Première chose : compter combien de symboles différents il y a dans le message

Deuxième chose : dresser un histogramme

Troisième chose : calculer l’indice de coïncidence (Friedman)

Casser Vigenere : calculer les IC pour chaque intervalle (lettres espacées de, 2, 3…). Arrivé à intervalle 5 on se rends compte que l’IC augmente puis diminue à l’intervalle 6. Il est fort probable que cela soit une clé de 5.

La cryptographie moderne :

* Le chiffrement par bloc
* Les systèmes à clefs
  + Clés privées
  + Clés publiques

**Diffie Hellman**

Le but de Alice et Bob avec le double cadenas est pareil que les puissances

(10^3)^2 = 10^6 = 10^(2\*3) = 10^(3\*2) = il y a permutation, du coup on fait passer le cadenas de Bob au-dessus de celui d’Alice et vice versa. RSA fonctionne sur des notions de puissance.

Par contre les ordinateurs ont beaucoup de mal du coup RSA s’appuie sur les puissances modulaires pour que ça soit plus facile pour chiffrer et déchiffrer.

(RSA,n,e) = Cryptogramme de CB par exemple 115 : 115^e (n) (n = modulo)

Et coté serveur : n = p\*q

RSA est basé sur le fait qu’on ne peut pas factoriser de gros nombres, sauf avec du temps et de la puissance de calcul, mais en soit l’algorithme est très simple