**Atbash**

500-600BC  \[\text{ATBASH Cipher (reverse alphabet)}\]

- Aleph Beth  Yod Kaph
- Shin Taw  Lamed Mem

**Skytale**

487BC  \[\text{Skytale or scytale (σκυτάλε)}\]

- WCTAEHSHRDELEDNADBLSOLIDOILROANYM

**Xerxes and Secrecy**

480 Xerxes has assembled army to attack Greece

Demaratus sends message hidden under wax of writing tablet.
Steganography and Cryptography

Steganography tries to hide the presence of message.
Cryptography tries to obscure the contents of the message.

Technical Steganography

- Message on silk in wax balls (ancient China)
- Xerxes
- Histiaeus (Herodotus)
- Invisible inks (at least 100AD)
- Giovanni Porta and the hardboiled egg (15th century)
- Hollow heels
- Spy coins
- Microdots

Linguistic Steganography

- Semagrams
- Francis Bacon
- Watermarking
- Open Code
- Weather Reports in *Breakfast at Tiffany’s*
- Velvalee Dickinson (“The Doll Woman”) (censorship)

“Robbers raided Honolulu with a scimitar hung all around its necks by their dirty belts until February.”
Linguistic Steganography

Polybius’ Cipher

200 BC

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

• Bipartite substitution cipher
• used with torches in antiquity
• 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 RUHV

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