Atbash (c. 500 BC)

Atbash is a simple substitution cipher for the Hebrew alphabet. It consists of substituting aleph (the first letter) for tav (the last), beth (the second) for shin (the one before last), and so on, reversing the alphabet. That is, atbash is self-descriptive when transliterated from Hebrew: Aleph-Tav-Beth-Shin. Note that modern Hebrew is written right-to-left.

The substitutions for the Latin (Roman) alphabet are:

```
ABCDEFGHIJKLM
ZYXWVUTSRQPON
```

Example: `NZGS RH UFM` decrypted reads `MATH IS FUN`

Example: `IRK LOW HOLY`

This is an example of a **monoalphabetic substitution**.

Caesar Cipher (c. 100 – 40 BC)

In the traditional Caesar cipher, the alphabet is shifted by 3 letters (Caesar shift +3).

```
ABCDEFGHIJKLMNNOPQRSTUVWXYZ
DEFGHIJKLMNNOPQRSTUVWXYZABC
```

Nothing is unique about 3. One could shift by any other number.

Example: Decrypt the following message (encrypted with Caesar shift +7)

```
ILDHYLAOLPKLZVMTHYJO
```

This is an example of a **monoalphabetic substitution**.

It is also an example of a **shift substitution**.

Alberti's Cipher Wheel (1404 – 1472)

Fig. 1.4 goes here

H	11	W	21
J	12	Y	22
K	13	the	23
U	14	and	24

"Pointer" letter is `k`. Use a simple nomenclator as well.

Example: To encrypt `I CAN'T GO ON LIKE THIS` if the pointer `k` lines up with `T` initially:

plaintext:

`I C A N T G O O O N L I K E T H I S`

ciphertext:

`T s z g h k o t B z a l d t q & L g n n x l`

This is an example of a **polyalphabetic substitution**.

Vigenère Autokey (1523 – 1596)

Blaise de Vigenère (1585) introduced Vigenère square.

Correspondents possess Vigenère square and agree on a **priming key**.

Example: To encrypt GOOD DAY TO YOU if the priming key is Q:

plain	G	O	O	D	D	A	Y	T	O	Y	O	U
key	Q	G	O	O	D	D	A	Y	T	O	Y	O
cipher	W	U	C	R	G	D	Y	R	H	M	M	I

Example: To decrypt JAHNXC if the priming key is Q:

cipher	J	A	H	N	X	C
key	Q	T	H	A	N	K
plain	T	H	A	N	K	S