Cryptanalyse de Vigenè

Annexe du cours de sécurité et ré

Babbage et Kasiki

- Trouver la longueur de la clé
  - repérer les répétitions de trois lettr
    plus)
  - chercher un diviseur commun (pro
  - en déduire la longueur de la clé *n*
- Analyse fréquentielle
  - en partant de chacun des *n* premie
    caractères
  - en prenant un caractère sur *n*

Babbage et Kasiki

- Message chiffré : ksemc ptnpl fhkzu g
  eoagf ldxhv ixsbi ogudt kadnh vixfh n
  bnsew gmobz llegz ewkam thviv gzte
  ekgmo bulte ckekp pekgm obuxu xllv
  mobgk agusa okslx flfhk e

Bazeries

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

Bazeries

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

Liens

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