conversation.png

13/03/2020

13:05 Laswo, totl xgwl hkto hgwk s'aooajwt ?

Gwm, ogwo tlo hkto. 13:17

Gwm gf lt rgmo wft xgzca ahktl axte wft hgwomft a Dglegw. 13:22

13:35 Gc a ogwot a s'itwkt.

---

secr@t.txt

abcdefg□ijklmnopq□stuv□xyz

A□□□□□UI□P□SD□GH□KL□WXQ□□N

L'ANALYSE DES FREQUENCES

L' analyse des fréquences génère un histogramme qui permet de déchiffrer un texte en rapprochant les fréquences d'apparition des lettres du message codé avec les fréquences théoriques d'apparition des lettres dans la langue du texte clair.

Fréquences d'apparition des lettres

Lettre	Fréquence	Lettre	Fréquence
A	8.15 %	N	7.12 %
B	0.97%	O	5.28 %
C	3.15 %	P	2.80 %
D	3.73 %	Q	1.21 %
E	17.39 %	R	6.64 %
F	1.12 %	S	8.14 %
G	0.97 %	T	7.22 %
H	0.85 %	U	6.38 %
I	7.31 %	V	1.64 %
J	0.45 %	W	0.03 %
K	0.02 %	X	0.41 %
L	5.69 %	Y	0.28 %
M	2.87 %	Z	0.15 %

Analyse des occurences et fréquences
1-grammes
% calculé | % attendu

T	11×	25%	
L	5×	11.36%	
E	4×	9.09%	
Y	4×	9.09%	
K	4×	9.09%	
O	3×	6.82%	
D	2×	4.55%	
A	2×	4.55%	
I	2×	4.55%	
R	2×	4.55%	
M	1×	2.27%	
W	1×	2.27%	
F	1×	2.27%	
U	1×	2.27%	
B	1×	2.27%	
#N : 15	Σ = 44.000	Σ = 100.00	#N : 15

Une analyse des fréquences sur le message chiffré <<Eteo tlm wf dtllaut eioyykt, tllabtk rt dt rteioyyktk.>> nous indique les lettres les plus fréquentes sont T, L, E, Y et K.

On peut déduire que T=E.
En supposant que L=S et Y=F, le message devient : <<Eeeo esm wf dessaue eioffke, essabek re de reeioffkek>>

Supposons que K=R et E=C (Pour E=A, certains mots du message ne correspondent à aucun mot de la langue française).
le message devient : <<Ceco esm wf dessaue cioffre, essaber re de recioffrer>>

En analysant notre nouveau message on reconnait quelques mots de la langue française tels que : Ceco = Ceci, essaber = essayer et esm = est.
On peut supposer que O=I, A=A, B=Y et M=T.
le message devient : <<Ceci est wf dessaue ciiffre, essayer re de reciiffrer>>.

En analysant à nouveau notre message on reconnait également des mots comme : message, chiffrer et déchiffrer. Quant à "wf", on peut déduire selon le sens de la phrase qu'il s'agit du mot "un".
On en déduit que D=M, U=G, R=D, I=H, W=U et F=N.
Le message orignal est donc : <<Ceci est un message chiffre, essayer de me dechiffrer>>.

Playfair

Voici les étapes pour chiffrer un message à l'aide du chiffrement de Playfair:

Voici les étapes pour générer la matrice de clé:

1. Écrivez la clé secrète dans une grille en éliminant les doublons et en remplaçant les lettres J par I.
2. Remplissez le reste de la grille avec les lettres restantes de l'alphabet, en commençant par A et en omettant J.

Pour le chiffrement

1. Divisez le texte clair en paires de lettres, en ignorant les espaces et la ponctuation, et en remplaçant les lettres J par I.
2. Si une paire de lettres est identique (par exemple, "AA"), insérez une lettre supplémentaire (généralement "X") entre elles.
3. Pour chaque paire de lettres, déterminez leur position dans la matrice de clé.
4. Si les deux lettres se trouvent dans la même ligne ou la même colonne de la matrice de clé, remplacez-les par la lettre de la même ligne ou colonne, respectivement, mais avec l'indice suivant (c'est-à-dire la lettre à droite ou en bas).
5. Si les deux lettres ne se trouvent ni dans la même ligne ni dans la même colonne, remplacez-les par les lettres situées à l'intersection du rectangle formé par leurs positions dans la matrice de clé. La lettre de la première ligne de ce rectangle doit être remplacée par la lettre de la deuxième ligne et vice versa.
6. Répétez les étapes 3 à 5 pour chaque paire de lettres dans le texte clair.

Nous aimerions déchiffrer le texte ci-dessous avec le mot clé "cryptis" :

"OKRFGYKOIFVZXLFYBMISNYIYYDVZJCDYFRKBBU"

LOCKBIT

03/07/2019

Groupe de hacker russophone basé actuellement au Pays Bas, et derrière le celèbre ransomware du même nom, dont la version 3.0 est sortie en Mai 2022 . Il dispose d'un outil et d'un service affiliation. Il est derrière l'attaque contre l'hopital Vvalia ou la ville de Liège par exemple. Le ransomware est numéro 1 en nombre d'attaques revendiquées en 2022. Le groupe a offert 1000$ à toute personne qui se tatouer lockbit. Le groupe aurait gagner des dizaines de milions de $ sur les plus 100 million $ demandée au total. Un de ses membres a été arrété au Canada en novembre 2022.

COZY BEAR

2008

Groupe de hacker russophone et présumèrent associé aux services de renseignement russe. Il est aussi connu sous le nom NOBELIUM, CozyCar, Dark Halo, etc. Il est derrière l'attaque de 2016 sur le parti démocrate qui avait pour but d'aider à faire élire Donald Trump. Il est aussi l'auteur d'une des plus grandes opérations de cyberespionnage, en réussissant à infecter le logiciel Orion de SolarWinds, qui est utilisé notamment par plusieurs branches du gouvernant Etats-Uniens.

NONAME057(16)

Mars 2022

Groupe de hacker russophone qui est spécialisé dans les attaques DDoS. Il est ouvertement pro-Ukraine et s'attaque notamment aux alliés de l'Ukraine. En mars 2023, il a par exemple rendu inaccessible le site internet public de l'Assemblée Nationale. En janvier 2023, le groupe s'est attaqué à plusieurs banques danoises, ce qui a rendu inopérant pour certains leur système bancaire en ligne.

SANDWORM

2004-2007

Groupe de hacker opéré par la section cyber du GRU. Il est connu aussi sous le nom de Telebots, Voodoo Bear ou Iron Viking. Il est présumant derrière l'attaque en décembre 2015 sur le réseau électrique en Ukraine. C'est la première cyber-attaque réussie sur un réseau électrique recencé. Il a réitéré sans succès avec une variante du malware en avril 2022. Il est aussi l'auteur de plusieurs efforts d'interférence dans les élections française en 2017, et les cyberattaques sur les Jeux Olympiques d'Hiver de 2018.

PLAY RANSOMWARE

Juin 2022

Nouveu groupe de hacker, et pourtant déjà beaucoup de hack à leur nom. Il possède un site où il expose chaque hack. Leur mode opératoire est l'infiltration dans les serveurs en utilisant un malware contenu dans un mail, puis exfiltration des données importantes et enfin chiffrement des données. Il menace ensuite de dévoiler les données si la rancon n'est pas payés. Leurs attaques ne sont pas ciblées mais opportunistes, leur but étant uniquement de demander des rancons.

EQUATION GROUP

1996-2000

Groupe de hacker spécialisé dans l'espionnage de haut niveau et probablement lié à la NSA. Son nom vient du fait qu'il utilise des méthodes de chiffrement sophistiqué. Il a infecté pas moins de 42 pays. Ils utilisaient plusieurs failles zero-day, et développé des malwares qui se loge directement dans le firmware des disques durs (résistant au formatage). En 2016, un autre groupe de hacker The Sadow Brokers a dévoilé plusieurs outils d'espionnage leur appartenant. Certains la décrive comme la plus vaste opération de piratage.

COLD RIVER

2016

Groupe de hacker russe qui vise notamment des politiciens, la défense et des organisations gouvernementales, des ONGs, journalistes et activistes, ce qui laisse à supposer qu'il soit en lien avec le Kremlin. Connu aussi sous le nom de Seaborgium ou Calisto. A tenté d'attaquer 3 réacteurs nucléaires Etats-Unien en 2022. À leaké les emails appartenant à l'ancien chef du service d'espionnage britannique MI6 sur les réseaux sociaux afin amplifier de faux récits complotistes.

SHINYHUNTERS

2020

Groupe de hacker principalement composé de français. Son nom vient des chasseurs de Pokémon shiny, un type de Pokémon rare, qui représente ici les données des utilisateurs. En effet, ce groupe est connu pour voler des données et les revendre sur le dark web. Ses victimes sont par exemple le vol de code GH de Microsoft, Pluto TV,Pixlr, Nitro PDF, et à l'origine d'autres dizaines de breach.