Atbash

500-600BC ATBASH Cipher (reverse alphabet)

Aleph Beth Yod Kaph

. . .

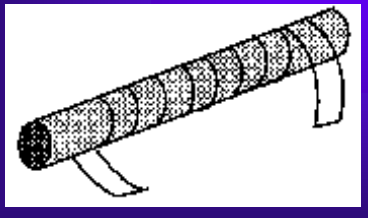
babel -> SHESHACH

. . .

Taw Shin Mem Lamed

Skytale

487BC Skytale or scytale (σκυτάλε)



WCTAEHSHRDELEDNADBLSOLITOOLIROANYM

Xerxes and Secrecy

480 Xerxes has assembled army to attack Greece

Demaratus sends message hidden under wax of writing tablet.

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

33151514323433155 4

- 200 BC
- used with torches in antiquity
- Bipartite substitution cipher
- Prisoner's Cipher (see Koestler's Darkness at Noon)
- Nihilist cipher based on it

Substitution and Transposition

Two basic methods of encryption

Substitution

- Replace letter/symbol/text with other letter/symbol/text
- leads to *confusion*

Transposition

- Rearrange the order of letters/symbols in the text
- leads to *diffusion*

Caesar's Cipher

40-50BC Caesar Cipher (Substitution Cipher)

```
omnia gallia est divisa in partes tres
                  ↓
RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV
```

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

Modern Beginnings

600 AD — Widespread use of monoalphabetic substitution ciphers for administrative use

700 AD — Al-Khalīl (philologist): use of a crib (In the name of God)

900 AD Al-Kindī: "A Manuscript on Deciphering Cryptographic Messages" (first systematic description of using frequency analysis to break a substitution cipher)

Taken from Simon Singh. The Code Book.

Frequency Analysis

1412 AD — Al-Qalqashandi: detailed description of frequency analysis in Arabic based on earlier writings by Ibn ad-Duraihim (1300 AD)

"When you want to solve a message which you have received in code, begin first of all by counting the letters, and then count how many times each symbol is repeated and set down the totals individually." ...

"When you see that one letter occurs in the message more often than the rest, then assume that it is alif; then assume that the next most frequent is lām."

Nomenclators

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

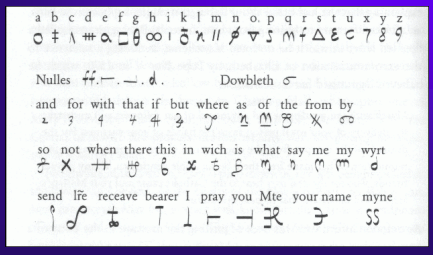
Philip of Spain (1589, see Kahn):

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



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

Johannes Trithemius

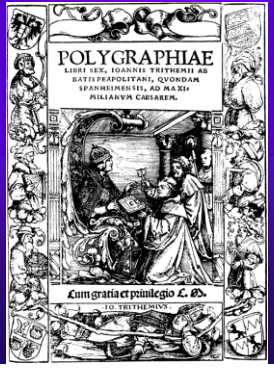
1462-1516, Germany

Polygraphiae, 1518
First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key

Steganographia, 1606

- hidden writing



Polygraphiae I

Ave Maria Cipher

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

1st page of Ave Maria Cipher, taken from the first book of the Polygraphiae

Steganographia

Begun in 1499; published posthumously in 1606

```
Parmesiel Oshurmi Delmuson Thafloin
          s u m           t a l i

Peano Charustrea Melany Lyamunto
      c a u t e         l a u t
```

Placed on Index Librorum Prohibitorum in 1609

"full of peril and superstition (M. A. Del Rio)

Polygraphiae II

Tabula recta, from the 6th book of the Polygraphiae.

Examples
- hunc caveto virum
- SUGKESUOAKATXO
- QUWWWQSGQSDZ

- Polyalphabetic substitution
- Progressive key

In hac tabula literarū canonica siue recta tot ex uno & usuali nostro latinarum literarum ipsarum per mutationem seu transpositionē habes alphabeta, quot in ea per totum sunt monogrammata, uidelicet quater & uigesies quatuor & uiginti, quæ faciunt in numero p. lxxvi. aperto tidē multiplicata, paulo efficiunt minus q. quatuordecē milia.

Giovan Batista Belaso

La cifra del. Sig. Giovan Batista Belaso, 1553

Idea: combine polyalphabeticity with keyword; that is, select cipher alphabet according to keyword

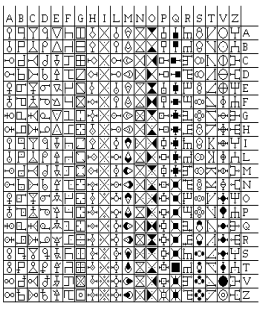
key	`viavia viaviav iaviav`
plaintext	`giovan batista belaso`
ciphertext	`bqoqin witdatv jegisj`

Only used standard alphabets (abcd...xyz)

Giovanni Battista Porta

De Furtivis Literarum Notis, 1563

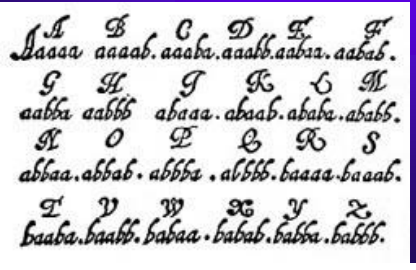
- Substitution/Transposition
- Digraphic Substitution
- symbol substitution
- Mixed polyalphabetic cipher
- crib



Bacon's Biliteral cipher I

1561-1626, England

First idea: encode letters in binary (1623)



Bacon's Biliteral cipher II

Wisdom and understanding are more to be desired than riches

Second idea: use two different typefaces to encode a/b decision.

Example:
tobeOrnottobeThaTIsThE Question

Girolamo Cardano

De Subtilitate, 1550; De Rerum Varietate, 1556

Autokeys:

key	SIC SICE SICERGOEL
plain	sic ergo elementic
cipher	NTF ZCLT ZVHRYVIPE

Problems?

Also invented the Cardano grille

Blaise de Vigenère

Traicté de Chiffres, 1585

Autokeys:

key	DA UNO MD ELETERNE
plain	au nom de leternel
cipher	XI AHG UP TMLSHIXT

key	DX HEE CO UMXGNABQ
plain	au nom de leternel
cipher	XH EEC OU MXGNABQO

Vigenére 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.aon.at/cipherclerk/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 Dechiffrirkunst, 1863

First general (published) solution to polyalphabetic cipher with repeating keyword (Vigenére 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*
- Breaking of Purple

ADFGX and ADFGVX

ADXDA XGFXG DAXXGX GDADFF GXDAG

- Invented by Fritz Nebel (1891-1967)
- Combination of digraphic substitution (like Polybius) and columnar transposition (based on keyword)
- Introduced by German intelligence as ADFGX in 1918 as a field cipher.
- Later, a sixth letter, V, was added: ADFGVX
- Fractional system

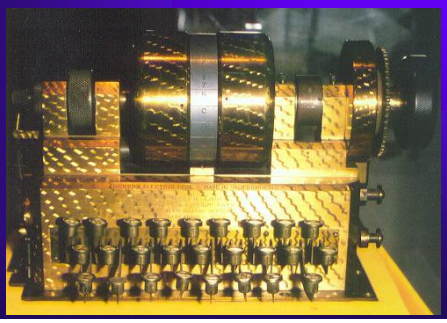
Lester S. Hill

Cryptography in an Algebraic Alphabet, 1929

- Block substitution cipher
- Based on matrix algebra

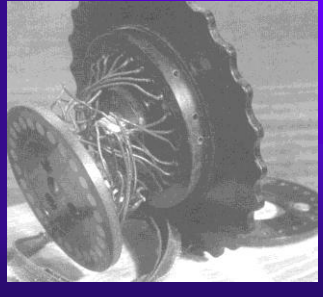
Hebern Single Rotor Machine

Patented by Edward Hebern in 1924 (filed 1921)



Rotors

Rotors



Wired inside to implement a (fixed) permutation.

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.

http://www.enigmaco.de/

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 US government in 1976

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.