

# Atbash

500-600BC    ATBASH Cipher (reverse alphabet)

Aleph Beth    Yod Kaph  
 כַּי ... אַב    babel -> SHESHACH  
 לַמ ... שְׁת    Taw Shin    Mem Lamed

---

---

---


---

---

---

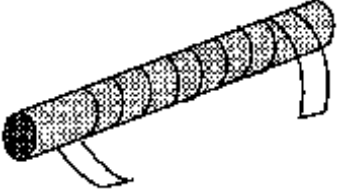
---

---



# Skytale

487BC    Skytale or scytale (σκυτάλε)



WCTAEHSHRDELEDNADBLSOLITOOIROANYM

---

---

---

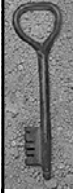
---

---

---

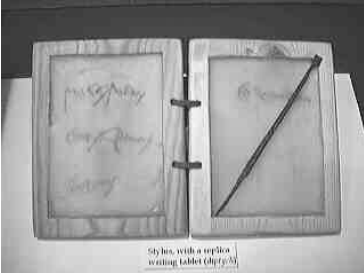
---

---



# Xerxes and Secrecy

480 Xerxes has assembled army to attack Greece



Demaratus sends message hidden under wax of writing tablet.

Scytale with a replica writing tablet (http://www.ancienthistory.org.uk)

---

---

---


---

---

---

---

---



## Steganography and Cryptography

στεγανος: covered  
 γραφειν: (to) write  
 κρυπτος: hidden

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  
 Histiaieus (Herodotus)  
 invisible inks (at least 100AD)  
 Giovanni Porta and the hardboiled egg (15<sup>th</sup> century)  
 hollow heels  
 frequency subband permutation  
 microdots

---

---

---


---

---

---

---

---



## Linguistic Steganography

Semagrams  
 Francis Bacon  
 Watermarking

Open Code  
 Weather Reports in *Breakfast at Tiffany's*  
 Velvlee Dickinson ("The Doll Woman")  
 (censorship)

"Although the Honolulu basketball game all  
 damages by their first, the first of February."

---

---

---

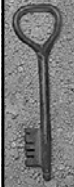
---

---

---

---

---



## Polybius' Cipher

200 BC

	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

331515143234331554

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

---

---

---

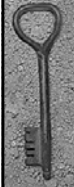
---

---

---

---

---



## 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*

---

---

---

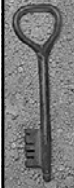
---

---

---

---

---



## Caesar's Cipher

40-50BC    Caesar Cipher (Substitution Cipher)

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

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

---

---

---

---

---

---

---

---