Table des matières

1) Message chiffré

Je place mon message chiffré et je compare les longueurs de clé proposées.

Message chiffré :

HNWKT GGFGA MEVVI TLWCA MJHYV RWUGZ KRHZB PFVHB XRVRL JBRKZ UMBRC OFKLR
QHPKT YVRMN HVUYY YVEFE YYWIU HYZLU WVZUK QCGYT MIPPI XXRQF WUGHW VNKLI
VAIYI VQWYZ LRQFC TLXKG OZBSP FFABW GANJN RGPFG MUWVL KLWGZ VRXEW WIAKH
JHCGV INHCJ XWEBH YMINY UZBSP FXUGX NNMZK SRUSY BUWRH UNWCC JXBXL NXOLU
WRFRX WGGUO XRVZI XMIUQ YPTHG COOLP QAAZX QRFJU NVSHI OVIUA IAOIC HNKLR
GFITM INYYY ISKAN GWZGA OKLNG AUIVY URFKL TJVFU LSRUY YWSPG DKLYK FAKGW

Longueur minimale clé : 2

Longueur maximale clé : 20

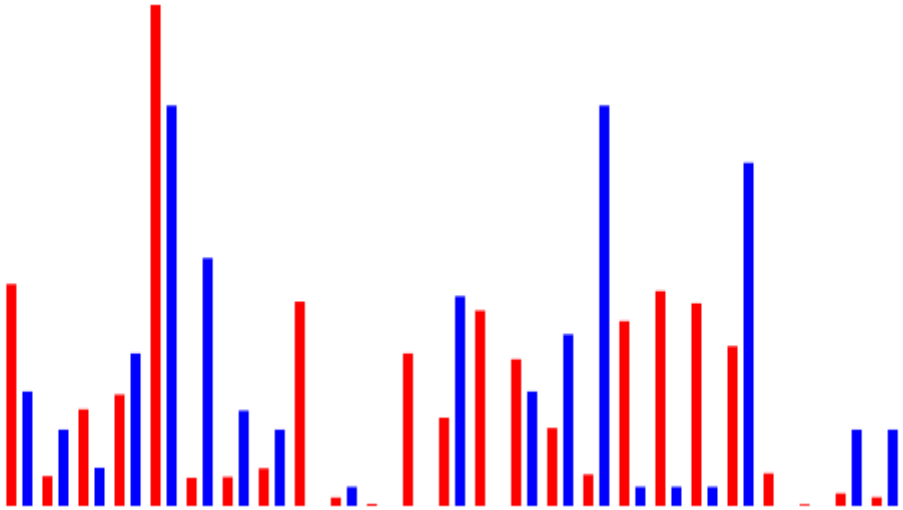
Calculer les indices de coïncidence

Résultat de l'analyse :

Pour une longueur de clé de 2, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 3, l'indice de coïncidence vaut 0.058
Pour une longueur de clé de 4, l'indice de coïncidence vaut 0.049
Pour une longueur de clé de 5, l'indice de coïncidence vaut 0.044
Pour une longueur de clé de 6, l'indice de coïncidence vaut 0.076
Pour une longueur de clé de 7, l'indice de coïncidence vaut 0.043

Je vois que pour une clé de 6 l'indice est le plus gros donc par exemple dans l'alphabet le A devient le G (6ème lettre)

Longueur de clé choisie :
6
Rang de la lettre de la clé analysée :
5
Lancer l'analyse
- H +



Je met ma longueur de clé choisie et je monte 1 par 1 le rang de la lettre de la clé analysée en analysant à chaque fois le diagramme en dessous. Je regarde quand le bleu se rapproche au maximum du rouge. Je sélectionne la lettre trouvé à chaque fois et je la met dans "clé proposé". Après l'avoir fait 6 fois je déchiffre le message et je corrige les espaces entre chaque mots. La clé trouvé est (CNUGTE)

Message déchiffré :

FACE A CES MUTATIONS SANS DOUTE CONVIENT IL DINVENTER DINIMAGINABLES NOUVEAUTES HORS LES CADRES DES U ET SQUIFOR MATEN TENCO RENOS CONDU ITESE TNOSP ROJET SNOSI NSTIT UTION SLUIS ENTDU NECLA TQUIR ESSEM BLEAU JOURD HUIAC ELUID ESCON STELL ATION SDONT LASTR OPHYS IQUEN OUSAP PRITJ ADISQ UELLE SETAI ENTMO RTESD EJADE PUISL ONGTE MPSPO URQUO ICESN OUVEA UTESN ESONT ELLES POINT ADVEN UESJE NACCU SELES PHILO SOPHE SDONT JESUI SGENS QUION TPOUR METIE RDANT ICIPE RLESA VOIRE TLESP RATIQ UESAV ENIRE TQUIO NTCOM MEMOI CEMES EMBLE FAILL IALEU RTACH EENGA GESDA NSLAP OLITI QUEAU JOURL EJOUR ILSNE VIREN TPASV ENIRL ECONT EMPOR AINSI JAVAI SEUEN EFFET ACROQ UERLE PORTR AITDE SADUL TESDO NTJES UISIL EUTET EMOIN SFLAT TEURJ EVOUD RAISA VOIRD IXHUI TANSL AGEDE PETIT EPOUC

ETTEE TDEPE TITPO UCETP UISQU ETOUT ESTAR EFAIR ENONP UISQU ETOUT ESTAF AIREJ ESOUH AITEQ UELAV IEMEL AISSE ASSEZ DETEM PSPOU RYTRA VAILL ERENC OREEN COMPA GNIED ECESP ETITS AUXQU ELSJA IVOUE MAVIE PARCE QUEJE LESAI TOUJO URSRE SPECT UEUSE MENTA IMESM ICHEL SERRE SPETI TEPOU CETTE

2) C’est Hashé

Pour trouver le mot de passe en clair je peux tenter de hasher des mots de passe via internet et comparer avec le hash du mot de passe

3) Entropie de mots de passe :

Cinema : 18.4 bits

c1n3m4 : 20.4 bits

cinem@ : 20.5 bits

6nema : 17 bits

cinemaharicotcielbleu : 79.1 bits