given the key

- Deducing the key
- Brute force (try all combinations)
- Espionage or bribery

History

Ancient Egypt

Hieroglyphics, small pictures representing sounds.

No cryptography for secret communications.

Varied letter shapes as an attention-getter, so people would read epitaphs.

Believed this would gain the deceased extra merit in the next world.

Ancient China

Write message on very thin paper or silk.

Coat the message in wax and swallow, or insert in rectum.

Short list of secret symbols with special meanings.

Insert symbol into an otherwise innocent message.

“Lovely weather [*need more arrows*] we're having”.

Used code names for people/places, e.g., POTUS.

Ancient India

Large spy network got assignments by secret writing.

Secret writing mentioned in Kama Sutra.

First true ciphers, including ...

Reciprocal cipher *muladeviya*

B C D F G H L M

N P R S T V W X

Hand alphabet, still used by mutes, money changers,
and commodity traders.

Sanskrit

संस्कृतम्

Hand Alphabet



Mesopotamia

Used cuneiform, wedge shapes pressed into clay.

Each group of wedges represents a syllable.

Multiple ways to represent the same syllable.

Cryptography:

- Used very obscure symbols.

- Used phonetically similar symbols.

- Used numbers to represent syllables.



Ancient Israel

Atbash cipher (DaVinci Code).

Reciprocal alphabet

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

Used mostly on names (Babel -> Sheshach).

Not used to conceal.

Belshazzar's Feast

Prophet Daniel

MENE MENE TEKEL UPHARSIN

Names of coins (penny, nickel, dime).

Aramaic roots: half, quarter, divided.

“You will be killed and your kingdom split up”.

Modern: You will be halved, quartered and *cent* to Hades.

Europe

First mention of secret writing in European literature in Homer's Iliad.

Incomparable Bellerophon, son of Poseidon.

Queen Sthenoboea, King Proetus.

Folded tablet with secret signs and writing.

King Iobates of Lycia, 9 day feast.

Chimera, Solymi, Amazons, Lycian ambush.



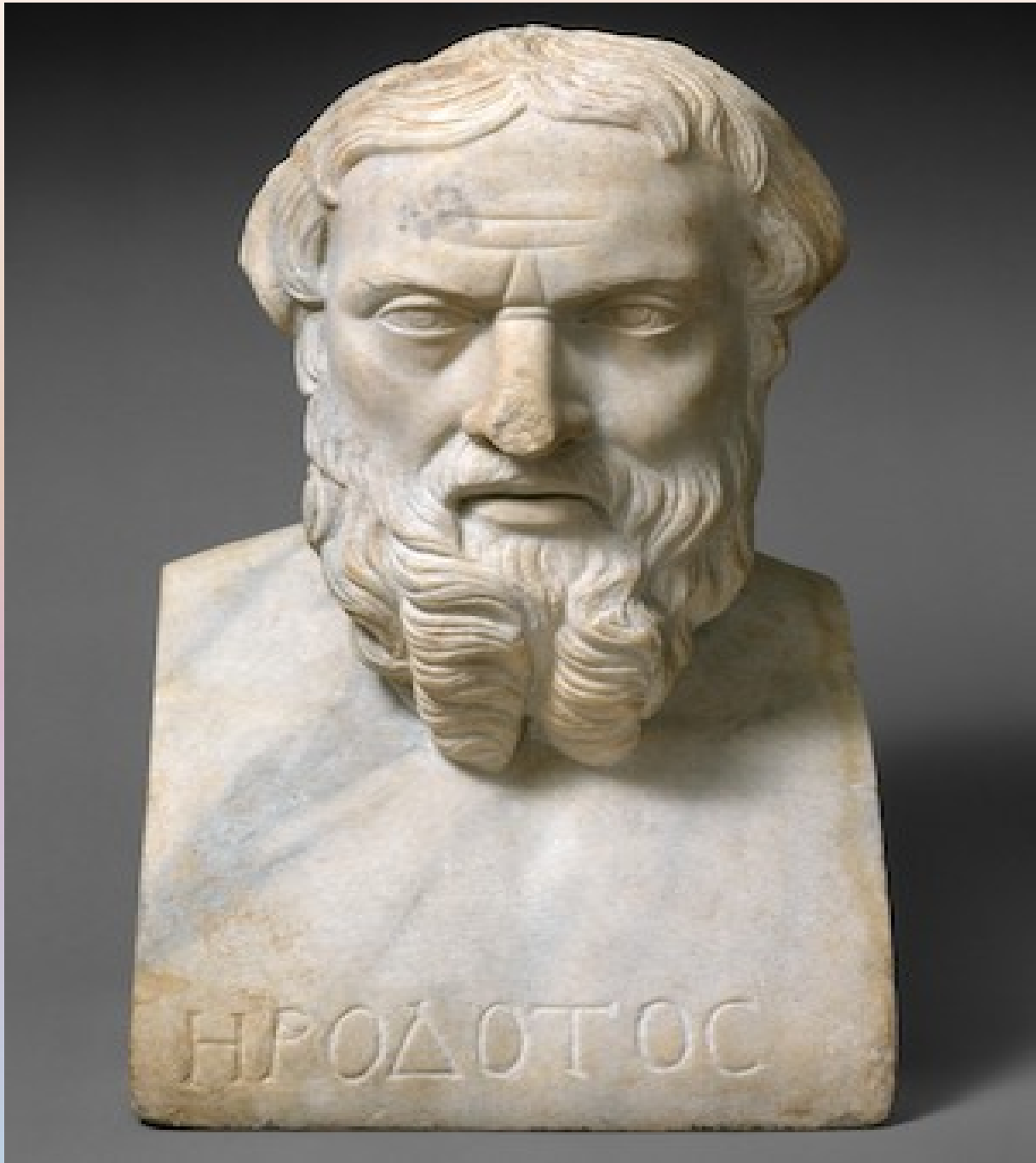
Herodotus

Steganography - hidden writing.

Harpagus dressed a messenger to Cyrus as a hunter and hid the message in the belly of an unskinned hare.

Histaieus sent message to Aristagoras tattooed on the scalp of a trusted slave.

Demaratus warned Sparta that Xerxes was coming to conquer Greece by scraping the wax off 2 writing tablets, writing the message on the wood below, then adding fresh wax. The message could not be read until Gorgo, daughter of Cleomenes discovered the secret.



Scytale / Skytale

Earliest cryptographic device, 7th century BCE

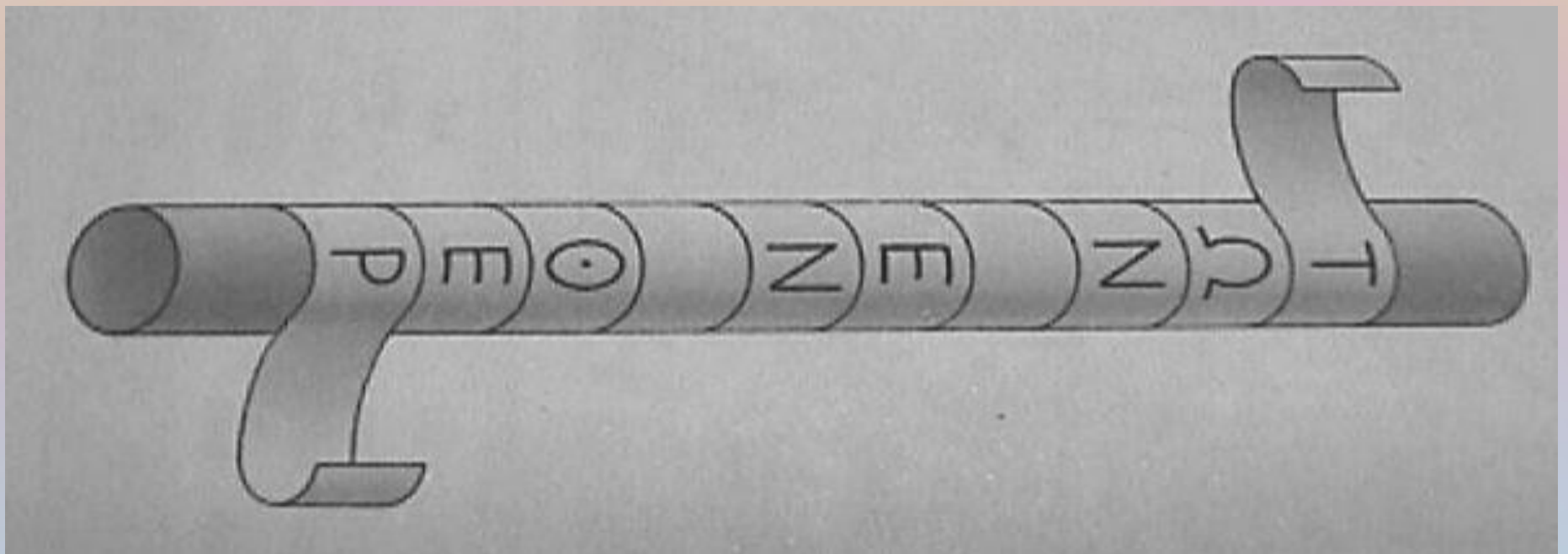
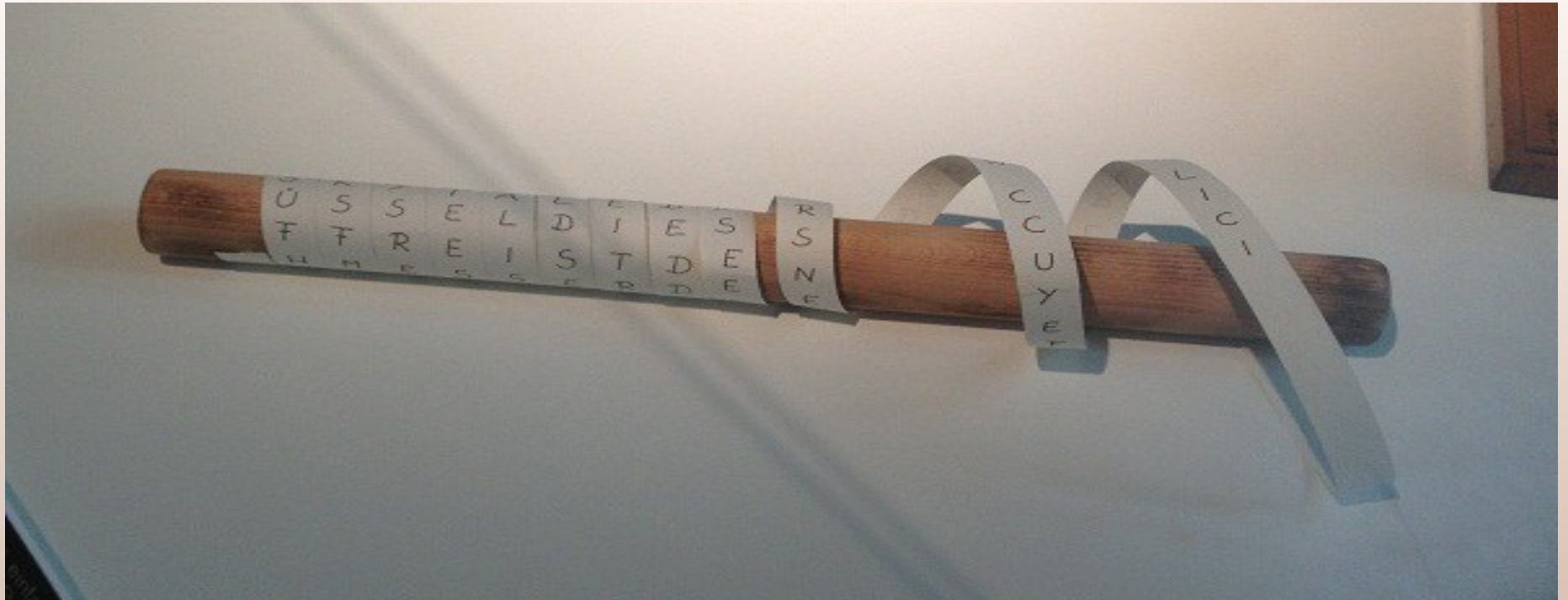
Greece, especially Sparta

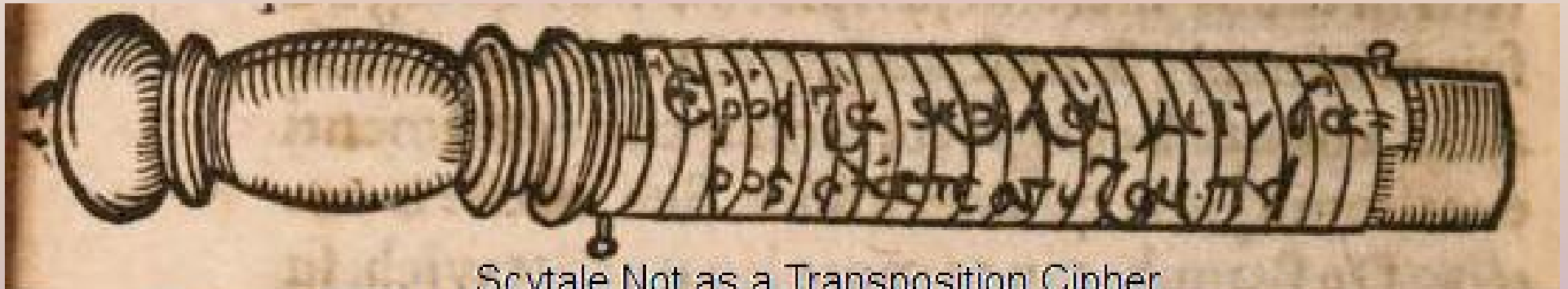
Narrow strip of cloth, leather or parchment wound helically around a wooden rod so that the edges of the strip match exactly

Sender and receiver have identical rods

Write the message along the rod, then unwind the strip

The messenger can wear the strip as a belt, to tie up his hair, sewn onto his garment as a decoration, etc.





Scytale Not as a Transposition Cipher
from Giovanni Battista Porta, *De Occultis Literarum Notis* (1593)



And now
for something
completely
different

Solving Simple Substitution Ciphers

In a simple substitution cipher each letter is replaced by a different letter or symbol consistently throughout the message. There is a one-to-one correspondence between the letter and its substitute.

So, if X represents H in one place, every X will represent H, and no other letter or symbol will represent H.

TIP: If the cipher uses symbols, it will be easier to solve if you first replace the symbols by letters.

Also called monoalphabetic cipher.

The Basics

Letter frequency

Letter contacts and combinations

Letter positions, prefixes and suffixes

Groups of letters

Common words

Pattern words

Grammar, sentence structure

Letter frequency

Normal frequency

ETAONIRSH **DCLUFMWYP** **BGVKJQXZ**

High frequency **ETAONIRSH** 70% of text

Medium frequency **DCLUFMWYP** 25% of text

Low frequency **BGVKJQXZ** 5% of text

Vowels **AEIOUY** 40% of text

Letter contacts

Q almost always followed by U and another vowel.

H usually follows a consonant and precedes a vowel.

Vowels are contacted by a variety of consonants on both sides. The only common vowel reversal is **AI** and **IA**.

Double letters: **SS, EE, TT, FF, LL, MM, OO**

Complete table at www.contestcen.com/contact1.htm

Summary at www.contestcen.com/contact2.htm

Letter contacts

	After	Vowels	Mixed	Consonants
Before				
Vowels		MVZ	RX	N
Mixed		BJQW	CDFGLPST	
Consonants		H	Y	AEIOU

Contact chart

CGHDCJH FGFAHECG KHGJDHA KCE

HF A H

HED C GJGM

JH D CH

CH E C

G F GA

HCFC G HFJ

DKAJG H DEGA

CG J HD

K HC

Vowel distribution

CGH : CGHDCJH FGFAHECG KHGJDHA KCE

CH : CGHDCJH FGFAHECG KHGJDHA KCE

GH : CGHDCJH FGFAHECG KHGJDHA KCE

Probable vowels are C, F, H

Bigram frequency

TH	2.71	EN	1.13	NG	0.89
HE	2.33	AT	1.12	AL	0.88
IN	2.03	ED	1.08	IT	0.88
ER	1.78	ND	1.07	AS	0.87
AN	1.61	TO	1.07	IS	0.86
RE	1.41	OR	1.06	HA	0.83
ES	1.32	EA	1.00	ET	0.76
ON	1.32	TI	0.99	SE	0.73
ST	1.25	AR	0.98	OU	0.72
NT	1.17	TE	0.98	OF	0.71

Trigram frequency

THE	1.81	ERE	0.31	HES	0.24
AND	0.73	TIO	0.31	VER	0.24
ING	0.72	TER	0.30	HIS	0.24
ENT	0.42	EST	0.28	OFT	0.22
ION	0.42	ERS	0.28	ITH	0.21
HER	0.36	ATI	0.26	FTH	0.21
FOR	0.34	HAT	0.26	STH	0.21
THA	0.33	ATE	0.25	OTH	0.21
NTH	0.33	ALL	0.25	RES	0.21
INT	0.32	ETH	0.24	ONT	0.20

Initial, final letters

Initial T, A, O, M, H, W, C, I, P, B, E, S

Final E, T, S, D, N, R, Y, G

Common words

Most common:

1-letter: A more common than I; O rare

2-letters: BE, TO, OF, IN, IT, ON, HE, AS, DO

3-letters: THE, AND, FOR, NOT, YOU

4-letters: THAT, HAVE, WITH, THIS, FROM

5-letters: WOULD, THERE, THEIR, WHICH,
ABOUT

Pattern: THAT, WILL, ALL, THERE, WHICH,
GOOD, EVEN

Word combinations: TO THE, OF THE, IN THE

Pattern words

LULL, TOMTOM, ONION, PEPPER, VOODOO,
COMMITTEE, SENSELESS, PREPARE,
ASSESESSES, TENEMENT

Pattern word lists, Aegean Park Press, Wayne Barker

www.aegeanparkpress.com/books_by_number.html

Grammar

Grammar can guide the solution

INDIGN MAN MYSELF POD

.E...E ARE A.....

ARE A.... could be ARE A..ING, probably ARE ASKING

INDIGN MAN MYSELF POD

.E...E ARE ASKING ...

The pattern word INDIGN fits PEOPLE

INDIGN MAN MYSELF POD

PEOPLE ARE ASKING ..O

Final word WHO

What's the plan?

First, look for small common words.

See if any of them have common letters or patterns.

TAME MEN could be WITH THE

MOSES could be THERE

Count letter frequencies.

Count contacts, identify vowels, and N, R and H.

Keep track of your guesses so you can backtrack.

Back to History

Pinhole cipher

Take a book and put pinholes at the successive letters of the message

**AS THE STORY WAS RECITED THE KIDS
ADDED THEIR OWN COLORFUL
VARIATIONS**

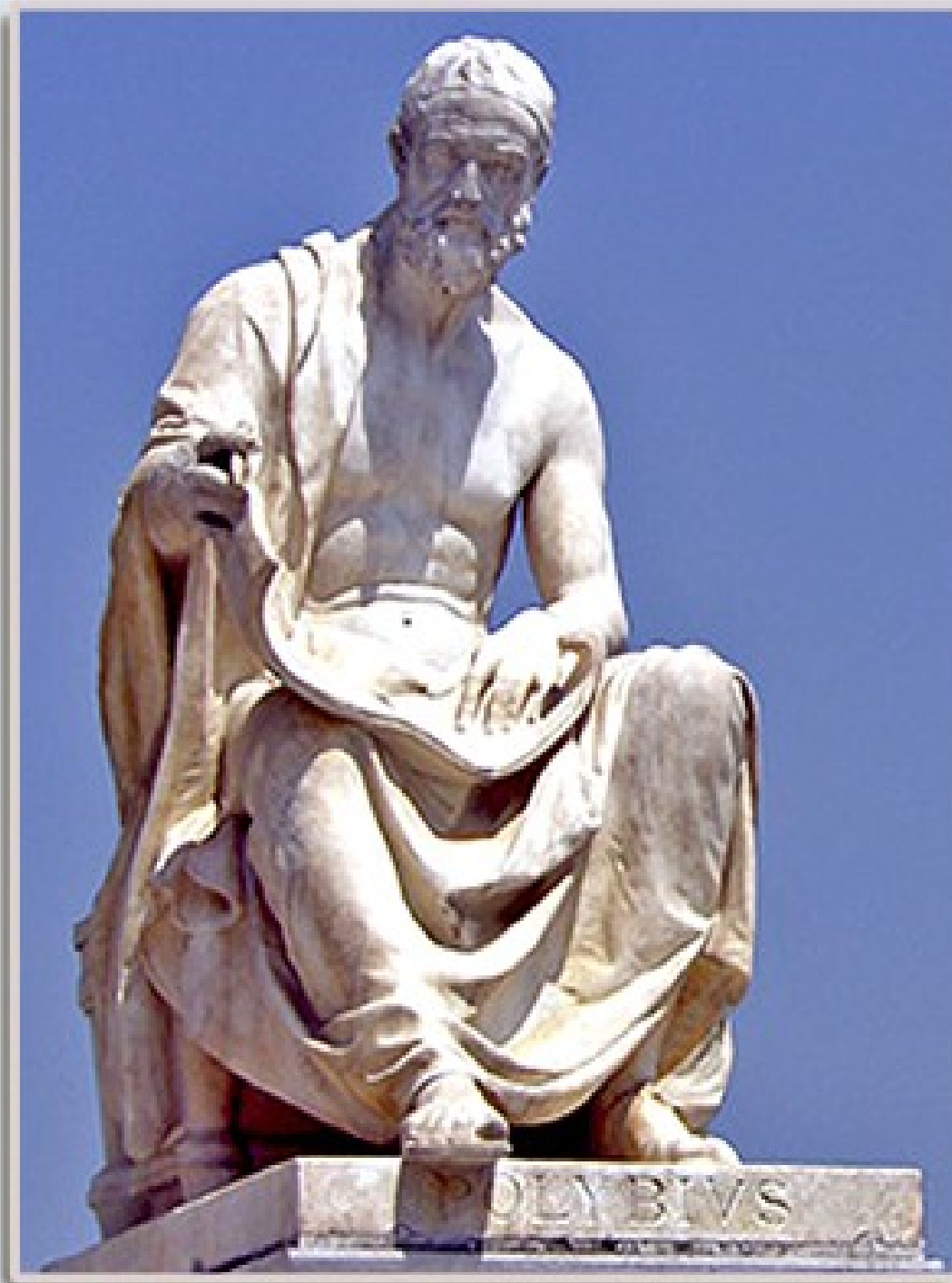
Used by Germans in WW II, e.g. by marking the letters in a newspaper with invisible ink

Polybius Square

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

A=11, B=12, C=13, etc.

Torches on hilltops



Modern use

Convert the letters to 2-digit form, scramble the digits, then convert back to letters

B E

1 1

2 5

11=A, 25=K, so BE becomes AK

Computer ASCII code A=01000001, B=01000010, etc.
so use an 8x8 array of bits

Caesar cipher

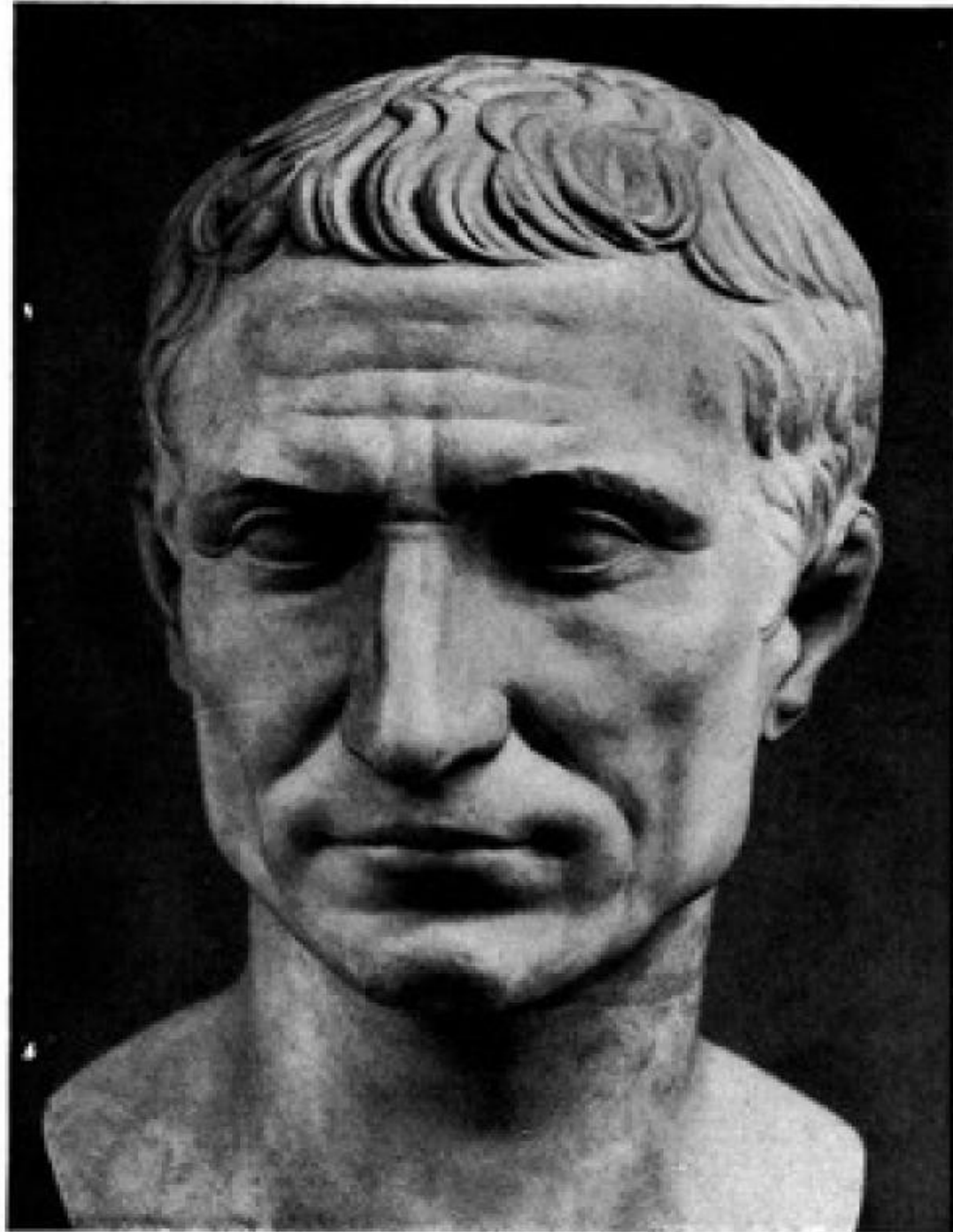
Roman generals wrote messages in Greek.

They replaced each Greek letter by the letter 3 places later in the alphabet.

ABCDEFGHIJKLMN OPQRSTUVWXYZ

DEFGHIJKLMN OPQRSTUVWXYZABC

This is the basis for many modern cipher methods.



500BCE - 500CE

Cryptography spreads throughout the known world.

Reciprocal alphabets.

Modified letter forms.

King-speak.

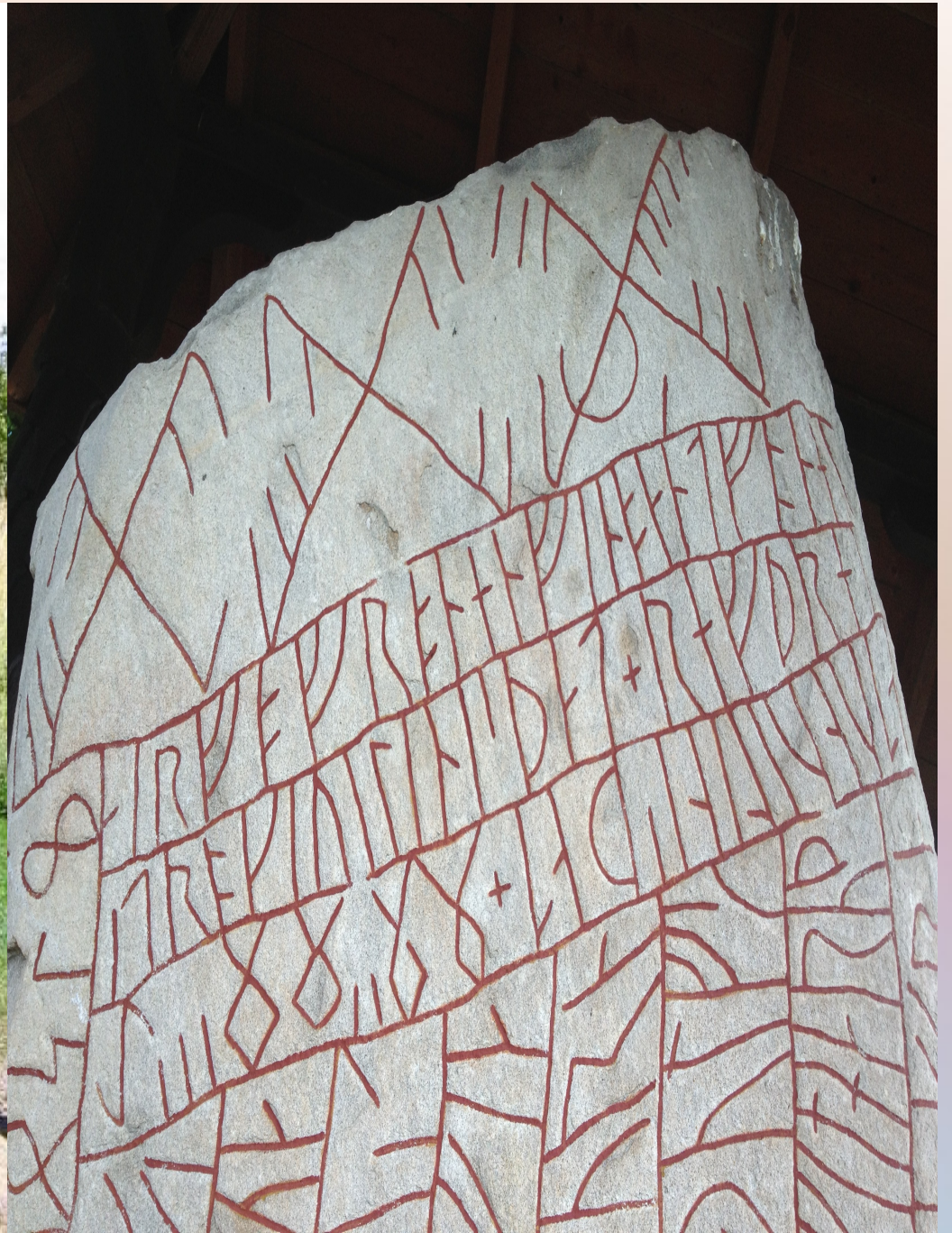
Rök Runestone

Sweden 7th-9th century CE.

Now in Ödeshög in Östergötland.

13 feet total height.

Not Latin/Greek letter forms.



Ogham

Old Irish, 1st to 5th century CE.

Sanctuary Ogham 6th to 9th century CE.

About 400 survive, monuments and tombstones.

Alphabet divided into groups of 5 letters.

Letters are indicated by slash marks above, below or across a reference line.

Lines run vertically on monuments, horizontally in manuscripts.

┌ B
└ L
≡ F
≡ S
≡ N
┌ H
└ D
≡ T
≡ C
≡ Q

┌ M
≡ G
≡ NG
≡ Z
≡ R
≡ P

┌ A
≡ O
≡ U
≡ E
≡ I
┌ A
└ O
≡ U
≡ E
≡ I

* EA
◇ OI
┌ UI
≡ IA
≡ AE

Tengwās īwerijonākā

Tut raddassodd trīs dītrebākī dīslondetun do bitū.

Tēgoddit in wāssākan do atareregiyī esyan kenutan writ dēwan.

Bāddar kina labarātun writ alaliyan qos qennan blēdaniyās.

Issit andan esset bīrt wiras dī ēbis writ alaliyan diyas blēdniyas:

“mati ad tāyomas.”

Bowet samali qos qennan blēdaniyās.

“Issit mati sodesin,” esset bīrt aliyas uiras.

Bāddar andan ēran sodesū qos qennan blēdaniyās.

“Tongū wo mō brattan,” esset bīrt trissas uiras, “ma nīt lēggītar kiyunessus do mū, imbit gabiyū wāssākan oliyan dū swi.”

Three holy men turned their back on the world.

They went into the wilderness to atone for their sins before God.

They did not speak to one another for a year.

At the end of the year, one of them spoke up and said, "We're doing well."

Another year went by the same way.

"Yes we are," said the next man.

And so another year went by.

"I swear by my smock," said the third man, "if you two won't be still I'm going to leave you here in the wilderness!"

Dark Ages (600-1400CE)

Almost no literacy.

Sciences, including cryptography, largely forgotten.

Replacing vowels by dots (v::w:ls b::: d::ts).

Writing words backwards (gnitirw sdrow sdrawckab)

Replacing letters by symbols (☼=A, ‡=B, ≷=C, etc.)

Writing phonetically using different alphabets (Greek, Hebrew, Arabic) **ליתם טרפיק ליק עי**

Cryptography becomes associated with magic and the occult.

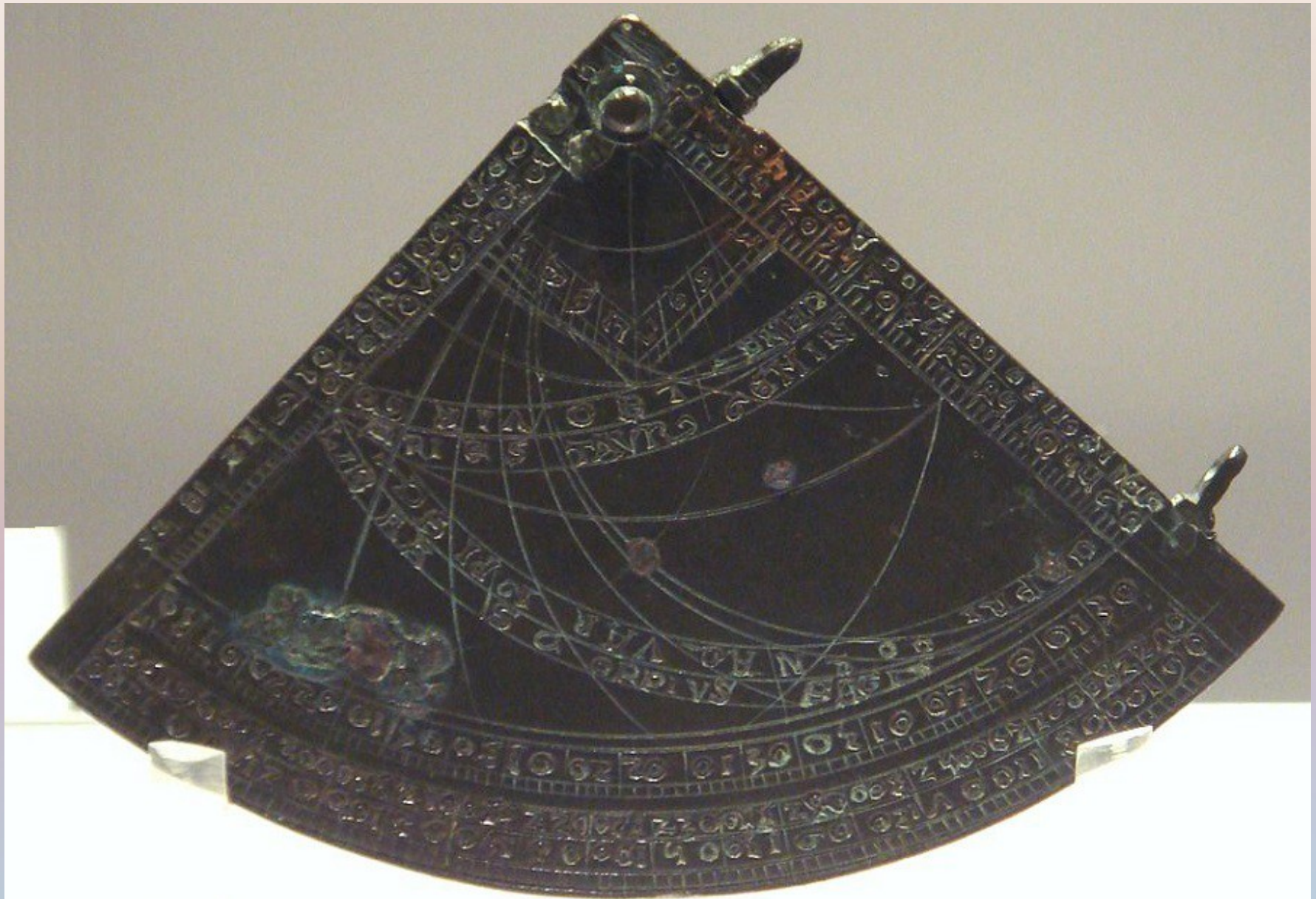
Geoffrey Chaucer

UGZT UVDWLO 1003ZUG
860 UB AGUEO 23 UB
UGO UVDWLO 68 03BV
1263 68 UGO H130
63 02UGO0 12R0

This table serveth for to entre in to the equacion of the mone on either side



Canterbury Astrolabe 1388



Qalqashandi

Shihab al-Din abu 'l'Abbas Ahmad ben Ali ben Ahmad 'Abd Allah al-Qalqashandi

Arab culture flourishing

14-volume 'Handbook for Secretaries', 1412

Needs: roadblocks, ambushes, careful examination

Seven methods of encryption:

Replace letters by other letters (substitution)

Write some words backwards

Reverse alternate letters (ATLENRAET LTETRES)

Replace a letter by its numeric value

Replace a letter by two letters that add to its value

Substitute names for letters (Helen Eric Linda Paul)

Substitute signs, symbols or drawings (§ P U © ☺ 🎵)



Dictionaries

First dictionaries, circa 750CE lead to awareness of letter frequencies.

Za is least, alif and lām most frequent due to the prefix al- meaning “the”.

Study of grammar gives

- Common and rare letter combinations

- Common initial and final letters and combinations

- Probable words, *bismillah* “God willing”

Cryptology emerges circa 1450CE.

15th century Europe

Cryptography becomes universal.

Every king, noble, ambassador, spy uses cipher.

Cipher secretary.

The Vatican has a cipher bureau.

Giovanni Soro in Venice, the first crypto superstar.

Venice founds the first cipher school, with exams.

Cipher contests.

15th century methods

Simple substitution.

Code names for important people, places.

Multiple substitutes for vowels (E could be Q or 16).

In 16th century multiple substitutes for consonants.

Birth of the nomenclators:

Long lists of letters, words, names.

Multiple substitutes for common items.

Used for years, sometimes 100+ years.

Nomenclator

Nomenclator means “name caller”.

Used from 15th through 18th centuries.

Included letters, numbers, words, names, syllables.

Later nomenclators were code books with up to 50,000 items.

Innovations:

Multiple substitutes.

Nulls (ignore this item).

Traps (ignore next/previous/enclosed item(s)).

Compiling a nomenclator

Compile a list of the terms to be used: ship, cannon, battle, armada, admiral, grapnel, latitude, etc.

Everything else will be spelled out in letters or syllables

Alphabetize the list

Assign code words to the list

AAA admiral

AAD armada

AAF battle

etc.

Solving a Nomenclator

Obtain a large number of messages (intercepts).

Hunt for repeated items, groups of items.

Guess at subject matter, people and events mentioned.

Use knowledge of sender, receiver and situation.

Guess common phrases, “Dear Sir,” “Yours truly,” etc.

Senders tend to use the same substitutes repeatedly.

Look for words repeated in some messages, but absent in others. Relate this to subject matter, people involved, etc.

Solving a Nomenclator

Look for near-repeats

14 29 **52** 07 81

14 29 **73** 07 81

could mean that 52 and 73 represent the same letter.

Plus ... espionage, bribery, break-ins, intercepting messengers with new code books, etc.

Intercepting deciphered messages gives a crib.

Phony messages

X is fighting Y. X sends a phony message in a weak cipher, knowing Y will intercept it and easily read it. When Y enciphers the message using the nomenclator and sends it to the king or general, X intercepts the enciphered message. Since X knows what the message says, that gives X a crib.

Or... just plain stupidity, like sending a message in both cipher and clear. Or, sending multiple copies of a message using different homophones. That reveals the equivalences.

16th Century

Bigger nomenclators.

Networks: general cipher for correspondence among peers (ambassadors, bishops, etc.), plus individual ciphers for correspondence with the hub (king, Curia, Council of Ten, etc.).

Lots of work for cipher secretaries, cipher bureaus.

Passing crypto knowledge in families.

Back-up ciphers for quick replacement when a breach is suspected.

Mixing the alphabet

Late 16th century innovation: message keys.

Use a message key to mix the alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

SAMPLEBCDEFGHIJKNOQRTUVWXYZ

Better

ABCDEFGHIJKLMNOPQRSTUVWXYZ

GFDCBSAMPLEZYXWVUTRQONKJIH

Mixing the alphabet

Even better

SAMPLE

BCDFGH

IJKNOQ

RTUVWX

YZ

Read down the columns

SBIRYACJTZMDKUPFNVLGOWEHQZ

Or, up the columns, right-to-left, alternate up/down, start in the middle, etc.

SBIRYZTJCAMDKUVNFP LGOWXQHE

Modern Ideas

Polyalphabetic cipher

Use multiple alphabets

Cycle through the alphabets

Use a key to determine the progression

Three ideas, three different innovators, over 100 years

Leon Battista Alberti

Born Genoa 1404, raised in Florence, died 1472.

A founder of the Renaissance.

Father of Western Cryptology.

Trained as lawyer (church law).

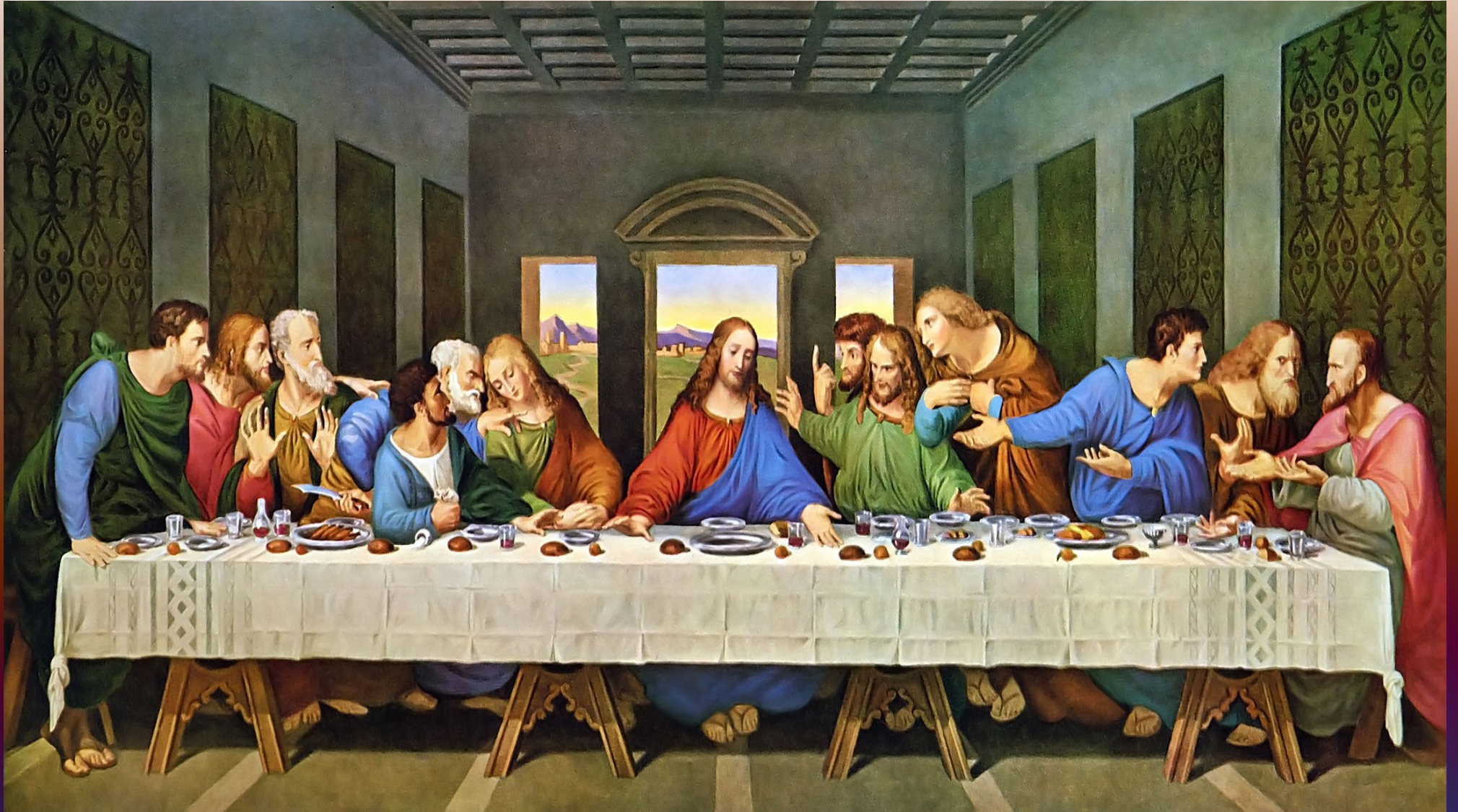
Becomes architect. Builds Pitti Palace, second Trevi fountain, church of Sant'Andrea in Mantua, temple of Malatesta at Rimini, many others.

Known today mainly as painter.

Composed music, one of greatest organists of his time.







Leon Battista Alberti

Wrote poems, comedies, treatise on the fly, first scientific book on perspective, books on morality, law, philosophy, family life, sculpture and painting.

De Re Aedificatoria first printed book on architecture.

Superb athlete, could ride wildest of horses.

Wrote first Western treatise on cryptography.

Joined papal curia, became bishop.

Invented polyalphabetic ciphers, cipher disk, 1467.

Two concentric copper disks divided into 24 equal sectors. Outer disk stationary, inner disk rotates.

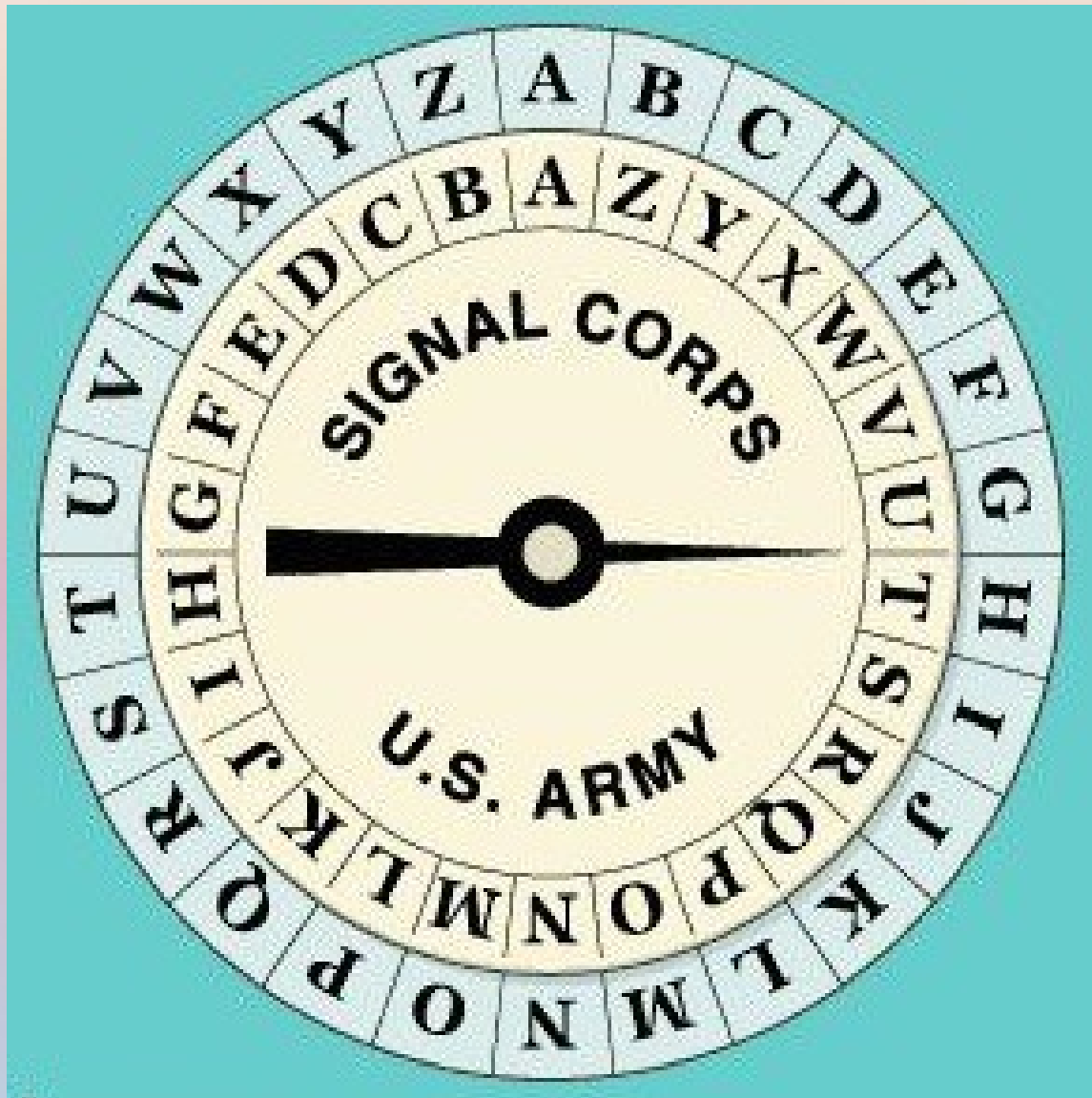
Alberti Cipher Disk



French cipher disk 16th century



Modern Cipher Disk



Cipher disk

Alberti's method:

Sender and receiver agree on an index letter on the outer disk.

Sender chooses a key letter, sets this letter on the inner disk next to the index letter. Writes the key letter into the message.

Encodes 3 or 4 words with this setting, plaintext on outer disk, ciphertext on inner disk.

Chooses a new key letter and repeats.

Enciphered code

Uses all combinations of the numbers 1,2,3,4 in groups of 2, 3 and 4 digits. Total of 336 combinations.

Uses a small code of 336 items (names, places, common words)

Enciphers the code groups the same way as the letters in the message

Solving a disk cipher

Assume Alberti's method, using mixed alphabets.

Collect several messages until you have two or more sections enciphered with the same key letter.

Solve those sections as a simple substitution.

Reconstruct the disk. If you know that XY with key Z gives AB , then the distance along the outer ring from X to Y is the same as the distance along the inner ring from A to B .

If XY with key Q gives CD , Then the distance on the inner ring from A to B is the same as the distance from C to D . Likewise the distance from A to C , and from B to D is the same as the distance from Z to Q

Piece such fragments together to get a full reconstruction.

Johannes Trithemius

Born 1462. Father Johannes of Heidenberg wealthy wine merchant dies 1463.

At 17 runs off to Heidelberg, pauper, taken in by headmaster Johannes of Dalberg.

Joins monastery, becomes abbot at age 24.

Writes numerous books, histories, biographies, etc.

First crypto book *Steganographia* gives 13 methods of hidden writing.



Steganographia

A=HOLY

A=GOD

A=GRANT

A=US

B=BLESSED

B=LORD

B=GIVE

B=ME

C=SACRED

C=FATHER

C=PROVIDE

C=MAN

D=REVERED

D=CREATOR

D=SHOWER

D=ALL

E=AWESOME

E=KING

E=ENDOW

E=FOLK

F=BELOVED

F=SPIRIT

F=SUPPLY

F=KIN

Encipher first letter from first column, etc

Resulting message looks like a prayer.

Polygraphia

Published 1516 by Johannes Haselberg of Aia, first printed book on cryptography.

Replaces disk by tableau

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BCDEFGHIJKLMNOPQRSTUVWXYZA

CDEFGHIJKLMNOPQRSTUVWXYZAB

DEFGHIJKLMNOPQRSTUVWXYZABC

EFGHIJKLMNOPQRSTUVWXYZABCD

...

Encipher the first letter using the top line, the second letter using the second line, etc., repeating after every 26 letters

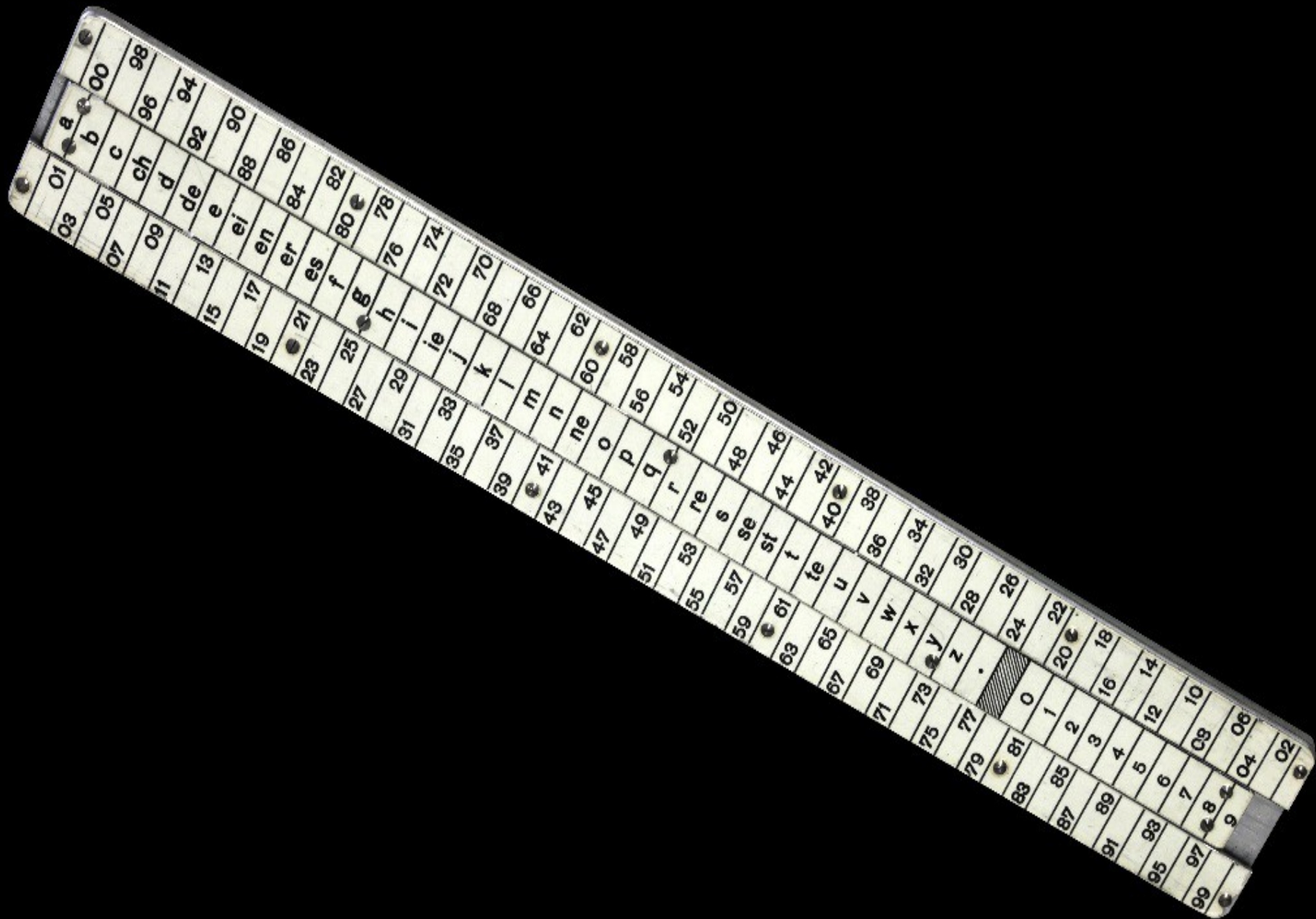
Modern practice

Instead of writing out a tableau, use a slide. Just slide one copy of the alphabet against another.

ABCDEFGHIJJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Make the stationary alphabet double-wide to avoid wrapping the moving alphabet end-around.





Solving the tableau

Trivial. Since the same sequence of cipher alphabets is used for every message, once the method is known, deciphering is rote.

TQOZJ

SPNYI

ROMXH

QNLWG

PMKVF

OLJUE

Giovan Battista Belaso

In 1553 invented the *countersign*, now called *keyword* or simply *key*.

Write the key over each letter of the message, and encipher that letter using that key.

SAMPLE SAMPLE SAMPLE SAMPLE S
thisis themes sageiw illsen d

Standard tableau with unmixed alphabets.

Today it is called the Vigenère cipher for Blaise de Vigenère.

How to solve it

- (1) Determine the period (key length).
- (2) Solve each of the alphabets separately.

For each of the 26 possible keys for that column, calculate the correlation coefficient with the known standard English letter frequencies.

Correlation coefficient was developed by Karl Pearson about 1900, and uses the simple, easy-to-remember formula.

Correlation coefficient

$$r = \frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2} \sqrt{n(\sum y^2) - (\sum y)^2}}$$

FUHGEDDABOUDIT

There's an easier way

Frequency matching

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XXXXXXXXXX XXXXX XXXXXX X

X XXXX XX X XX XXXX

X X X XX XXX

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XXXXXXXXXX XXXXX XXXXXX X

X XXXX XX X XX XXXX

X X X XX XXX

91449414900419910999411010 = 102

Frequency Matching

ABCDEFGHIJKLMNOPQRSTUVWXYZ

XXXXXXXXXX XXXXX XXXXXX X

X XXXX XX X XX XXXX

X X X XX XXX

ZABCDEFGHIJKLMN OPQRSTUVWXYZ

XXXXXXXXXX XXXXX XXXXXX X

X XXXX XX X XX XXXX

X X X XX XXX

03246622600023930099621000 = 75

Works for standard and mixed alphabets.

Frequency Matching

Or... just make up the histograms for each alphabet, and for standard English, then slide them past each other, and match them up visually. The place where the peaks and valleys match best is usually the correct one.

After a little practice you will know the standard frequency by heart, and can determine the correct key just by inspection.

Landmarks: three peaks 4 spaces apart at AEI, two peaks together at NO, three peaks together at RST.

The valleys are are important as the peaks.

Giovanni Batista Porta

Born Naples 1535

At 22 publishes *Magia naturalis*, scientific oddities.

Founds two scientific societies (Galileo).

Writes books on human physiognomy, meteorology, refraction of light, pneumatics, design of villas, astronomy, astrology, distillation and memory improvement, plus 17 stage plays.

Expands *Magia naturalis* to 20 volumes; translated and reprinted 27 times. Many recipes for invisible ink, including ink on human skin, so a message can be carried undetected.

Giovanni Batista Porta

In 1563 (age 28) writes 4-volume *De Furtivis Literarum Notis* covering the entire history and scope of cryptology. Still read today.

First digraphic cipher 20x20 tableau of 400 symbols.

Pulled together all 3 elements of polyalphabetic ciphers, Alberti's mixed alphabets, Trithemius's tableau and Belaso's mnemonic key.

Gave the first (albeit weak) methods for solving polyalphabetic ciphers.



Girolamo Cardano

Pavia 1501 - Rome 1576.

Physician and amateur mathematician.

Founder of probability theory.

Obsessed with fame, published 131 books, left behind 111 unpublished manuscripts.

Invented Grille Cipher.

Cut small holes in a stiff sheet of cardboard, et al.

Write the message through the holes, remove the grille, then fill in innocent text to conceal the real message.



Cardano Grille

DADDY HUNG HER CLEVER POEM
ABOUT THEE CAT ON THE FIRE
PLACE

Impractical; very hard to fill in text to make the message look natural.

Sir John regards you well and speaks again that
all as rightly 'wails him is yours now and ever.
May he 'tone for past d'lays with many charms.

S

p

ain

s

wails

i

n

May

'to

arms.

Modern Grille

Baron Edouard Fleissner von Wostrowitz, 1880.

Used by Germany in WW I.

Mark the square grille into a grid.

Cut holes in 1/4 of the grid squares. Sender and receiver must have identical grilles.

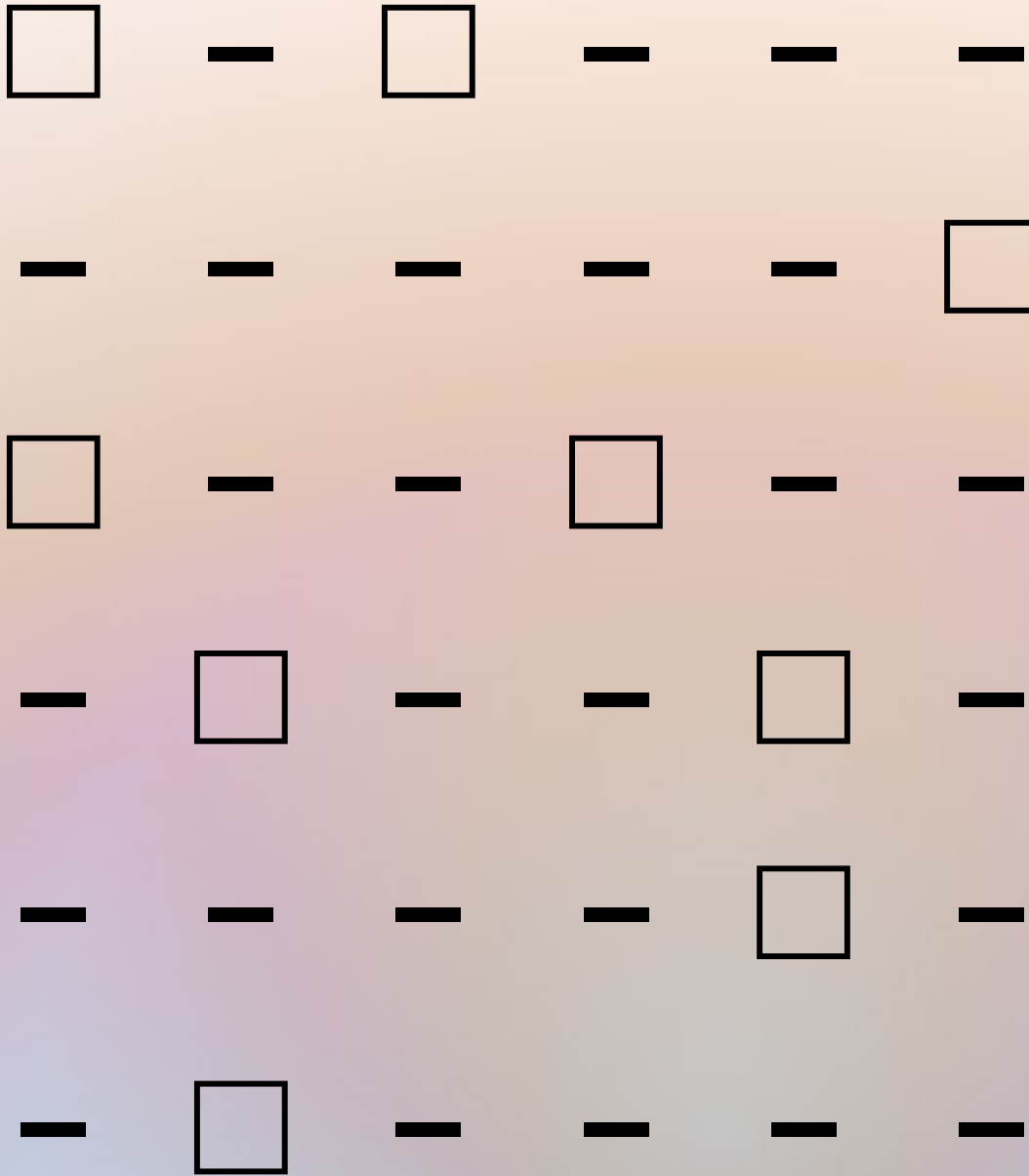
Write the first 1/4 of the message through these holes.

Turn the grid 90° and write the next 1/4 of the message.

Repeat for 3rd and 4th quarters of the message.

Can leave some positions uncut and use them for nulls.

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1



H - E - - -
- - - - - A
V - - Y - -
- I - - S -
- - - - T -
- H - - - -

H	-	E	E	-	H
E	-	A	-	-	A
V	-	-	Y	-	D
-	I	-	T	S	-
-	H	A	-	T	-
-	H	-	-	T	-

H - E E W H

E E A - - A

V A - Y R D

- I S T S T

H H A - T -

- H - E T R

H O E E W H

E E A Y A A

V A L Y R D

C I S T S T

H H A R T O

W H N E T R

H O E E W H

E E A Y A A

V A L Y R D

C I S T S T

H H A R T O

W H N E T R

HOEEW HEEAY AAVAL YRDCI

STSTH HARTO WHNET R

Blaise de Vigenère

French 1523-1596.

CREDITED with inventing Belaso's tableau cipher.

ACTUALLY invented the autokey cipher.

SAMPLE	HEREIS	THEMES	SAGETH	ATIWAN	T
hereis	themes	sageth	atiwan	ttosen	d
ZEDTTW	ALVQMK	LHKQXZ	STOATU	TMWOEA	W



How to solve it

Try each key length in turn. Then try each possible value for the first key letter. Let's try length 6.

S	H	T	S	A	T
ZEDTTW	ALVQMK	LHKQXZ	STOATU	TMWOEA	W
H	T	S	A	T	D

This key letter gives us every 6th letter of the message. If this matches normal English letter frequency, then try the second letter of the key, and so forth.

Second letter:

SA HE TH SA AT T

ZEDTTW ALVQMK LHKQXZ STOATU TMWOEA W

HE TH SA AT TT D

and so forth.

Probable word

Try a probable word in each position

MES SAGE

ZEDTTW ALVQMK LHKQXZ STOATU TMWOEA W

eis them

MES SAGE

ZEDTTW ALVQMK LHKQXZ STOATU TMWOEA W

eth atiw

Vigenère

History treats Vigenère very badly. Even though he describes both mixed alphabets and autokey, later descriptions of his work include neither of these important concepts.

He gets credit only for the tableau cipher with standard alphabets, which Belaso had invented.

Vigenère's cipher using both autokey and mixed alphabets would have been indecipherable for 16th to 19th century cryptographers.

Instead, the nomenclator remained the standard method for 300 years.

Pros and Cons

Secure: Vigenère's cipher using autokey and mixed alphabets would have been unbreakable before computers. Impossible for hobbyists.

Slow: Must write out the key and message and work one character at a time.

Error prone: Drop a letter, add a letter, or change a letter and the message may be unreadable. Then they would have to send a messenger back to get an ungarbled message. This triples the transmission time.

French cipher device

Out-of-context

French cipher device disguised as a book with the coat of arms of French king Henri II, 1519-1559.

(Henri II invented the concept of the patent, where an inventor publicly discloses an invention in exchange for exclusive rights.)



17th Century

John Falconer, distant relative of David Hume.

Crypto clerk for future King James II.

Cryptomenytices Patefacta 1685. Reissued in 1692 as *Rules for Explaining and Decyphering all Manner of Secret Writing*.

First mention of columnar transposition.

First practical transposition cipher, still in use today.

Complete and incomplete (regular and irregular).

Transposition key

Choose any keyword or keyphrase, say **SAMPLE**.

Denote the earliest letter in alphabetic order as 1.

Denote the second earliest as 2, etc. If the same letter appears more than once, go left to right.

SAMPLE

ALABAMA

-1---2

1-2-3-4

-14-32

1625374

614532

SAMPLE

614532

THISIS

MYNEWS

ECRETM

ESSAGE

HYCS

SAMPLE

614532

THISIS

MYNEWS

ECRETM

ESSAGE

HYCSS SME

SAMPLE

614532

THISIS

MYNEWS

ECRETM

ESSAGE

HYCSS SMEIW TGINR SSEEA TMEE

LONGERKEYWORD

68742A53DC9B1

INCOMPLETECOL

UMNARTRANSPOS

ITIONCIPHER

LONGERKEYWORD

fhgdbjecmlika

LSMRN EAPOA OLRII UICNI NMTCP RPTCO

OESET NH

How to solve

Complete: Factor the cipher length to get possible key lengths. For example, 28 characters suggests either 4 or 7 columns. If there are several messages with the same key, look for common factors.

Incomplete: Guess the likely number of columns. For hobbyist ciphers the most probable are 5, 6, 7, 4, 8, 9 and 10.

Write the columns onto strips of stiff paper. For incomplete transposition add 1 or 2 letters at either end to allow for unequal columns.

Try different pairings of the strips to see if they form common digrams (letter pairs), TH, ER, IN, etc. Use the contact frequencies at

www.contestcen.com/CLS.htm

Try to extend the digrams into trigrams, and then into words. For incomplete transpositions you will need to slide the strips up and down as well as changing their order.

Or ... just eyeball it.

HYCSSSMEIWTGINRSSEEATMEE 24 chars

HYCSSS MEIWTG INRSSE EATMEE 4 columns

HYCS SSME IWTG INRS SEEA TMEE 6 cols

H M I E

Y E N A

C I R T

S W S M << Unlikely, not 4 cols

S T S E

S G E E

HYCSSMEIWTGINRSSEEATMEE 24 chars

HYCS SSME IWTG INRS SEEA TMEE 6 cols

H S I I S T this, sit, his

Y S W N E M new(s), men, sew

C M T R E E tree, meet, mere

S E G S A E sage, ease, sea

HYCSSSMEIWTGINRSSEEATMEE 24 chars

HYCS SSME IWTG INRS SEEA TMEE 6 cols

TH S I I S this, is

MY S W N E new(s), sew(n)

EC M T R E term, met

ES E G S A sage, sea, gas

HYCSSSMEIWTGINRSSEEATMEE 24 chars

HYCS SSME IWTG INRS SEEA TMEE 6 cols

TH S ISI this, is

MY S NEW new, news

EC M RET

ES E SAG sage

HYCSSSMEIWTGINRSSEEATMEE 24 chars

HYCS SSME IWTG INRS SEEA TMEE 6 cols

THISI S is

MYNEW S news

ECRET M (s)ecret

ESSAG E (m)essage

*Time for
some light
refreshment*

Railfence

The simplest transposition cipher

Write the text in a zigzag, like a rail fence, and read it out straight across the rows.

T		A		E		P		R					
H		S	R		F	N		I	H		O	Y	
	I	I		A	L		C	C		E	F		O
		S			I			E			R		U
TAEPR	HSRFN	IHOYI	IALCC	EFOSI	ERU								

Compact form

TA-E-P-R

HSRFNIHOY

I IALCCEFO

S-I-E-R-U

TAEPR HSRFN IHOYI IALCC EFOSI ERU

How to solve it

Just guess the number of rows. It's usually 3, 4 or 5.

Route transpositions

Simple transpositions suitable for children. But make sure the rows and columns are straight!

Write the message into a rectangular grid using one route, then take it out using a different route.

Across the rows left to right, across the rows right to left, alternating left/right/left, down the columns, up the columns, alternating columns, diagonally, alternating diagonals, inward spiral, or outward spiral.

In: Across the rows

S I M P L E S

I M O N M E T

A P I E M A N

G O I N G T O

T H E F A I R

Out: Alternating columns

SIAGT HOPMI MOIIE FNENP LMMGA

ITAE E STNOR

How to solve it

First factor the length of the message. This will suggest probable dimensions for the grid. For example, a message of 63 characters probably uses a 7×9 or a 9×7 grid. (These are equivalent for a route transposition.) The correct dimensions are usually close to a square, so 3×21 is very unlikely.

Try the various ways of reading out the message.

Once you have filled in the grid, you can see where there are words in the rows or columns or diagonals.

Antoine Rossignol

French Jan. 1, 1600-1682. Greatest cryptographer of the 17th century. Started dynasty.

Cryptographer to Cardinal Richelieu and Louis XIV.

Invented the double nomenclator.

Single nomenclator has codes in order, a=21, able=24, abbot=27, etc.

Very easy for the cryptographer to guess words by interpolation. If 274=captain and 280=cargo, then 277 might be capture.



Double nomenclator

Assigned codes in random order.

Used 2 lists, one with plaintexts in alphabetic order, the other with the codes in alphabetic or numeric order.

Much harder to solve, but slower to use and much more costly to compile.

Most nomenclators were a compromise, sections in random order, but numeric order within sections.

2000 to 3000 items by the end of the century.

18th Century

The rise of the Black Chambers.

The greatest was Vienna Geheime Kabinets-Kanzlei.

Every day at 7AM all the diplomatic mail was delivered, opened by warming the wax seals, deciphered, the contents copied out by clerks who were speed-writers or knew shorthand, or dictated to as many as 4 stenographers, then resealed with the original wax and forged seals, and delivered.

Two translators were on hand for every language in Europe.

At 10AM letters in transit through Vienna arrived.

American Revolution

Both the American and British armies made extensive use of invisible ink. American ink supplied by James Jay, brother of John Jay, later the first chief justice.

Spy Benjamin Church Jr., Chief of Hospitals, used weird monoalphabetic cipher $\xi\mu\varphi\mathfrak{K}\delta$ easily broken. Tried, jailed, expelled, dies in shipwreck.

Extensive use of ciphers on both sides, but little cryptology due to few intercepts.

How cryptography won the war

About 2 weeks before the battle James Lovell solved a British cipher. Guessing that this was the general cipher used by all British, Lovell sent a copy of the cipher tableau to Washington and other commanders.

Despite the French fleet, Cornwallis and Clinton sent messages by small boats across Chesapeake Bay. One of these gets intercepted, and the message from Clinton to Cornwallis is read using Lovell's key.

This gives away the British plan to send a relief fleet from New York under General Graves.

The war is won

The plan is sent to Gen. Washington, and also to the French fleet under Comte de Grasse.

Cornwallis held sham surrender negotiations for 3 days, expecting the relief fleet. (Yorktown VA, James River, Chesapeake Bay.)

De Grasse positioned the French fleet of 24 ships of the line to block the British fleet.

It works. The British turn back, Cornwallis surrenders for real, the Americans capture 6000-7000 British troops, and the war ends.

Cryptography won the war.

Morning & Night of the 5th, & Morning of
the 6th.

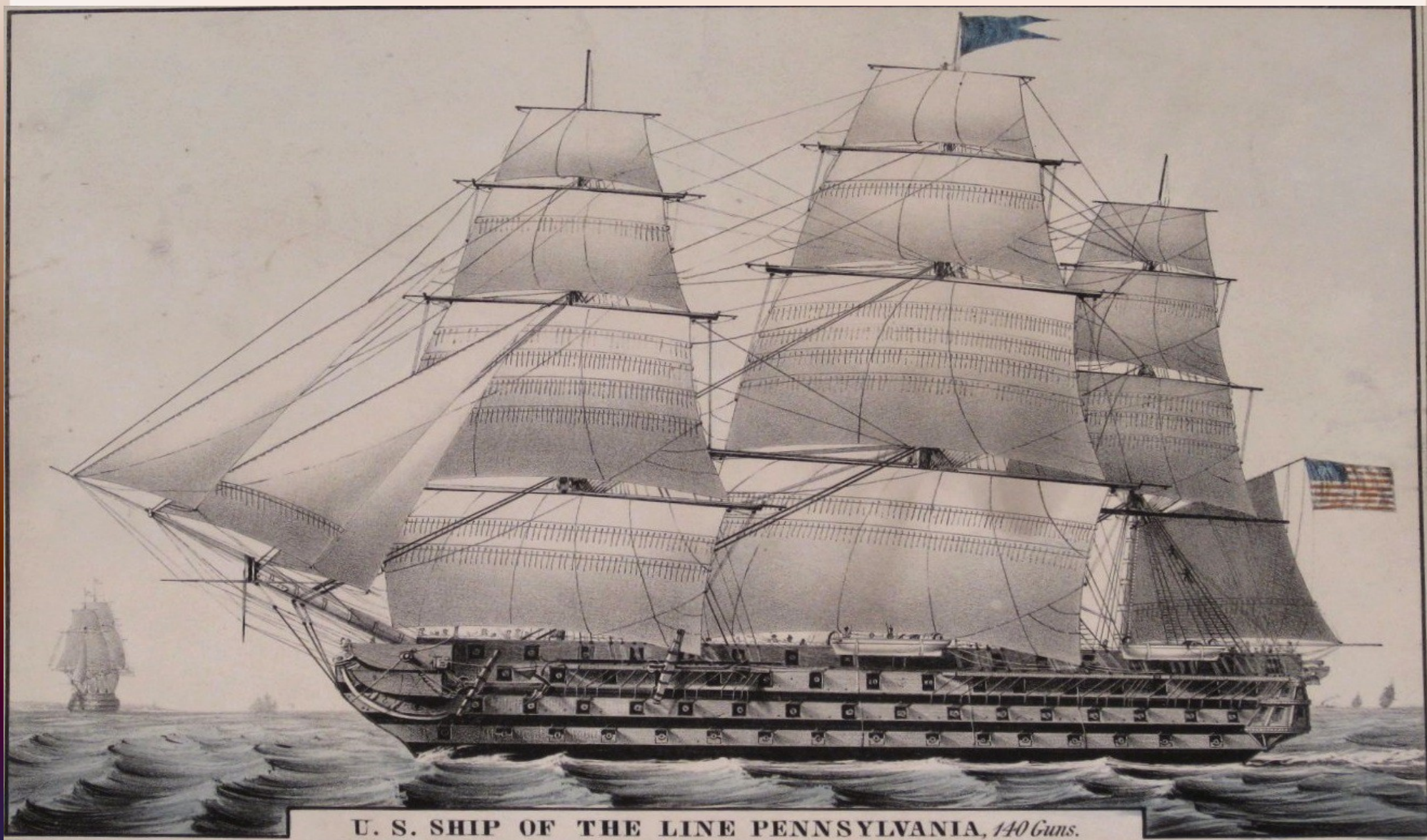
The French Troops, landed
at James Town, are said to be three thousand
eight hundred. Washington is said to be
shortly expected, & his Troops are intended
to be brought by water from the head of
Elk under Protection of the French Ships,
The Marquis de La Fayette is at or
near Williamsburgh, & the French
Troops are expected there, but were not
arrived last night, 16, 22, 10, - 16, 16, 22, 26 -
14, 19, 13, 23, 16 - 14, 11, 13, 14, 6, 19, 7 - 1, 6, 10, 16, 7, 10, 7, 11 - 19, 5,
2, 11, 5, 11, 6, 3, 11 - 1, 2, 9, 10, 0, 11, 7, 10, 25, 11, 6 - 10, 16, 7, 13, 19, 6, 29 -
9, 19, 16, 1, 7, 1, 19, 6², 19, 12, 7, 19, 5 - 7, 29, 11, 7, 19, 14, 5⁵ - 13, 32, 3 -
23 - 3, 19, 9, 17, 26 - 26, 17, 7, 22, 23, 9, 1, 25, 3, 7, 5 - 3, 0, 0, 23, 26 -
7, 24, 5, 17, 14, 2, 0, 12 - 7, 29, 0, 25, 24 - 13, 6, 3, 11, 24 -
0, 25, 24, 3, 7, 19, 10 - 23, 12, 9, 17, 0 - 15, 24, 7, 10, 12, 23, 11, 22, 6,
10 - 13, 7, 17, 15, 23, 12, 23, 17, 9, 12, 29, 17, 7 - 12, 23, 4, 26, 24,
22, 12, I will be very carefull of it.

I have the honour to be,
with great respect,

Sr,

Your most Obedient &
Most humble Servant.

Conrad



U. S. SHIP OF THE LINE PENNSYLVANIA, 140 Guns.

British cipher

Polyalphabetic using 3 alphabets of numbers from 00 to 30.

All numbers above 30 were nulls, which were used liberally.

Use first alphabet for 10 lines. Use second alphabet for 4 more lines. Use third alphabet for 3 lines. Repeat. Mark each change with a] bracket.

Since the first 10 lines all used the same alphabet Lovell could treat it as a simple substitution with nulls. Where that stopped working, treat the next 4 lines as another simple substitution.

19th Century

The end of the Black Chambers.

Public and parliaments protest against governments opening private mail.

American Decyphering Bureau closes in 1844. Lovell and Willes pensioned off.

Vienna Geheime Kabinets-Kanzlei closes in 1848.

Fertig.

The Telegraph

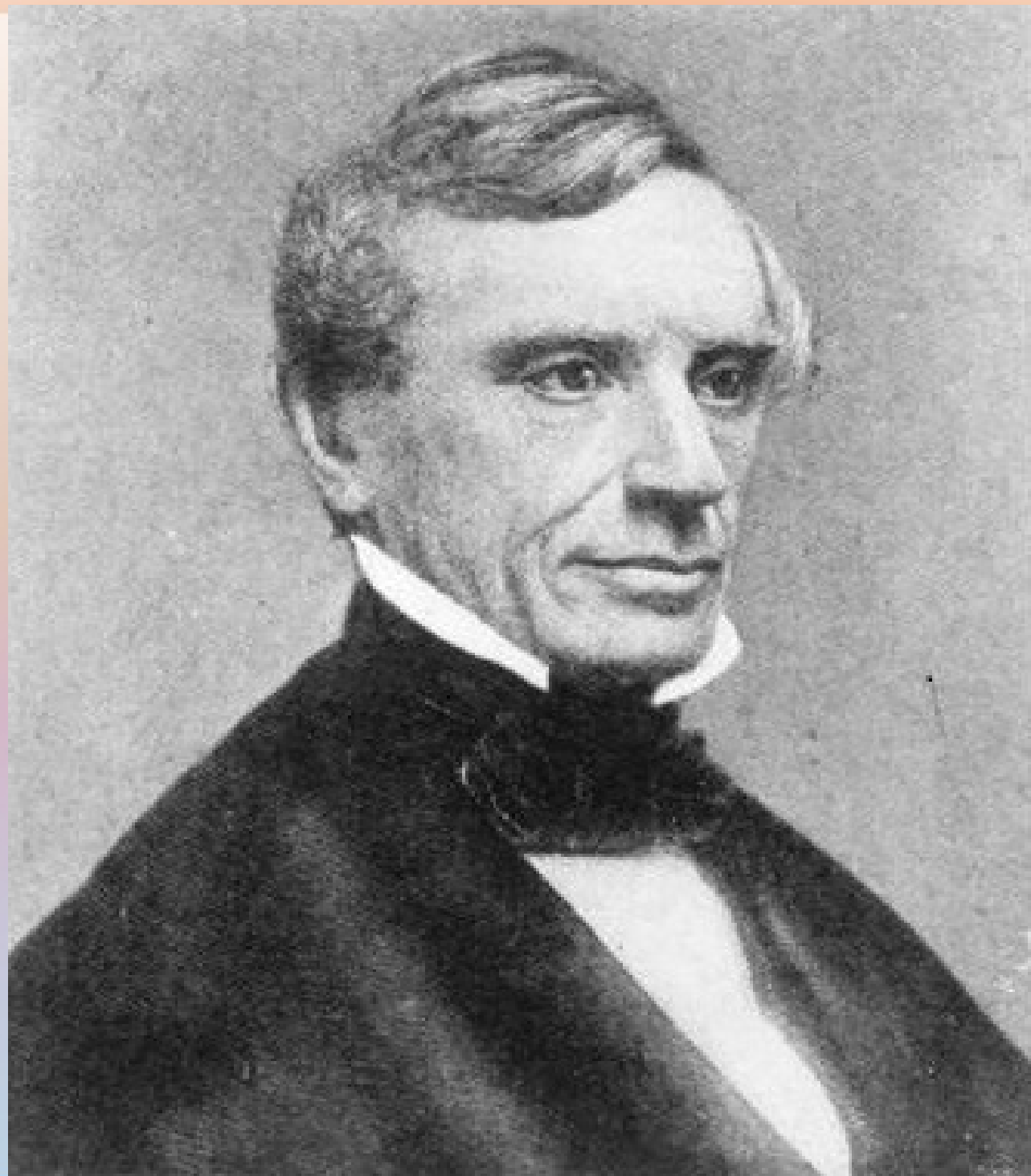
The telegraph was invented by Baron Pavel Schilling in 1832. He demonstrated the system between two rooms in his apartment. He also invented the concept of a binary code for transmission.

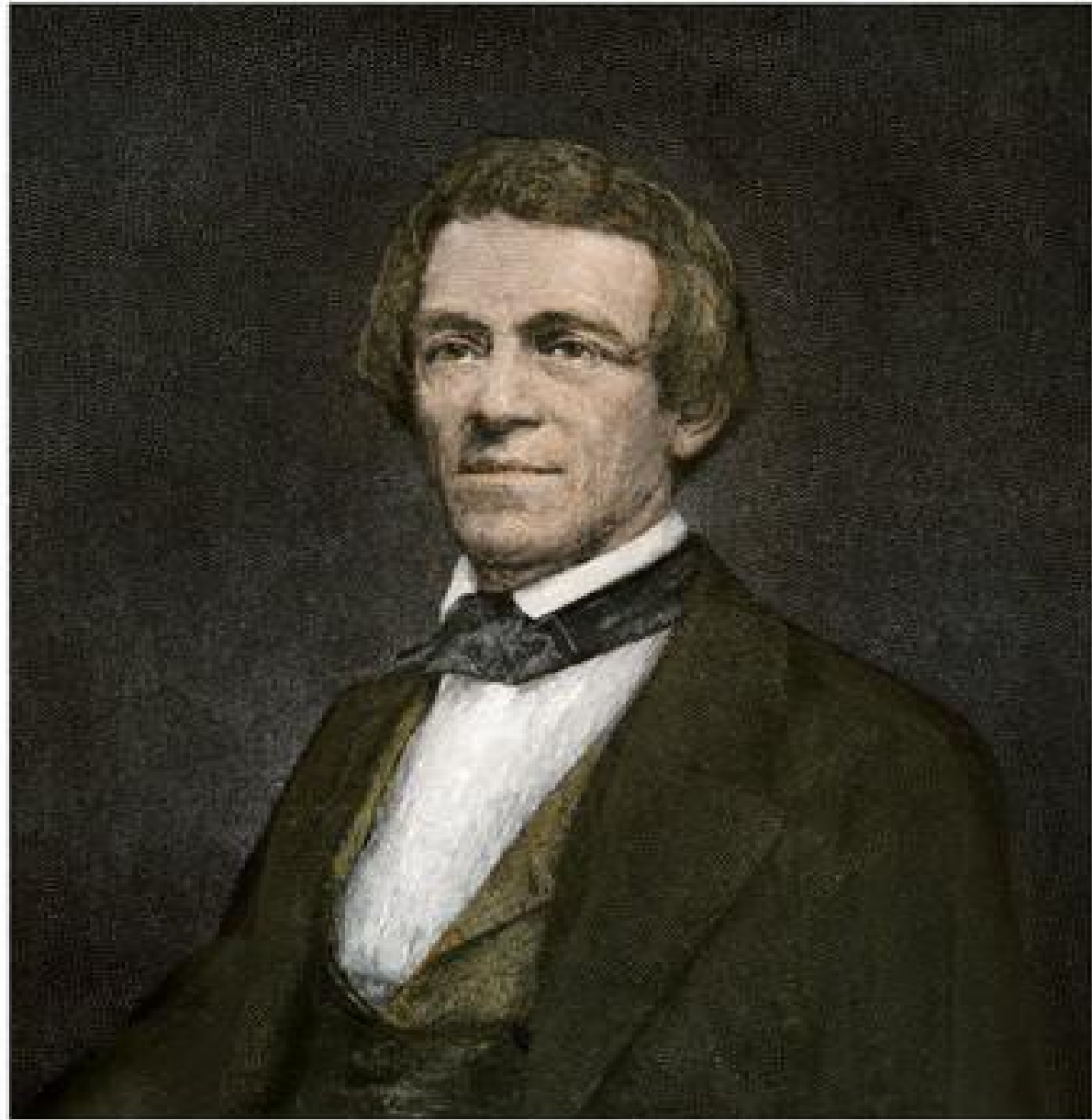
The first commercial telegraph system was set up by Sir Charles Wheatstone and William Cooke in 1837. By 1852 they had 2200 miles of wires in Britain.

Samuel F. B. Morse patents his telegraph in 1837.

Alfred Vail invents the “Morse” code.

The Morse apparatus becomes the world standard (except Britain) in 1851.





Wheatstone telegraph



The Telegraph

The era of codes begins.

At first everyone is concerned about privacy, since five or more clerks handle each telegraph message.

Francis O. J. Smith, Morse's lawyer and publicist, brings out *The Secret Corresponding Vocabulary*, about 50,000 words, but only 67 phrases.

Real value is economy. Later codes contain about 5,000 words but 50,000 phrases.

Codes

Nomenclators were the first codes. One letter, syllable, word or phrase is replaced by a code word.

One part and two part.

Numeric 614, 27-19, 306.14

Alphabetic BC, MRPT, CF:WA

Words ABLE, COMMA, PARIS

Artificial words MANOTIC, CARAVET, DIOFEAN

Using words or artificial words reduced telegraph errors.

Military use

Military commanders begin using the telegraph to control armies spread over wide areas. Command posts become communications hubs.

Telegraph is easily tapped. Codes and nomenclators can be captured. Field ciphers are needed.

Vigenère fills the bill. Fits on one page, easy to change keys, easy to correct garbles via telegraph.

Until 1863 considered unbreakable.

Maj. Friedrich W. Kasiski

1805-1881 Prussian infantry officer.

In 1863 publishes a book *Secret Writing and Deciphering* giving the general method for attacking a polyalphabetic cipher.

Find repeated groups of letters and note their positions. They are often common words enciphered with the same portion of the key. The distance between them will be a multiple of the key length.

Factor these distances and look for common factors.

Example:

Suppose CWB occurs at position 40 and again at position 103. The difference is 63, which factors to $3 \times 3 \times 7$. This suggests possible key lengths 3, 7, 9 or 21.

Suppose that PFO occurs at position 71 and again at 211. The difference is 140, which factors into $2 \times 2 \times 5 \times 7$. This suggests key lengths of 2, 4, 7, 10, 14, 20, 28 or 35.

The only key length that fits both cases is 7.

In general, the factor that occurs most often will be the correct period (key length).

Once the period P is known, the cipher is reduced to P simple substitutions.

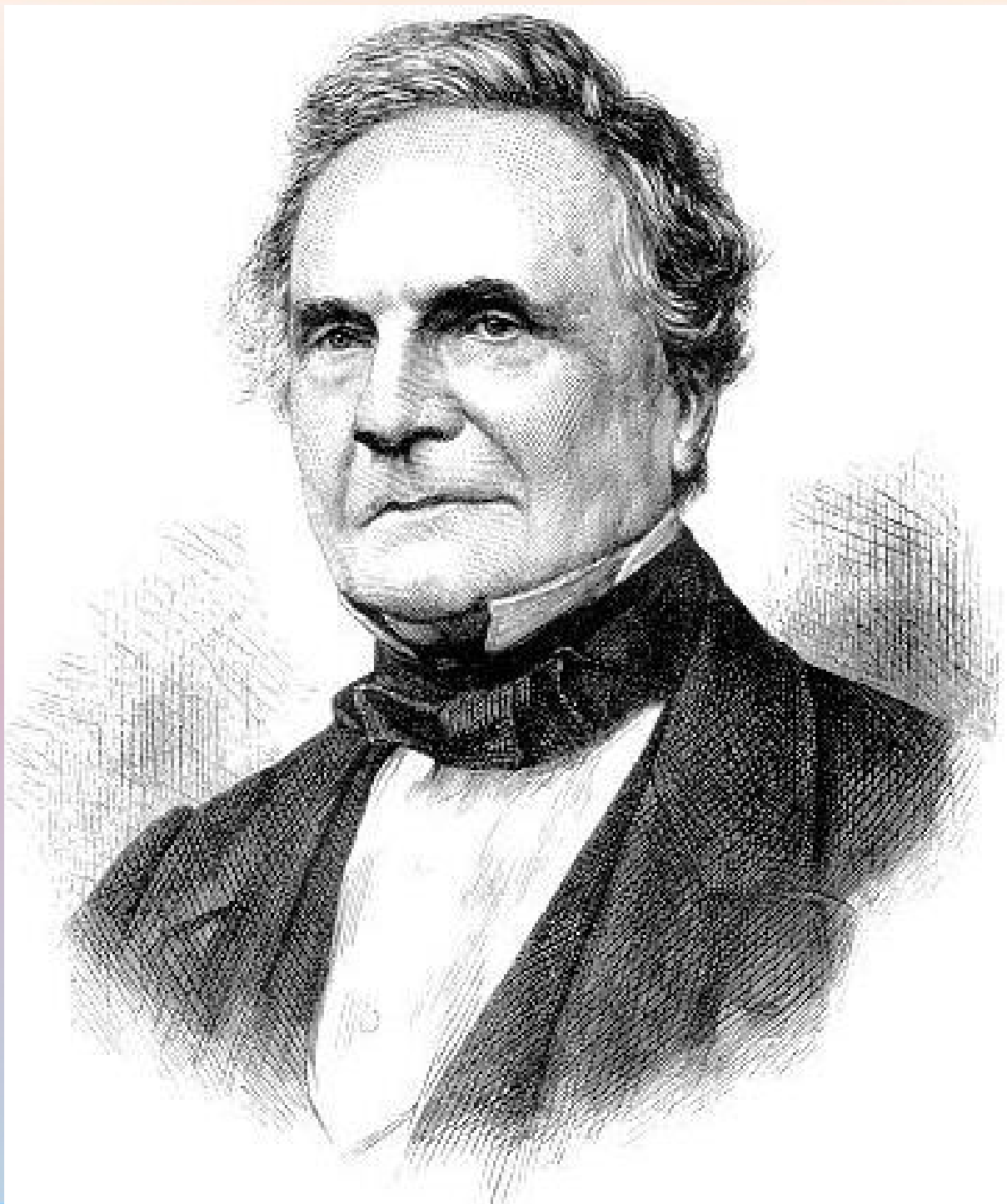
Some characteristics of the letters remain the same as for a single alphabet.

Vowels still tend to be high-frequency and have a wide variety of contacts on both sides.

When a few vowels are identified, the letters they contact on either side are probably consonants.

N is still usually preceded by a vowel and followed by a consonant. R is still usually preceded by a consonant and followed by a vowel.

Once the vowels and consonants are separated and a few letters are identified the solution follows easily.



Jefferson Cypher Wheel

Invented by Thomas Jefferson circa 1790-3.

Also called multiplex cipher.

A set of disks mounted on a rod so that they can turn independently. Each disk has a mixed alphabet written on its outer edge.


The disks are numbered, and the order of the disks on the rod is the secret key.

The message is spelled out by turning each disk in order to line up the letters in one row.

The ciphertext can be read out from any of the other 25 rows on the device.

Jefferson Cypher Wheel



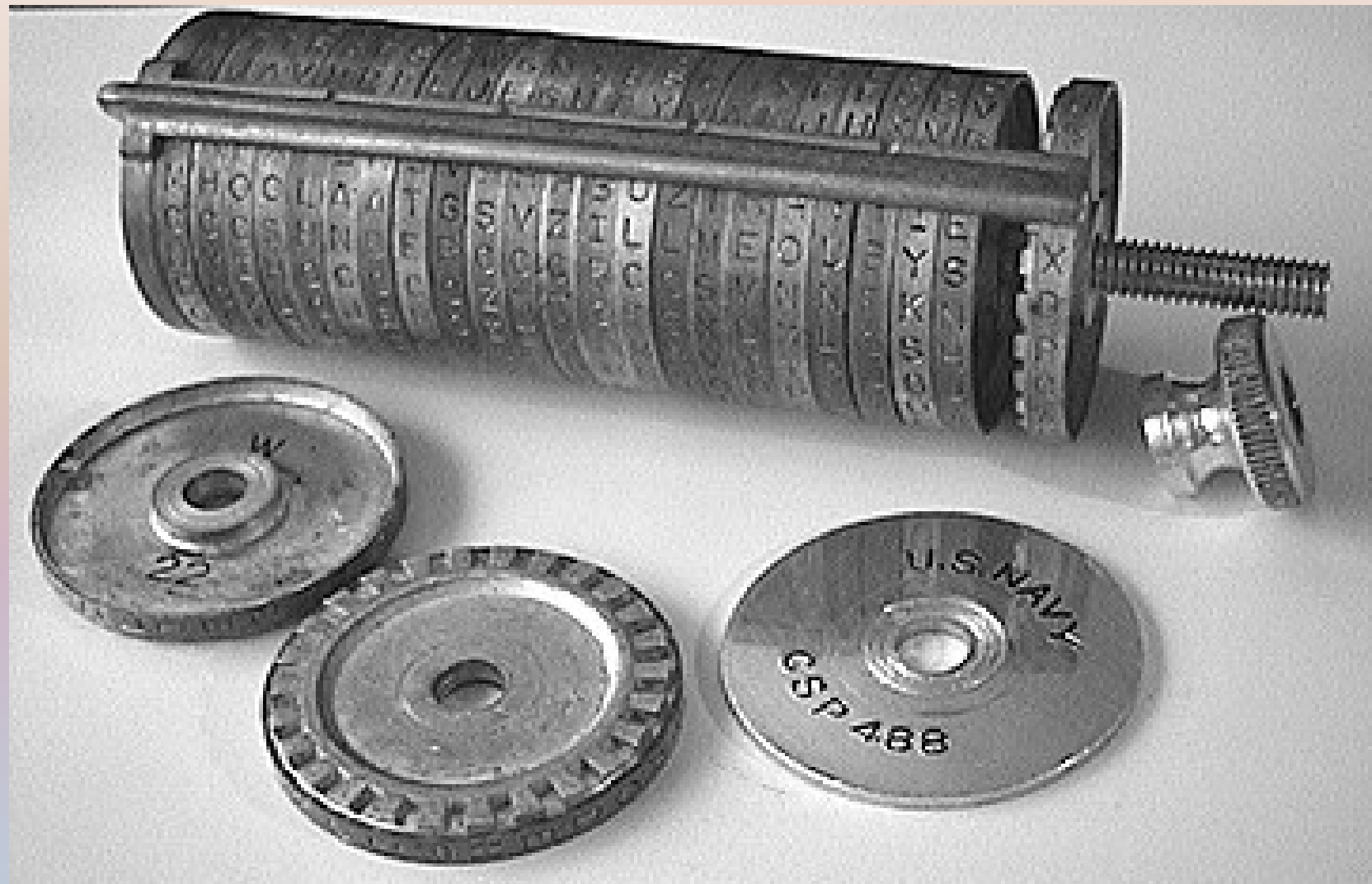
The image displays the components of Jefferson's Wheel Cipher. At the top is a cylindrical wooden cipher wheel with a brass axle and a brass knob. The wheel is divided into 26 vertical columns, each containing a different permutation of the alphabet. Below the wheel are four circular wooden discs, numbered 1 through 4, each with a central hole. To the left of the wheel is a small brass knob. The entire setup is on a light-colored surface.

Jefferson's Wheel Cipher

Signal Corps M94 version



Naval version, partly disassembled



Toys Я Us version



Gripenstierna cylinder

The Jefferson wheel had a forerunner invented by Fredrik Gripenstierna (1728–1804) in 1786.

It was a cipher cylinder with 57 disks constructed for King Gustav III of Sweden.

The 57 disks had a fixed order, so there was no key.

The King would enter the message on his side and the clerk would copy out the message (reading upside down and backwards) from the opposite side.

Flat version

In 1916 Col. Parker Hitt (US 1873-1971) invented a flat version of the cylinder using paper strips instead of disks.

This meant that new strips could be made in the field.

This device was called the M138 cipher machine (25 slots, 25 strips) and later the M138A machine (30 slots, 100 strips).

The Naval version was known as Venus.

These machines were used until about 1960.

SIGNAL CORPS U.S. ARMY

CIPHER DEVICE M-138-A

1-11-43
100

100

A large metal frame containing numerous horizontal strips of paper, each with a sequence of letters. The strips are arranged in two main sections, separated by a horizontal bar. On the left side, several strips are partially visible, with numbers and letters written on them: 19 K X Y, 20 B, 22 J R L, 24 W T, 26 P A Y, 28 K, 30 J, 32 X L, 34 F U O I P. The strips themselves contain various letter sequences, such as "U S E R A T O R C R O S E R D U M P R V", "K E E D O X S P A T A R K C R O S E R D U M P R V", "R E M N S B A X L E D E C F P S E C R T O Y", "H E R N J E R A D L G E D T P P S I C A Q", "O D J F Y T N H T O R E O L R E S H A S C", "X I E R F F Y V E T R A T O R S E L L A R P P A R C H", "J R C E M Q V S E P F R E T H T U A", "Z L E K T I R E N H A S C C F R L Y E R T F O O C", "D L A V V I C I P H S E C R P P T P P", "L E E E E P T T E T V G R A B C Y H B E V D H", "P L E E K E V I I P G S A K D P A R K A R", "Z B S E E P S E C I Z H T Y Q A T Y H L A K D", "W J U S C E P A S C I R E P P E R T Y R A R", "D E W F I C E T L M D U T Y G H P Q R A R", "A C C E R F I C E T L M D U T Y R A P P A R A R", "W E T E S J R C I R Y L P H A T R P E R D E E", "C U T R G J C O R N E L K A R T E R A R", "T R E M T O L E C V O R E E P T E R E C A R R Y", "S Y N T H E L C O U R E B Y T E H H A R Y", "R O P T I O E M T R O G Y A R F L Z Z E A", "W U R T I O E M T R O G Y A R F L Z Z E A", "Y T E R E C C R A C E P P L E R E T T E E", "Y T E R E C C R A C E P P L E R E T T E E", "O B E R T J E P O P Y E L C R T R E S S", "H A P E R E R T J E P O P Y E L C R T R E S S", "V G A N E P O L Y O N Y C A U T I R", "H A L E R E R T J E P O P Y E L C R T R E S S", "E N Y I M E R S U L L E T C E W E P T O R", "Y T A C K E R E R T J E P O P Y E L C R T R E S S", "D E R Y E P T L P C M D L A N G Y V", "H U A P E R E R T J E P O P Y E L C R T R E S S", "K U T R E A L Y V E M S C E R T P L E A D E", "A L L I G A L Y T A R E R T J E P O P Y E L C R T R E S S", "S O R I E P Y T A E C E H U S E L Y A S", "K A Y T E R E R T J E P O P Y E L C R T R E S S", "R A U Y E T A R R Y T R E M D L L A N G E", "C O S T A G E R E R T J E P O P Y E L C R T R E S S", "D C E I P Z H L E M E U D Y T E R Y A R", "L A P E L L E R E R T J E P O P Y E L C R T R E S S", "E K E J U P O R R H I G A T C A L C E Y", "V O A R E R E R T J E P O P Y E L C R T R E S S", "T O M A M A Y T R E S C E J E V T E R", "E L O U P O R E R T J E P O P Y E L C R T R E S S", "D E M A A R E R O S E L C N E S S A L Y E", "L A G A T E R E R T J E P O P Y E L C R T R E S S", "A R T O C E R E M L P A T O R S U S W C", "L L E C A T E R E R T J E P O P Y E L C R T R E S S", "K E L C H A T J O R T", "L L E C A T E R E R T J E P O P Y E L C R T R E S S", "Y O R E P C E P R O D I E L E C T R Y", "L L E C A T E R E R T J E P O P Y E L C R T R E S S"

M - 138 - A
 Strip Cipher
 1930's - 1960's

How to solve it

Computer solution by Frank Rubin, 1978.

Assume: you have a copy of the device and an intercepted message, but you do not know the key, that is, the order of the disks or strips.

Try all possible combinations for the first 2 disks.

For each line of the message, look at the 25 bigrams. Multiply the probabilities for the most-probable of the 25 bigrams (or add their logarithms).

Choose the most-probable 5% of these and try all possibilities for the third disk or strip.

Multiply the bigram probabilities for the contacts between the second and third disk. Take the most-probable 5% of these. You are now working with just $.05 \times .05$, or $\frac{1}{4}$ of 1% of the possible arrangements. (Or, use trigram frequencies.)

Try all possible fourth disks. Multiply the contact probabilities between the third and fourth disk.

By this point common words will start to appear on some of the lines. This will help narrow down the possibilities. At this stage you can narrow it down the top .001% of all the arrangements.

And so forth.

Charles Wheatstone

England 1802-1875.

Invented English concertina, automatic telegraph, stereoscope, spectroscope and spectral lines, and the Wheatstone bridge for measuring electrical resistance.

Built the first commercial telegraph line in 1837.

Invented Wheatstone cryptograph and Playfair cipher.

Wheatstone's friend Lyon Playfair was a professor of chemistry, Postmaster General, baron.

Advocated Playfair cipher, also use of poison gas in Crimean War.





Wheatstone Cryptograph



Danish military version



Playfair cipher

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

Rectangle: use opposite corners.

Same row: use letter to the right.

Same column: use letter below.

Break up double letters. Use **fo lx lo w** for **fo ll ow**

an->MK **fr->BW** **do->OV** **ru->UV**

How to solve

Long repeated sequences represent common words.

Repeated bigrams represent the most common bigrams
TH, HE, ER, IN, AN, etc.

Reversals are common pairs, ER/RE, ON/NO, TR/RT

When you have a letter and its substitute, they are probably on the same row in the square. For example if XQ represents TH then X is probably on the same row as T, and Q on the row with H.

There are only 5 possible substitutes for each letter of the alphabet (4 in same row, 1 below).

Letters will not appear equally often. Letters in rows with several high-frequency letters get used more often.

Letters that appear most often in the ciphertext are the ones in the same row as high-frequency letters.

This makes it possible to separate letters that appear in the same row. After you have identified the 5 most-frequent letters as a row, the next 5 most-frequent are likely another row.

Look for bigrams that come from just those 2 rows.

This will help sort out positions within those rows.

Digraph substitution

Playfair is a special case of digraph substitution, where pairs of letters are replaced. That is, simple substitution on letter pairs.

Uses a fixed 26×26 tableau of letter pairs.

Too big to mix the tableau, but can change the alphabets along the top or left.

Solved like a nomenclator.

A B C D E F G H I J ...

A BY DN ZT MD EA EK BR GU XF QR

B EM YM QS EW HQ CL FA LC CO EZ

C DC MI GA EN ZA UC DW TA BT UI

D HB XB DQ FP NO XB PP DL GY FI

E AZ RC FC HS DH ZO EC GI VN GM

F DS HE DF GB YK TH XC TE ET EF

G EG YA RF EV HO BE LA FD ST WJ

H RG FO CC DU EJ CH GC SN DM SV

...

Civil War

The North used primarily word transpositions, invented by Union telegraph operator Anson Stager, later a cofounder of Western Union.

Stager noticed that cipher groups like BNCGXG or Y7G6P4 often got garbled, but normal words were usually sent accurately.

They combined the transposition with the use of nulls and codes for key people, places, etc.

By the end of the war the North had dozens of routes, and a code book of 1608 terms covering 36 pages.



BE AT THE MAIN FIELD TENT
NOON TODAY FOR NEWS ON THE
SIEGE AT FORT YORK GENL LEE
MUST BE SENT BACK TO VA
WITH HIS HEAD HELD LOW

BE NOON SIEGE MUST WITH AT TODAY AT
BE HIS THE FOR FORT SENT HEAD MAIN
NEWS YORK BACK HELD FIELD ON GENL TO
LOW TENT THE LEE VA

The South used many systems, but relied chiefly on Vigenère using tableau and cipher disk. They used only 3 keys for the whole Civil War, namely MANCHESTER BLUFF, COMPLETE VICTORY, and COME RETRIBUTION (last 2 months only).

The North read these easily, although it often took too long for tactical situations.

The South never penetrated the word transpositions (they even published some in their newspapers), though the North sent 6,500,000 such messages, and on at least 2 occasions the South captured the North's code book.

The North simply issued new code books.

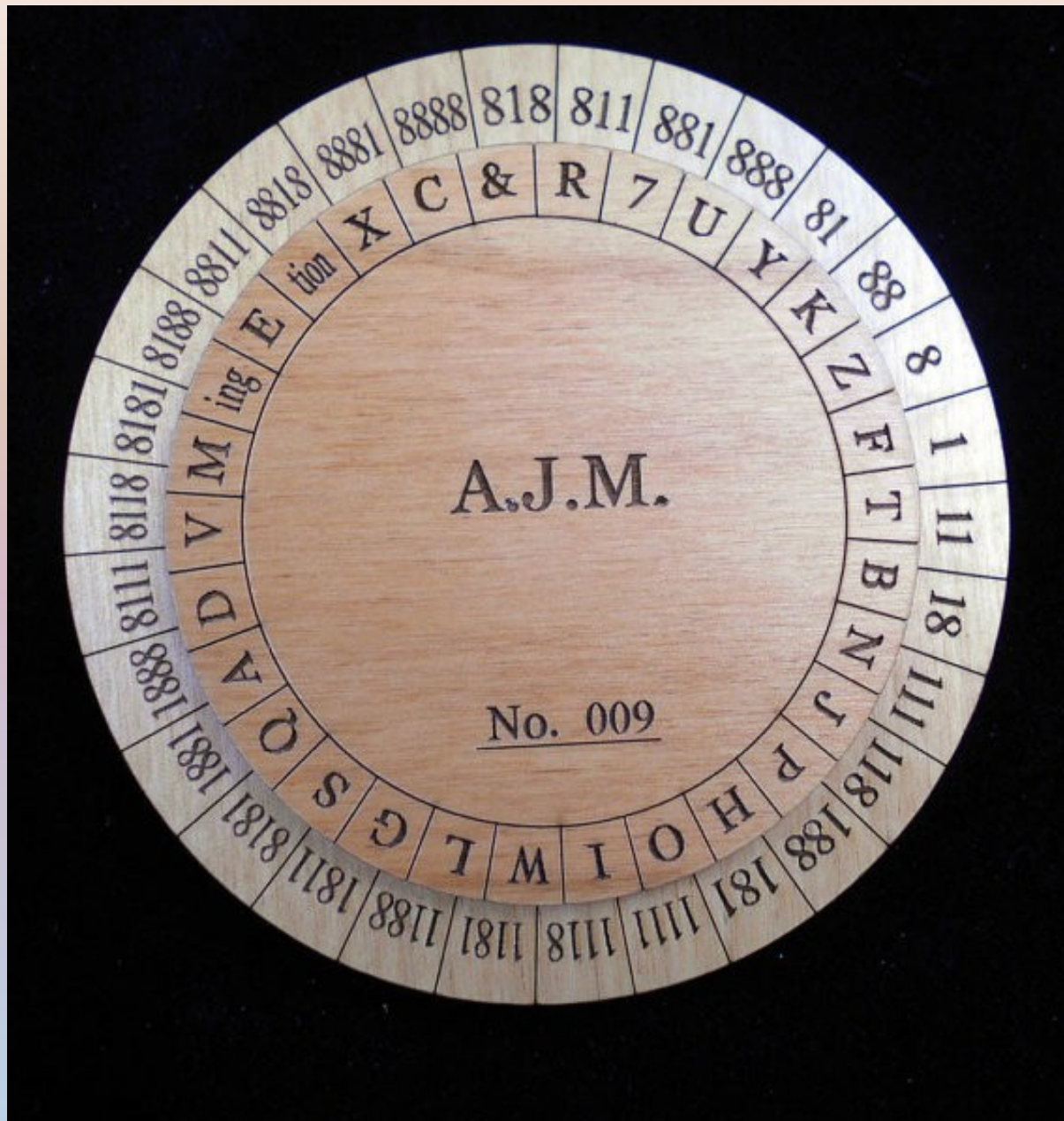
Confederate cipher disk



Mexican Army cipher disk



Union cipher disk



Auguste Kerckhoffs

*Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs
von Nieuwenhof*

French 1835-1903.

Professor of German, English, Latin, Greek, Italian,
history and mathematics.

Books on Flemish, English, German, drama and
religious art.

Advocate of Volapük, an artificial language invented
by Johann Martin Schleyer.

Wrote *La Cryptographie Militaire*, first book on
cryptanalysis, circa 1882.



Six Principles

For a military field cipher:

1. Unbreakable, at least in practice.
2. ... even if the enemy learns the system.
3. Key easy to remember (without notes!) and change.
4. Transmissible by telegraph.
5. Apparatus and documents easily carried by 1 person.
6. Easy to use; no complex rules or computations.

Only cryptographers are qualified to judge the security of a cipher.

Superposition

Suppose you know that the opponent uses a tableau,
and always uses the same key, too long for Kasiski.

AMNETRUPULMWYDCV . . .

UROTVKLECXTRXFC . . .

AMNWOAHTVKXCRPLN . . .

RMIBCGUIULTGEWDC . . .

ASFTEYIOAEVMUSCE . . .

KPLTZQITULVOADPL . . .

Doubling up

If the cryptanalyst can determine (by matching up the frequency distributions) that two columns were enciphered by the same key letter, then there is twice as much material to work with.

Suppose there are 100 columns. There are only 26 key letters, so each one must be used roughly 4 times.

If there are two consecutive columns using the same two alphabets, then there may be repeated bigrams .

Kerckhoffs also gave some rules for reconstructing the tableau, but this works only when each row is a simple shift from the one above.

France leads

After Kerckhoff's book France became the leading cryptographic nation.

Over the next 25 years 4 cryptographers led France's cryptographic efforts, Gaetan de Viaris, Paul Valério, Felix Delastelle, and Étienne Bazeries.

A few of their inventions are especially noteworthy.

Felix Marie Delastelle invented the Bifid, Trifid and FourSquare ciphers.

Bifid

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

A T T A C K F O R T S M I T H

2 1 1 2 2 2 3 4 5 1 1 2 1 1 5

1 4 4 1 2 3 5 1 4 4 1 5 3 4 3

A T T A C K F O R T S M I T H

2 1 1 2 2 2 3 4 5 1 1 2 1 1 5

1 4 4 1 2 3 5 1 4 4 1 5 3 4 3

21=A 12=B 21=A 44=G 12=B ABAGB

23=K 45=Q 13=I 51=X 44=G KQIXG

12=B 11=S 51=X 53=H 43=L BSXHL

ABAGB KQIXG BSXHL

Weakness

A B C D E

A1 B1 C1 D1 E1

A2 B2 C2 D2 E2

A1B1 C1D1 E1A2 B2C2 D2E2

If **B1=A2** then the first ciphertext letter will be **A**.

If **D1=C2** then the second ciphertext letter will be **C**.

If **A1=E2** then the third ciphertext letter will be **E**.

If **E1=A1** then the third ciphertext letter will be **A**. etc.

There is better than 20% chance that any given plaintext letter will appear in the ciphertext.

Trifid

	<u>D</u>	<u>E</u>	<u>C</u>	<u>A</u>	<u>D</u>	<u>E</u>
111-B						
112-E	1	1	1	1	1	1
113-A	2	1	2	1	2	1
121-D	1	2	2	3	1	2
122-C						

111-B, 111-B, 212-L, 121-D, 122-C, 312-W

BBLDCW

FourSquare

ABCDE MijXED

FGHIJK ABCFG

LMNOP HKLNO

QRSTU PQRST

VWXYZ UVWYZ

ALPHB ABCDE

ETMRW FGHIJK

CGNSX LMNOP

DijOUY QRSTU

FKQVZ VWXYZ

FO UR SQ UA RE

FC QY PO PB TL

Étienne Bazeries

French 1846 to 1931.

Natural cryptanalyst, nasty disposition.

Invented improved version of Jefferson cylinder that became the M94 military cipher.

Circa 1890 invented a simple substitution plus transposition cipher.

Example with key 3-2-4.

abcdefghijklmnopqrstuvwxyz

plain

GFDCBSAMPLEZYXWVUTRQONKJIH

cipher

3

2

4

3

2

M E E

T M

E I N S

T L O

U I S

E E M

M T

S N I E

O L T

I U S

B B Y

Y Q

R X P B

W Z Q

P O R

BBYYQ RXPBW ZQPOR

Rosario Candela, *The Military Cipher of Commandant Bazeris*, 1938.

Fractionated Morse

M.E. Ohaver (Merle) proposed fractionated Morse about 1910.

S A M P L E

. . . / . - / - - / . - - . / . - . . / .

3 2 2 4 4 1

1 4 4 2 2 3

. / . . . - / - - . - / - . / . - / . . .

E V Q N A S

EVQNAS

The standard Morse alphabet is used for both the expansion and compression steps.

Morse code provides 30 codes of 1 to 4 dots and dashes, but there are only 26 letters, so 4 extra characters are needed. Ohaver used German vowels ä, ë, ö, ü.

The only key is the block length (period), so there is negligible security.

There are two ways these problems can be overcome.

Morse 26

Use only 1, 3 and 4 symbol Morse groups, total 26.

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

A T T A C K

-/.-.-/.-.-/-/-..-.-.-/

1 4 4 1 3 4

4 3 1 4 4 1

-.-./-.-././-.-.-./.-.-./-/-

J O S F U A

JOSFUA