

Antiquity

500-600BC ATBASH Cipher (reverse alphabet)

Aleph Beth Yod Kaph

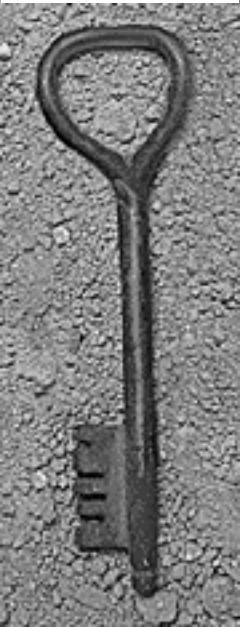
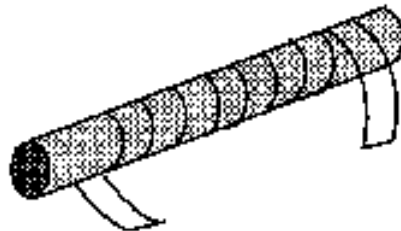
כא ... כי

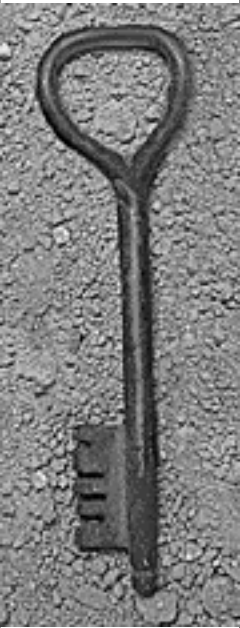
שת ... למ

babel -> SHESHACH

Taw Shin Mem Lamed

487BC Skytale (Transposition Cipher)





Polybius' Cipher

	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

- Bipartite substitution cipher
- Prisoner's Cipher (see Koestler's Darkness at Noon)
- Nihilist cipher based on it

331515143234331554

Caesar's Cipher

40-50BC Caesar Cipher (Substitution Cipher)

omnia gallia est divisa in partes tres



RPQLD JDOOLD HVW GLYLV D LQ SDUWHV WUHV

- First cipher documented in military use.
- Generalization (with shift other than 3, also sometimes, inaccurately, called Caesar Cipher)



Modern Beginnings

700AD

Al-Khalīl: use of a crib

1412AD

Al-Qalqashandi: frequency analysis



Nomenclators

Early code/cipher, popular form 1400s-1800s.

Philip of Spain (1589, see Kahn):

LO = Spain

POM = King of Spain

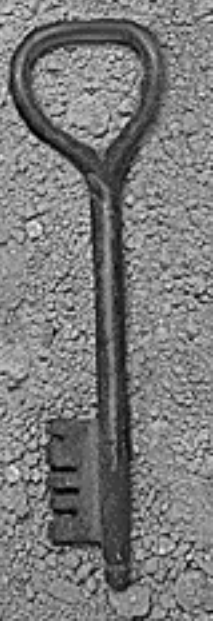
64 = confederation

overlined two-digit groups = null

+ substitution cipher with homophones

Nomenclator Example

Nomenclator used by Mary, Queen of Scots
in 1586 in the plot against Elizabeth I



a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z
○	‡	∧	‡	α	□	θ	∞	ι	ō	κ	∥	∅	∇	∫	∩	∪	Δ	ε	⊂	7	8	9

Nulles ff. — . — . d. Dowbleth σ

and for with that if but where as of the from by
2 3 4 4 4 3 2 2 2 2 2 2 2

so not when there this in wich is what say me my myrt
2 X † † † 6 x † 2 m n m m d

send lre receave bearer I pray you Mte your name myne
1 2 † T 1 1 1 2 2 2

Taken from Simon Singh. The Code Book.

Alberti's Cipher Disk

Invented by Leon Battista Alberti in 1460s.



Correspondents agree on index letter on inner disk.

Key: corresponding letter on outer disk.

Key can change during encryption (polyalphabetic cipher)



Johannes Trithemius

Polygraphiae, 1518

First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key

abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyz
cdefghijklmnopqrstuvwxyzab
Defghijklmnopqrstuvwxyzabc

. . .

Ave Maria Code

a	deus	a	clemens
b	creator	b	clementissimus
c	conditor	c	pius
d	opisex	d	pijssimus
e	dominus	e	magnus
f	dominator	f	excelsus
g	consolator	g	maximus
h	arbiter	h	optimus

Bacon's Biliteral cipher

*Wisdom and understanding
are more to be
desired than riches*

A	B	C	D	E	F
Aaaaa	aaaab	aaaba	aaabb	aabaa	aabab
G	H	I	K	L	M
aabba	aabbb	abaaa	abaab	ababa	ababb
N	O	P	Q	R	S
abbaa	abbab	abbba	abbbb	baaaa	baaab
T	V	W	X	Y	Z
baaba	baabb	babaa	babab	babba	babbb

a. b. a. b. a. b. a. b. a. b. a. b. a. b.
 { A. B. a. a. B. B. b. b. C. C. c. D. D. d.

a. b. a. b. a. b. a. b. a. b. a. b. a. b.
 { E. E. e. F. F. f. G. G. g. H. H. h.

a. b. a. b. a. b. a. b. a. b. a. b. a. b.
 { I. I. i. K. K. k. L. L. l. M. M. m.

a. b. a. b. a. b. a. b. a. b. a. b. a. b.
 { N. N. n. O. O. o. P. P. p. Q. Q. q. R.

b. a. b. a. b. a. b. a. b. a. b. a. b.
 { R. r. S. S. s. T. T. t. V. V. v. u. u.

a. b. a. b. a. b. a. b. a. b. a. b. a. b.
 { W. W. w. X. X. x. Y. Y. y. Z. Z. z.



Blaise de Vigenère

Traicté de Chiffres, 1585

Autokeys:

key	DA	UNO	MD	ELETERNE
plain	au	nom	de	l'eternel
cipher	XI	AHG	UP	TMLSHIXT

key	DX	HEE	CO	UMXGNABQ
plain	au	nom	de	l'eternel
cipher	XH	EEC	OU	MXGNABQO

Vigenère Cipher

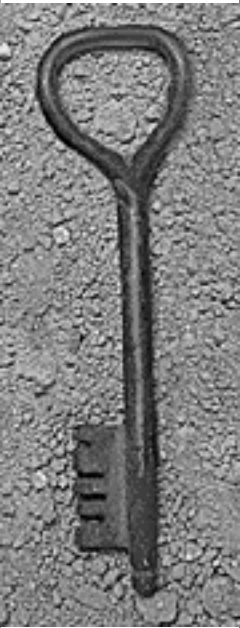
Thomas Jefferson

Wheel cipher (1790s)

- Polyalphabetic
- Mixed alphabets
- Key determines sequence of wheels

Reinvented by Parker Hitt (1913) and used by the military (M-138-A of WW-II)

<http://members.magnet.at/wilhelm.m.plotz/VirtualM94.html>



Wheatstone and Playfair

Playfair Cipher

- Invented by Charles Wheatstone
- Publicized by Lyon Playfair in 1854
- First literal digraphic system
- Mixed alphabet, keyword
- Used in the Boer War (1899-1902)

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

cipher -> DRAEGI

abrupt -> BHIVFN





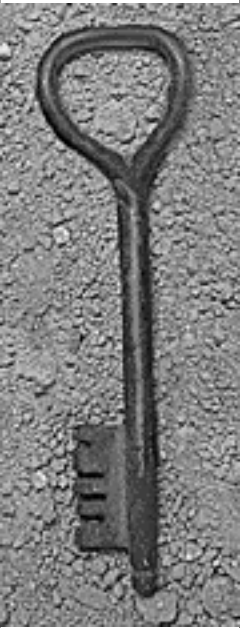
Friedrich W. Kasiski

Die Geheimschriften und die Dechiffirkunst, 1863

First general (published) solution to polyalphabetic cipher with repeating keyword (Vigenère cipher) using “Kasiski test”.

Babbage might have known solution earlier.

Cipher was still in use in WWI.



William Frederick Friedman

- Father of US cryptanalysis
- General solution to polyalphabetic ciphers using statistical methods (even with long repeating keys that defeat Kasiski's test)
- *Index of Coincidence, 1920*



ADFGVX

- Introduced by German intelligence as ADFGX in 1918.
- Combination of digraphic substitution and transposition (based on keyword)



Lester S. Hill

Cryptography in an Algebraic Alphabet, 1929

- Block substitution cipher
- Based on matrix algebra

Scherbius and the Enigma

- Rotor machine, 1923; similar machines invented, and patented, earlier, by Koch (Netherlands), Damm (Sweden), and Hebern (US)
- Used by Germans in WWII
- First broken by Rejewski (Poland), then in Bletchley Park by Turing and others.





Feistel Ciphers

- Type of block ciphers invented by Horst Feistel at IBM Watson Research labs in 60s. Works in binary, and is based on repeated substitution, transposition.
- Lucifer
- With modifications to S-boxes (substitution part), Lucifer is adopted as DES (Data Encryption Standard) by NSA



Diffie, Hellman, Merkle

New Directions in Cryptography, 1976

- First publication of public key cryptography in open literature
- Describes method allowing two parties to agree on a secret key using public channels



RSA

Rivest, Shamir, Adleman, 1977 find a mathematical way of implementing public-key cryptography: RSA.

Both Diffie/Hellman key exchange, and RSA was discovered earlier by British intelligence, but not published (or patented).



Quantum Cryptography

Charles Bennett, Gilles Brassard, 1990 develop quantum cryptography, using quantum physics to secure a channel.



AES

In 2001 Rijndael is adopted as AES (Advanced Encryption Standard), replacing DES as the accepted government standard for secure communication.