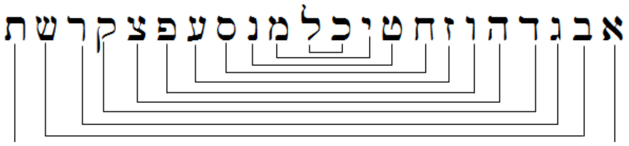
Historical Ciphers—ENEE/CMSC/MATH 456
Atbash Cipher (600 B.C.)

From Wikipedia: **Atbash** is a simple substitution cipher for the Hebrew alphabet. It consists in substituting *aleph* (the first letter) for *tav* (the last), *beth* (the second) for *shin* (one before last), and so on, reversing the alphabet. In the Book of Jeremiah.



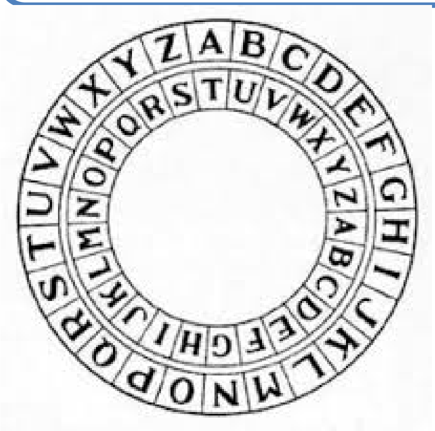
A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

helloworld → SVOOLDLIOW

1. Key space? Size?
2. Encryption/Decryption algorithm?
3. Security?

Shift/Caesar Cipher (100 B.C.)

From textbook: One of the oldest recorded ciphers, known as Caesar's cipher is described in "De Vita Caesarum, Divus Iulius" ("The Lives of the Caesars, The Deified Julius"), written in approximately 110 C.E.

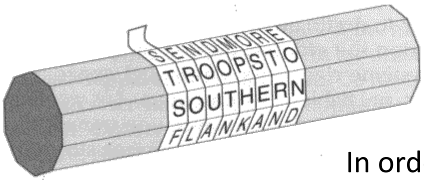


Example: Caesar cipher with shift 19.
Outer wheel is plaintext letter.
Inner wheel is ciphertext letter.

1. Key space? Size?
2. Encryption/Decryption algorithm?
3. Security?

Scytale Cipher (600 B.C.)

From Wikipedia: From indirect evidence, the scytale was first mentioned by the Greek poet Archilochus, who lived in the 7th century BC. Other Greek and Roman writers during the following centuries also mentioned it, but it was not until Apollonius of Rhodes (middle of the 3rd century BC) that a clear indication of its use as a cryptographic device appeared. A description of how it operated is not known from before Plutarch (50-120 AD):



Thin sheet of papyrus wrapped around staff. Messages are written down the length of the staff.

In order to recover the message, a staff of equal diameter must be used.

1. Key space? Size?
2. Encryption algorithm?
3. Security?

Monoalphabetic Substitution (800 A.D.)

Each plaintext character is mapped to a different ciphertext character in an arbitrary manner.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	E	U	A	D	N	B	K	V	M	R	O	C	Q	F	S	Y	H	W	G	L	Z	I	J	P	T

tellhimaboutme → **GDOOKVCXEFLGCD**

1. Key space? Size?
2. Encryption/Decryption algorithm?
3. Security?