

Cryptanalyse de Vigenère

Annexe du cours de sécurité et réseau

Babbage et Kasiki

- Trouver la longueur de la clé
 - repérer les répétitions de trois lettres (ou plus)
 - chercher un diviseur commun (probable)
 - en déduire la longueur de la clé n
- Analyse fréquentielle
 - en partant de chacun des n premiers caractères
 - en prenant un caractère sur n

Babbage et Kasiki

- Message chiffré : ksemc ptnpl fhkzu ggtak
eoagf ldxhv ixsbj ogudt kadnh vixfh nlneh
bnsew gmobz llez ewkam thviv gztec wrxop
ekgmo bulte ckekp pekgm obuxu xllvx pksww
mobgk agusa okslx flfhk e

Bazeries

- Deviner un mot probable
- Chercher la position du mot probable dans le texte
 - en déduire la clé
- Appliquer la clé sur le texte

Bazeries

- Message chiffré : ogvmg lbkmc dnksv hdxzq
urxxg stgix rzbiu oqvmg rd
- Extrait de "Le Magicien d'Oz", Frank Baum

Liens

- Lien : <http://www.apprendre-en-ligne.net/crypto/vigenere/index.html>