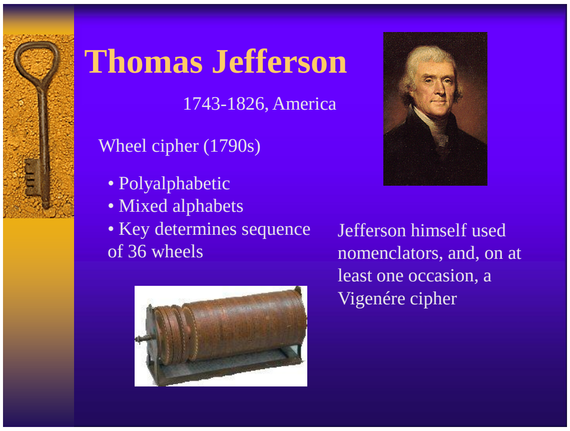


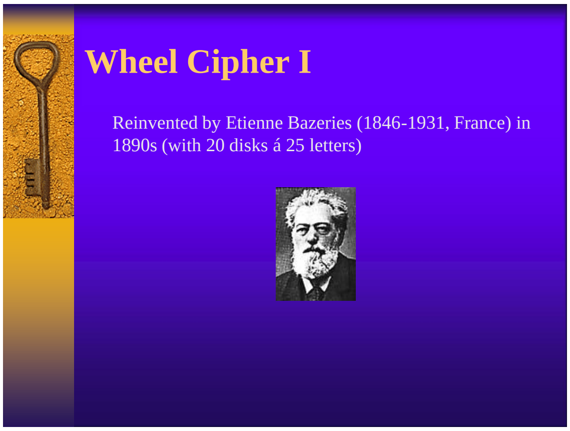
Thomas Jefferson

1743-1826, America

Wheel cipher (1790s)

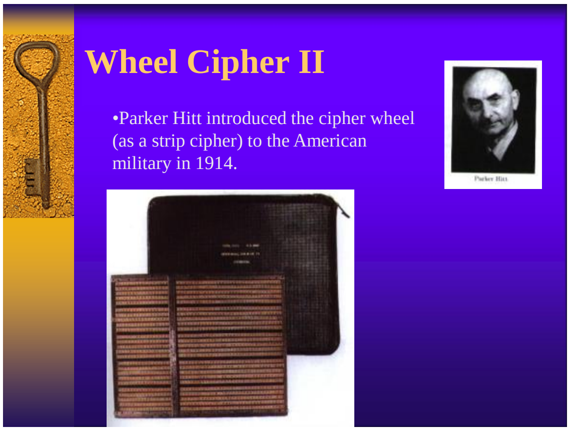
- Polyalphabetic
- Mixed alphabets
- Key determines sequence of 36 wheels

Jefferson himself used nomenclators, and, on at least one occasion, a Vigenére cipher



Wheel Cipher I

Reinvented by Etienne Bazeries (1846-1931, France) in 1890s (with 20 disks á 25 letters)



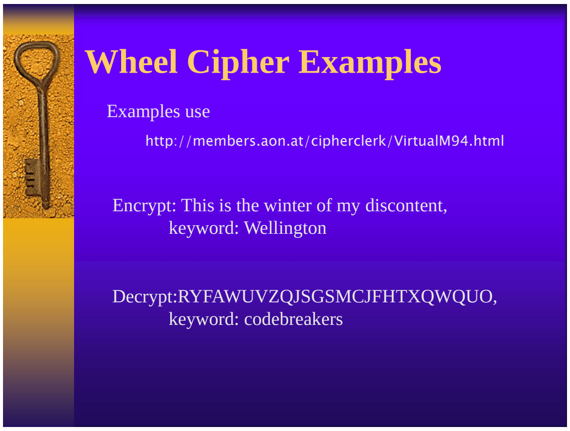
Wheel Cipher II

•Parker Hitt introduced the cipher wheel (as a strip cipher) to the American military in 1914.

Parker Hitt

Wheel Cipher III

- In different versions (M94 after WW I, M138 in WW II) used in the first half of the 20th century



Wheel Cipher Examples

Examples use

http://members.aon.at/cipherclerk/VirtualM94.html

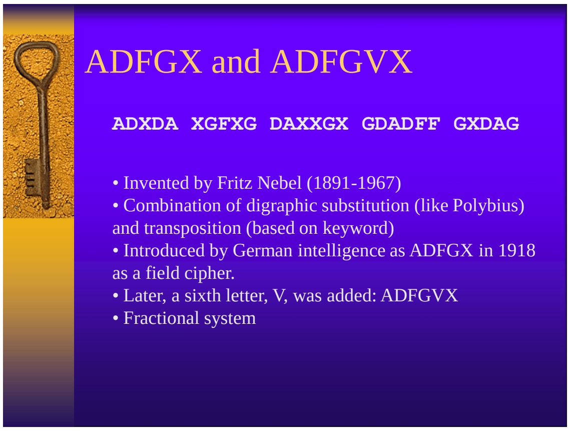
Encrypt: This is the winter of my discontent,
keyword: Wellington

Decrypt:RYFAWUVZQJSGSMCJFHTXQWQUO,
keyword: codebreakers

ADFGX

ADXDA XGFXG DAXXGX GDADFF GXDAG

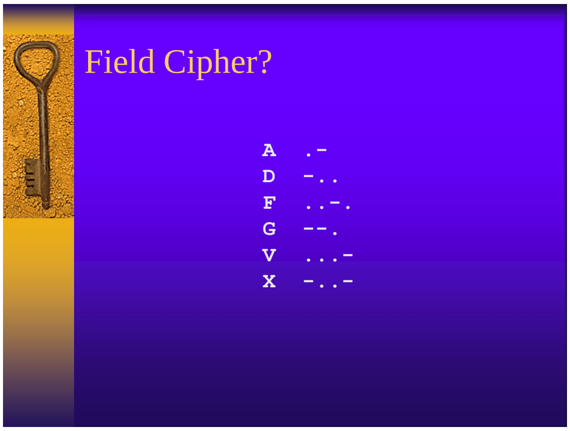
?



ADFGX and ADFGVX

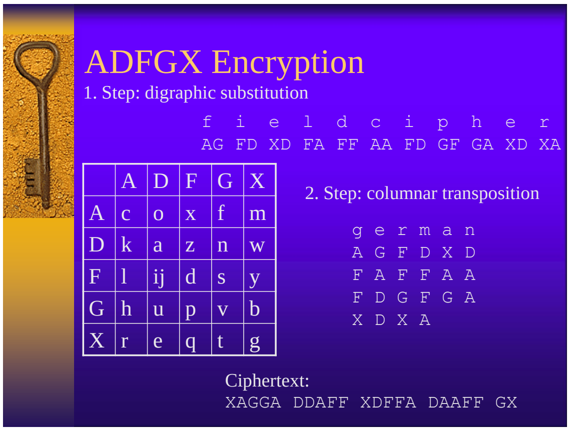
ADXDA XGFXG DAXXGX GDADFF GXDAG

- Invented by Fritz Nebel (1891-1967)
- Combination of digraphic substitution (like Polybius) and transposition (based on keyword)
- Introduced by German intelligence as ADFGX in 1918 as a field cipher.
- Later, a sixth letter, V, was added: ADFGVX
- Fractional system



Field Cipher?

A	.-
D	-..
F	..-.
G	--.
V	...-
X	-..-



ADFGX Encryption

1. Step: digraphic substitution

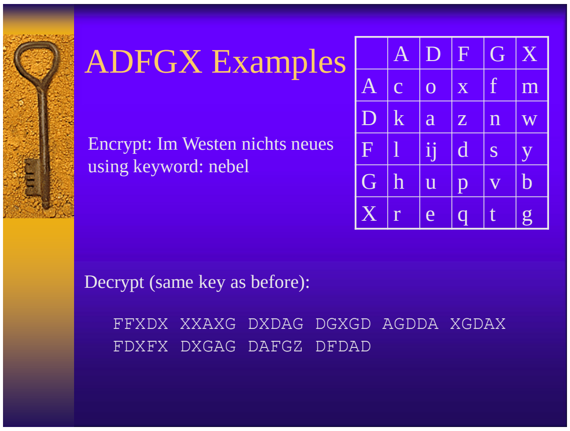
```
f  i  e  l  d  c  i  p  h  e  r
AG FD XD FA FF AA FD GF GA XD XA
```

	A	D	F	G	X
A	c	o	x	f	m
D	k	a	z	n	w
F	l	ij	d	s	y
G	h	u	p	v	b
X	r	e	q	t	g

2. Step: columnar transposition

```
g e r m a n
A G F D X D
F A F F A A
F D G F G A
X D X A
```

Ciphertext:
XAGGA DDAFF XDFFA DAAFF GX



ADFGX Examples

	A	D	F	G	X
A	c	o	x	f	m
D	k	a	z	n	w
F	l	ij	d	s	y
G	h	u	p	v	b
X	r	e	q	t	g

Encrypt: Im Westen nichts neues
using keyword: nebel

Decrypt (same key as before):

```
FFXDX XXAXG DXDAG DGXGD AGDDA XGDAX
FDXFX DXGAG DAFGZ DFDAD
```