

*Unil*

UNIL | Université de Lausanne



David-Olivier Jaquet-Chiffelle

# **Cryptanalyse du Chiffre de Vigenère**

# Attaque sur le texte chiffré

EMWGSJBMPLDIZVGSURMLGTIOXPQLSJLCGOCLNLKMSJOWWMDVPB  
UHFKDZFNBDJBSNSEKIULOEOEQNGGZZFBHVNBQNHCVPCBBVZBNX  
RVPQNXHEZUQUXVXBGSDRNYWXJFNIOBGJJVVLIINMVJIVQWWLDR  
MTGSPRNMEHIKZHDBSEXMEBHVOMCMSKZMPIOEOWWYZVKWTMSJXT  
QLSJXPGSJFPAUTBJPVVXAFDVSNWJJCHYZVQWWLRZOMUTZFMKE  
ZVVCREIJHGUMSIDMWQRVQWUTAZNLGVCVPZQNGZQWWLZRDUGSAZ  
ZCZOCLNUWKALMMBMCLOAGNZTMWATBKKZGLELZDQNGKVQTXRRIA  
NXTFILFNBNVXIXXOKMMPMSGDMFLGFPVXFIZCPECKYMUUIZIDE  
SRLCGEELZQPWWMDLWVSDJBSNSMJCUVFFTMBJIVGWPGOGVAGGHV  
ILWJIVQWWLRZLNQGSZWIUWOENCPEWVPAQNFUZZBUHASMMEHIOI  
RXWEZTCVVVKITMPFILKMGFMBFXZFHJTXHVIMBBZVNBFXVMAKE  
QFIVCBHJJVEASDDVKEARMKJXWCVLGNLGDMLIEWIVHBRGIOTWE  
YMDHBJNWWEWVMAHXFIZAWGDRNAGICIOMPXSXGMCNPNVNWKGWCKZ  
GGRIVQVWSJVQNXGTJUOXZRDONXWCQWWLSTCIRISZGNWBHIDMPG  
SCVZTXHVMIKEGLDBNXELVQHKOEXPKMZRKTCVSVOKCXHVMIRTGJ  
ZTGTIJVVUUOKZIWWOENTCLOZNPWSJXZXWGVODCMCLOIVKOMZZ  
UNBUZLCESUZZWXGUMWKMQYZHNBBUDDKWIUJVVOCLNIXXNGVZNX  
WCNIKMZVICOXFFGMVTUVDTCBOTGMKEAFIBGESJXINBSIJCXKSC  
VXQKHVKIULSVIBTXOIMQXXSKMIKEZVPZTXURMLCGHCCWOFVIN  
CVSUDBOXJFDTCCSJZUWSCVJQNQYZLWGHVGMVVSJONCBHMJCUT  
JVUCPXBEZUKFCIOMN

Data & Results

Encrypted message Cleartext

Encrypted message

```

KITMPFILKMGFMFBFXZFHJTXHVIMBBZV
NBFXYVMAKEQFIVCBHJJVEASDDVKEAR
MKJXWCVLGNLGDMLIEWIVHBRGIOTWE
YMDHBJNWEWVMAHXFI ZAWGDRNAGICI
OMPFKXGMCNPNVNRGWCKZGGRIVQVWSJ
VQNXGTJUOXZRDONKWCQWNLSTCIRISZ
GNWBHIDMPGSCVZTXHVMIKEGLDBNXEL
VQHKOEFPKZKTKCVSVOKCXHVMIKGTGJ
ZTGTIJVVUOKZIWNOENTCLOZNPWSJ
XZXKGVODCMCLOIVKOMZUNBUZLCE SU
ZZWXGUMKMQYZHNBBDKWIUJVVOCUL
NIXXNGVZNXKCNIMZVICOXFFGMVTUV
DTCEOTGMKEAFIBGESJXINBSIJCKKSC
VXQKHVKIULSVIBTXOIMQXXSRMIKEZV
FZTKURMLCGHCCWQFSVINCVSUDBOXJF
DTCCSJZUWSCVJQNOYZLWGHVGMVVSJ
    
```

Operations

Step 1: Length of the key

The goal is to find the length of the key. Two options can be used:

- 1. Kasiski
- 2. Index of coincidence
- Final key length

Select n (repetitive n-grams will be searched for in the encrypted message)  Search

Show GCD frequencies

See less details

Info: In this exercise, for design reasons, only GCD smaller than 25 are shown.

Show 10 entries

Pattern	Occ.	Distances	GCD
QWW	5	90 144 312 534	6
WWL	5	90 144 312 534	6
VQW	4	90 126 312	6
SJX	4	6 582 690	6
LCC	3	372 907	1
JVV	3	623 702	1

<https://esc-edu.unil.ch/vigenere/>