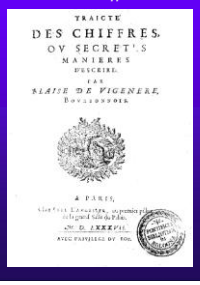
Blaise de Vigenère

1523-1596, France

Traicté de Chiffres, 1585


TRAICTE
DES CHIFFRES,
OV SECRETS
MANIERES
DESCRIRE.
PAR
BLAISE DE VIGENERE,
Bourbonnois.
A PARIS,

- several autokey systems
- grilles
- discusses polyalphabetic ciphers (with mixed alphabets)

Blaise de Vigenère

Traicté de Chiffres, 1585

Autokeys:

```
key     DA UNO MD ELETERNE
plain   au nom de leternel
cipher  XI AHG UP TMLSHIXT

key     DX HEE CO UMXGNABQ
plain   au nom de leternel
cipher  XH EEC OU MXGNABQO
```

Le Chiffre Indéchiffrable I

```
plain   lechiffreindechiffrable
key     vraivraivraivraivraivra
cipher  GVCPDWFZZZNLZTHQAWRIWCE
```

Look familiar?

Le Chiffre Indéchiffrable II

"...impossible of translation."
Scientific American, 1917

"...weaving them into a coherent and powerful new cipher."
Simon Singh, 1999

"I may at this point mention a letter of this sort sent me a while ago ... To his surprise I interpreted it within the very hour I received it ..."
Porta, 16th century

"... telling me that it was not possible to find it out, and I quickly found out the countercipher which was of 10 alphabets and the motto."
Argenti, 1581

Le Chiffre Indéchiffrable III

Many early solutions were found by guessing the key.

Porta: omnia vincit amor
Argenti: in principio erat verbum

Also, remember Porta's ideas on analyzing polyalphabetic ciphers.

However, with mixed alphabets, the cipher would have been virtually unbreakable for Renaissance cryptanalysts.

Le Chiffre Indéchiffrable IV

- Why were the more general forms of polyalphabetic ciphers not used?
- Why did the Vigenère cipher (as it became called) become popular?
- Why did the nomenclator survive so long?