AGUILAR_Flavien_Cryptographie

Flavien AGUILAR

12/10/2020

Cybersécurité ou pas :

Message chiffré :

Pour déchifrer le message suivant :

```
HIUGO EMKOI VILKC PAKCB ULGWH GKGPJ KMFVW NLAPJ GVLGF FQFKA COAPO DTWUB
     QCNGO WBWUV QZKNS UKSFF GAVGG WMLUE WQXQF OILGB VMFEC TMFQG EWFFI
    KBWUS VVGUD TWBGH UVGUW PALKH WBAQB UTMKG GVLFI PMUNO VYMKF GAKGA
    DTWCI LWMTR JCACQ GTMKR GAUQB UBWNZ CBAQB ULGPH NIKVF QXZAG KYMGB
    QCKCD RZAVX CLAUE WMDNS UMLCW GVLOC TBWUR GRSFS RCAUZ QVYVS OXKRC
    WZIWC KKWUB QCNGO WBWUB GAGPH GTDGG RWAPH CLNGB WMKLS PIUEI UMDGG
    RPANC UWHJS ULGPH LMKWW UOWPG SCAQB VXGWF OMLKS TLSPH KKARS TTWUO
    XWATS VTWUD TILKE WMKCJ GVATS VYMKC PBUQA OMEQW EMEGG GUTNS HIANZ
    KIDGI TBSEV GMFIO IMKFO PADCD QTAVW SCWCI LWMTZ GRGWF KTKPS XQJGB
    VXSUJ GVATZ GKGPH GUHQF CQFUW LINCW UMMGB GNXGH CKJQE WMJNS RWJVF
    CQLFS UIVWZ VMKFC PBBGG WQKKZ GCLGH GUGKB UNDCH VMMTX GDGWR TIAUO
    XWATR KFZWW VIFUZ COWFS RMLKH GXGWQ GBLGS VLWRS VQLRC WKWVD WQKSI
    GBGWH GALCF GNSKF GVGPD WQKSI GBGWH GALCT CQJGX GAGWV CQLGE WMDCJ
    KMEGZ CQKUS CAKGN FMLGA RAHQI TGLTO XIANZ GZWPQ QZWGB EWERO IVAGR
    GKWUD GBAVG CCPSI GTKLO KDGWS OINKS RIJES SCWLS NMKCW VWMLC WZKTS
    UXWEH WMMUS OMFVO KUWUA KKZGZ UMJTS UXWVW VMHQI EMLVS
```

Nous allons utiliser site http://www.bibmath.net/crypto/index.php?action=affiche&quoi=poly/chasvig .

Sur ce site, nous allons pouvoir rentrer notre message chiffré et commencer à chercher les indices de coincidences de la clé. Plus l'indice sera élevé, plus la probabilité que la longueur de clé correspondante soit la bonne.

Dans notre cas, nous relevons une longueur de clé de 5 caractères. Une fois la longueur de clé trouvée, nous allons chercher les caractères formant la clé en essayant de faire correspondre au maximum la fréquence théorique et la fréquence théorique.

Dans notre cas la fréquence sera « CISCO ».

En décodant le message, nous allons obtenir le message déchifré suivant :

```
FACEA CESMU TATIO NSSAN SDOUT ECONV IENTI LDINV ENTER DINIM AGINA BLESN
     OUVEA UTESH ORSLE SCADR ESDES UETSQ UIFOR 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
```

En arrangeant un peu les espaces, nous pouvons obtenir un message tout à fait lisible en français :

```
FACE A CES MUTATIONS SANS DOUTE CONVIENT IL....
```

C’est Haché :

Pour déchifrer les mots de passes suivants :

```
ernesto:fff8f7c569ec2dae6a49baabe0a27daded6c5308
philippe:6f71c072b5870a0c0dd993cdcac7dd3d19bffe2b
peter:70d83d9b6f653c2fe741848b84a571f5cd3e80a8
admin:c8fed00eb2e87f1cee8e90ebbe870c190ac3848c
```

Nous allons tout d’abord trouver la clé de chiffrement, dans notre cas, la méthode sha1 est utilisé.

Nous pouvons maintenant essayer de hasher un mot et le comparé avec le hash du mot de passe :

```
[detp Cryptographie]# echo "philippe" | sha1sum
6f71c072b5870a0c0dd993cdcac7dd3d19bffe2b
```

Nous pouvons maintenant comparer ce hash avec le hash contenu dans le fichier. Pour ce faire nous allons créer le script suivant :

```
#!/bin/bash

pass1=$1
pass2=$2

if [ $pass1 == $pass2 ]; then
    echo "Le mot de passe est le bon"
else
```

```
    echo "Le mot de passe n'est pas bon"
fi
```

```
[detp Cryptographie]# ./test.sh 6
   f71c072b5870a0c0dd993cdcac7dd3d19bffe2b 6
   f71c072b5870a0c0dd993cdcac7dd3d19bffe2b
Le mot de passe est le bon
```