Antiquity

500-600BC  ATBASH Cipher (reverse alphabet)

Aleph Beth   Yod Kaph
כ" før נא
לך ... שתה
babel -> SHESHACH

487BC  Skytale (Transposition Cipher)
Polybius’ Cipher

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>2</td>
<td>f</td>
<td>g</td>
<td>h</td>
<td>ij</td>
<td>k</td>
</tr>
<tr>
<td>3</td>
<td>l</td>
<td>m</td>
<td>n</td>
<td>o</td>
<td>p</td>
</tr>
<tr>
<td>4</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
</tr>
<tr>
<td>5</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
</tbody>
</table>

- 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 GLYLVD 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):

\[
\begin{align*}
\text{LO} &= \text{Spain} \\
\text{POM} &= \text{King of Spain} \\
64 &= \text{confederation} \\
\overline{64} &= \text{null} \\
\text{+ substitution cipher with homophones}
\end{align*}
\]
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 (polyalphabetic cipher)
Johannes Trithemius

Polygraphiae, 1518
First printed book on cryptography.

- Ave Maria Cipher
- Polyalphabetic substitution
- Progressive key

\[abcdefghijklmnopqrstuvwxyz\]
\[bcdefghijklmnopqrstuvwxyzacdefghijklmnopqrstuvwxyzab\]...

Ave Maria Code

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>deus</td>
<td>a</td>
<td>clemens</td>
</tr>
<tr>
<td>b</td>
<td>creator</td>
<td>b</td>
<td>clementissimus</td>
</tr>
<tr>
<td>c</td>
<td>conditor</td>
<td>c</td>
<td>pius</td>
</tr>
<tr>
<td>d</td>
<td>opisex</td>
<td>d</td>
<td>pijssimus</td>
</tr>
<tr>
<td>e</td>
<td>dominus</td>
<td>e</td>
<td>magnus</td>
</tr>
<tr>
<td>f</td>
<td>dominator</td>
<td>f</td>
<td>excelsus</td>
</tr>
<tr>
<td>g</td>
<td>consolator</td>
<td>g</td>
<td>maximus</td>
</tr>
<tr>
<td>h</td>
<td>arbiter</td>
<td>h</td>
<td>optimus</td>
</tr>
</tbody>
</table>
Giovanni Battista Porta

*De Furtivis Literarum Notis, 1563*

- Substitution/Transposition
- Digraphic Substitution
- Symbol substitution
- Mixed polyalphabetic cipher
Bacon’s Biliteral cipher

Wisdom and understanding are more to be desired than riches.
Blaise de Vigenère

Traicté de Chiffres, 1585

Autokeys:

<table>
<thead>
<tr>
<th>key</th>
<th>DA UNO MD ELETERNE</th>
</tr>
</thead>
<tbody>
<tr>
<td>plain</td>
<td>au nom de leternel</td>
</tr>
<tr>
<td>cipher</td>
<td>XI AHG UP TMLSHIXT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>key</th>
<th>DX HEE CO UMXGNABQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>plain</td>
<td>au nom de leternel</td>
</tr>
<tr>
<td>cipher</td>
<td>XH EEC OU MXGNABQO</td>
</tr>
</tbody>
</table>

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.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)

<table>
<thead>
<tr>
<th>P</th>
<th>L</th>
<th>A</th>
<th>Y</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>R</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>G</td>
<td>H</td>
<td>K</td>
<td>M</td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>Q</td>
<td>S</td>
<td>T</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Z</td>
</tr>
</tbody>
</table>

cipher -> DRAEGI
abrupt -> BHVFN
Friedrich W. Kasiski

Die Geheimschriften und die Dechiffrierkunst, 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*
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.

http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/enigma.html
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.