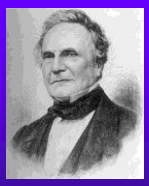
Charles Babbage

1791-1871, England



- Difference Engine
- Analytical Engine
- Interested in cryptography

Charles Babbage and the Vigenére Cipher

key	RUNRUNRUNRUNRUNRUNRUNRUNRUN
plain	tobeornottobethatisthequestion
cipher	KIOVIEEIGKIOVNURNVJNUVKHVMGZIA

Observation: if the same piece of key meets the same piece of plaintext, then the ciphertext is identical.

Therefore, if we see identical pieces of ciphertext, we can try assuming that key/plaintext repeated.

In that case the difference between positions has to be a multiple of the key-length.

Friedrich W. Kasiski

Die Geheimschriften und die Dechiffrirkunst, 1863

First general and published solution to polyalphabetic cipher with repeating keyword (Vigenére cipher) using Kasiski examination.

Kasiski Examination

- Find (long) repeated ciphertext fragments
- Discard spurious repetitions
- gcd of position differences is multiple of keylength

Kasiski Examination

```
key     RUNRUNRUNRUNRUNRUNRUNRUNRUN
plain   tobeornottobethatisthequestion
cipher  KIOVIEEIGKIOVNURNVJNUVKHVMGZIA

key     COMETCOMETCOMETCOMETCOMETCOME
plain   thereisanotherfamouspianoplay
cipher  VVQVXKGMRHVVQVYCAAYLRWMRHRZMC
```

However: http://www.ics.uci.edu/~gts/268/vigenere.html

Le Chiffre Indéchiffrable

Later methods:

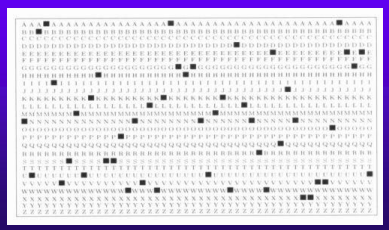
- Index of coincidence (William Friedman)
- Kappa Test (Solomon Kullback)
- Chi Test (Solomon Kullback)

Vigenére cipher still in use in WWI.

Kappa Test

Kappa test with strips

Kappa test with perforated sheets



From Bauer. Decrypted Secrets (Section 17.3.2)

Wheatstone and Playfair

Playfair Cipher

- Invented by Charles Wheatstone
- Publicized by Lyon Playfair in 1854
- First literal digraphic system
- Mixed alphabet, keyword
- Used in the Boer War (1899-1902)

Playfair Cipher I

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

encodes pairs of letters

1. find pairs of letters in matrix
2. same row: move one pair to the right
3. same column: move one pair down
4. form rectangle: replace with other corners, remaining in same line

Examples: cipher -> DRAEGI
abrupt -> BHIVFN

Playfair Cipher II

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

encodes pairs of letters

1. find pairs of letters in matrix
2. same row: move one pair to the right
3. same column: move one pair down
4. form rectangle: replace with other corners, remaining in same line

Encrypt: go to rome; marriner
Decrypt: AQMNKGCV
Encrypt: playfair with key wheatstone

What are weaknesses of the system?

Playfair Cipher III

Exploit weakness in a known plaintext attack:

```
tonightyoujokeagedbursar
YTOHHNYEPTOTICGEBICQSTFW
```

What is the matrix?
Can you guess the key?