Influence of Secret Codes on our History

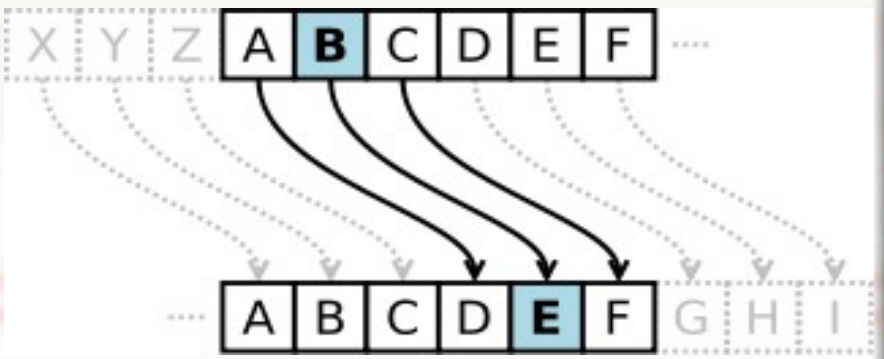
Fabrice Durand

Contents

- A simple example : Julius Caesar's code
- Al-Kindi and frequency analysis
- Mary Stuart Queen of Scotland
- Coded Zimmermann Telegramm & WW1
- Alan Turing and the Enigma & WW2
- Conclusion

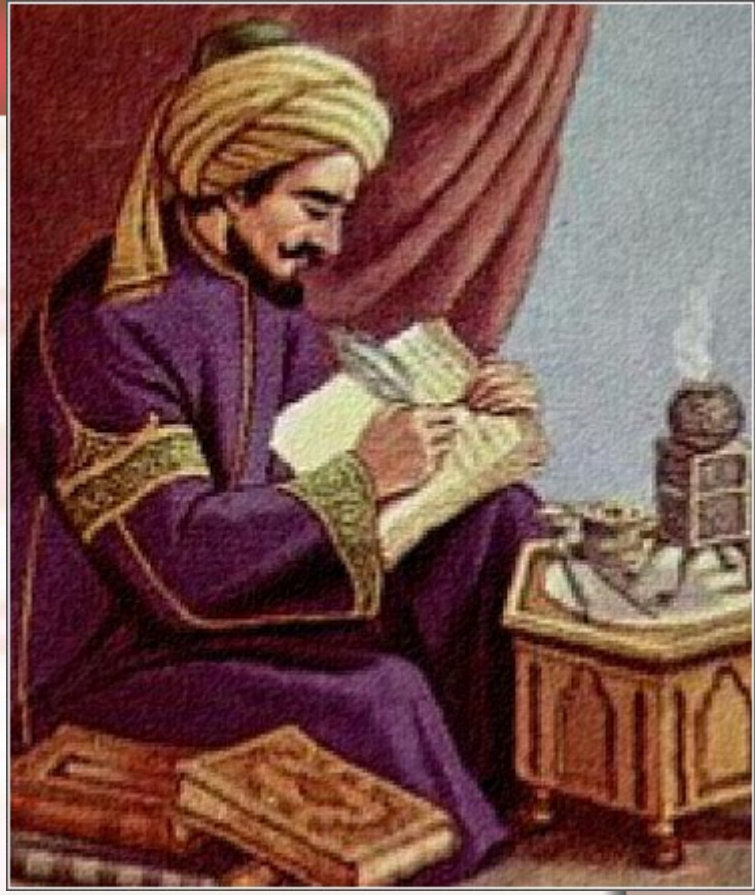
A simple example : Julius Caesar cipher

- Caesar's code or Caesar shift
- One of the first ciphers in history
- It consists in replacing each plaintext letter with one fixed number of places down the alphabet



- This example is with a shift of three, so that a B in the plaintext becomes E in the ciphertext.

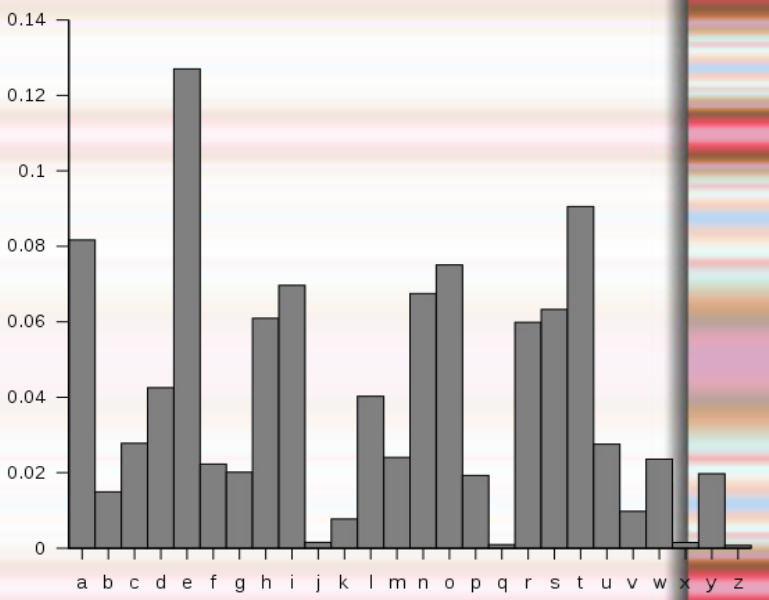
Al-Kindi and frequency analysis



- Muslim Arab philosopher, mathematician and musician of 9th century AD
- Developed a method called “frequency analysis” by studying the Qur'an
- The variations in the frequency of the occurrence of letters could enable to break ciphers

Al-Kindi and frequency analysis

- Frequency analysis to break ciphers : study of the frequency of letters or groups of letters in a ciphertext
- Use of the typical distribution of letters in a language
- Al Kindi was the first to discover how to break Caeser cipher
- While Europa was still struggling with the basics of cryptography



Mary Stuart Queen of Scotland

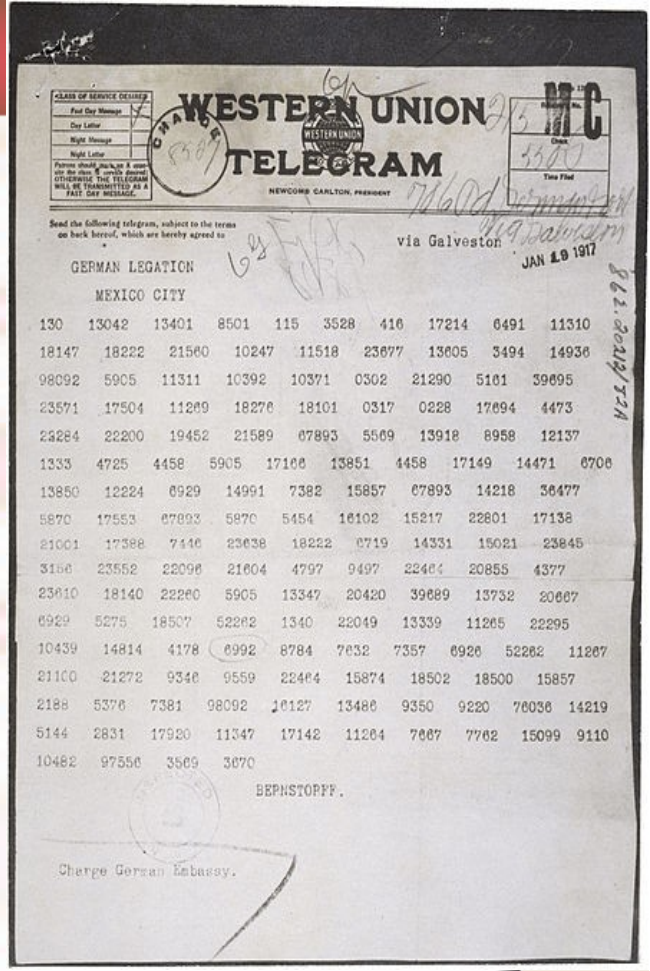
- Used Caesar's improved cipher to communicate with her friends in order to assassinate Queen Elizabeth I
- the best British cryptanalysts can easily intercept and decipher its correspondence
- Then she was convicted in a trial
- So she was executed under the command of Queen Elizabeth I.

Coded Zimmermann Telegramm & WW1

- State Secretary for Foreign Affairs of the German Empire in 1916-1917
- Zimmermann wanted to decrease the likelihood of America entering the war, by persuading President of Mexico :
  - To invade America from the South
  - To act as a mediator and persuade Japan to attack America from the west.
  - And Germany would pose a threat to America's east coast.

Coded Zimmermann Telegramm & WW1

- This would pose America such problems at home that it could not afford to send troops to Europe.
- Zimmermann sent his encrypted telegramm to the Mexican president but it fell into British hands...
- The telegramm was decrypted and finally America entered the war, destroying the hopes of Zimmermann



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

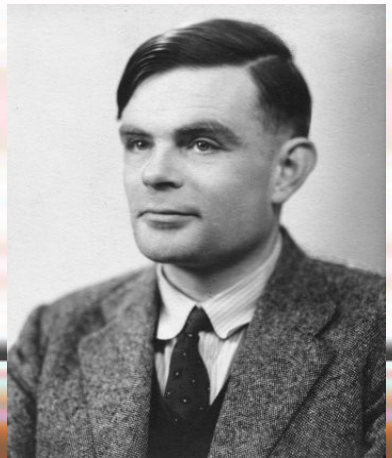
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7146 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BERNSTORFF.

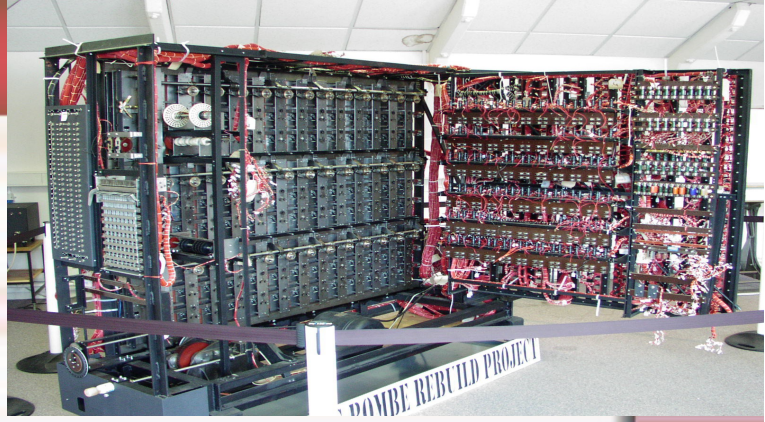
Charge German Embassy.

Alan Turing and the Enigma & WW2

- During WW2, the Germans used mechanical machine « Enigma » to code their communications and it was very difficult to break these sophisticated codes.
- Mathematicians such as Marian Rejewski (Polish Cipher Bureau) and Alan Turing (Bletchley Park) were leading participants in the breaking of these codes



Alan Turing and the Enigma & WW2



- We can say that thanks to their contribution and especially to that of Alan Turing, the Allied Army won WW2 against Nazi Germany
- Unfortunately he was not considered as deserved because after being declared a war hero, he was accused of being homosexual and forced to take hormone therapy.
- He then entered into a depression and ended his days by eating a poisoned apple.

Conclusion

- Cryptography and cryptanalysis have had a huge impact on main events of our history
- There is a perpetual war between coders and code breakers
- We can not say that the most modern techniques of encryption are inviolable
- If we could build a quantum computer, it would be a child's play to break modern codes.
- Use codes but be aware it may be broken so hide your private information !

Thank you for your attention !