François QUIQUET, Architecte Cybersécurité, Bouygues Télécom
Décryptement du jeu du Calendrier 2021 de Global Security Mag

Cette année, le magazine Global Security Mag a organisé un jeu du Calendrier 2021. Il s'agissait de réussir à décoder un message chiffré que vous pouvez télécharger depuis le site du journal. J'ai eu la chance de gagner ce challenge en étant le premier à proposer une solution que je décris ci-dessous.

Merci à Arnaud Lasgorceix et Lazulie (pseudo) pour leur aide précieuse et leur soutien morale pendant cette longue soirée.

Si vous voulez, vous aussi, jouer et tenter de trouver le code alors ne lisez pas la suite de ce message.

Cette année, le message avait été chiffré par **Hervé Lehning** et **Herbert Groscot** de **l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information).**

Le crypto est un PDF de 4 pages. Le début du crypto a la forme suivante :

ICNGI GVDTD OGVOE XEPRR QUITD NWUIU HTKFT SUNGG IWHAT OTRHA TOLGH IGURG REGHL VVDOP

EUHEF UUGXC UUPGO DUWPN WRGVE NUTGR EQQQV LLTHO UVEGT AGHRV WVROI NSEUH SGFSC LLWHL

Le PDF représente des lignes de 14 blocs de 5 caractères soit des lignes de 70 caractères. En tout cela représente 3330 caractères (espace non compris).

Etant amateur de chasse au trésor, je connais certains codes de base souvent utilisés dans ces jeux. En général, on commence toujours par tester tous ces codes les uns après les autres avant de chercher autre chose. C'est ce que j'ai fait ici grâce au site www.decode.fr.

J'ai d'abord fait une analyse des fréquences : G=8%, E=7,4%, U=6,9%, H=6,7%, etc .... Il y a beaucoup de répétitions. A noter, qu'on a également les 26 lettres de présentes. Cela ne représente pas les fréquences d'un texte en français. Il ne s'agit donc pas d'un simple code par transposition, il y a forcément un code par substitution (comme le code césar) ou un mélange des deux.. L'IC (indice de coïncidence) = 0,05037. L'indice de coïncidence est une technique de cryptanalyse qui permet de savoir si un texte a été chiffré avec un chiffre mono-alphabétique ou un chiffre poly-alphabétique ou autre en étudiant la probabilité de répétition des lettres du message chiffré.

Pour tout chiffre monoalphabétique, la distribution des fréquences est invariante, donc l'IC sera le même que pour le texte clair. Idem pour les chiffres de transposition. Donc, si on calcule l'IC d'un texte chiffré avec un chiffre monoalphabétique, on devrait trouver IC égal environ à 0.074 (en français). Si l'IC est beaucoup plus petit (p. ex. 0.050 comme ici), le chiffre est probablement polyalphabétique ou un double chiffrement.

J'ai d'abord commencé par tester quelques codes de base comme le chiffre de Vigenère, le chiffre de Beaufort, le chiffre de Vernam, un 2 carrés, un 3 carrés, etc ... Pour les clés, j'ai testé avec GSMAG, CALENDRIER, ARCSI, etc ... J'ai même testé avec le nom des auteurs : HERVELEHNING et HERBERTGROSCOT. Mais ça n'a rien donné.

J'ai ensuite testé le chiffrement par la scytale spartiate. C'est assez compliqué à décoder car il faut connaitre le nombre de tour. Le déchiffrement par brute force propose en premier une scytale de 15 tours pour obtenir le meilleur résultat. C'est assez étrange car on voit des bouts de mots apparaitre, en particulier on voit souvent le mot NOUILLES.

IDEULFDWLRQGHOD **CONFITURE DE** NOUINNGUOGUFCOGUOGUGHPRLVHOOHVPHVVIEURS
LA CONFITUR GFGPQWKNNGUSWKGVWXQHGHVJORLUHVDE **LA CONFISERIE**
FTCPECKUGTGOQPVGDXQHHSRTXHIRUWO **OINTAINE DAPRES**
LGUTGPUGKIPGOGPVVTXLQRXVRQWHWHF **OMMUNIQUES PARLE**

J'ai ensuite testé un carré de césar par brute force et le meilleur résultat qui sort en premier est également un rectangle de largeur 15. En fait, c'est normal car la scytale spartiate est une application pratique du carré de César.

Ci-dessous, un exemple de scytale spartiate pour comprendre la méthode de chiffrement.

Une scytale de 15 tours correspond donc à un rectangle de césar de largeur 15, c'est à dire avec 15 colonnes. Pour notre texte, il y aura donc 222 lettres par tour de scytale car 222x15=3330.

En faisant quelques recherches sur internet avec les mots que je voyais apparaitre (CONFITURE, CONFISERIE, NOUILLES, etc ...), je suis vite tombé sur le texte de Pierre Dac, " Fabrication de la confiture de nouilles".

Maintenant, il fallait trouver comment passer de

IDEUL FDWLR QGHOD **CONFI TURED ENOUI** NNGUO GUFCO GUOGU GHPRL VHOOH VPHVV
IEURS

à

FABRI CATIO NDELA **CONFI TURED ENOUI** LLESM ESDAM ESMES DEMOI SELLE SMESS **IEURS**

On se rend vite compte qu'il y a des décalages constants.

Première série de 3 blocs, c'est un décalage de 3 (César 3) : IDEUL FDWLR QGHOD => FABRI CATIO NDELA

Deuxième série de 3 blocs, il n'y a pas de décalage (César 0) : CONFI TURED ENOUI => CONFI TURED ENOUI

Troisième série de 3 blocs, c'est un décalage de 2 (César 2) : NNGUO GUFCO GUOGU => LLESM ESDAM ESMES

Quatrième série de 3 blocs, c'est à nouveau un décalage de 3 (César 3) : GHPRL VHOOH VPHVV => DEMOI SELLE SMESS

Et ainsi de suite... J'appelle cela un César différentiel ou un César progressif : César 3 sur la première série de 3 blocs, puis César 0 sur la deuxième série, puis César 2 sur la 3e série et ainsi de suite ...

On voit alors apparaitre :

FABRI CATIO NDELA CONFI TURED ENOUI LLESM ESDAM ESMES DEMOI SELLE SMESS IEURS LACON FITUR EDENO UILLE SQUIE STUNE DESGL OIRES DELAC ONFIS ERIEF RANÇA ISERE MONTE AUNEE POQUE FORTL OINTA INE

qui correspond au début du texte de Pierre Dac suivant :

Fabrication de la confiture de nouilles. Mesdames, Mesdemoiselles, Messieurs, La Confiture de Nouilles, qui est une des gloires de la confiserie française remonte à une époque fort lointaine ....

Voici la solution que j'ai proposée et qui m'a permis de gagner au jeu. Si vous trouvez une solution plus simple ou plus élégante, je suis preneur.

Bravo aux deux auteurs, Hervé Lehning et Herbert Groscot de l'ARCSI. Merci à GSMAG et à Marc Jacob Brami.

Fabrication de la confiture de nouilles, texte de Pierre DAC

Mesdames, Mesdemoiselles, Messieurs,

La confiture de nouilles, qui est une des gloires de la confiserie française, remonte à une époque fort lointaine ; d'après les renseignements qui nous ont été communiqués par le conservateur du Musée de la Tonnellerie, c'est le cuisinier de Vercingétorix qui, le premier, eut l'idée de composer ce chef-d'œuvre de gourmandise.

Il faut reconnaître d'ailleurs que la nouille n'existant pas à cette époque, ladite confiture de nouilles était faite du gui ; mais alors, me diront les ignorants : « Ce n'était pas de la confiture de nouilles, c'était de la confiture de gui ! » « Erreur », que je leur répondrai, « c'était de la confiture de nouilles fabriquée avec du gui. »

Avant d'utiliser la nouille pour la confection de la confiture, il faut évidemment la récolter ; avant de la récolter, il faut qu'elle pousse, et pour qu'elle pousse, il va de soi qu'il faut d'abord la semer. Les semailles de la graine de nouille, c'est-à-dire les senouilles, représentent une opération extrêmement délicate.

Tout d'abord, le choix d'un terrain propice à la fécondation de la nouille demande une étude judicieusement approfondie. Le terrain nouillifère type doit être, autant que possible, situé en bord de route départementale et à proximité de la gendarmerie nationale.

Les senouilles sont effectuées à l'aide d'un poêle mobile dans lequel est versée la graine, laquelle est projetée dans la terre par un dispositif spécial dont il ne nous est pas permis de révéler le secret pour des raisons de défense nationale que l'on comprendra aisément. Après cela, on

arrose entièrement le champ avec de l'eau de seltz dans la proportion d'un verre à bordeaux par hectare de superficie, on sèche avec du papier buvard, et on n'a plus qu'à s'en remettre au travail de la terre nourricière généreuse et démocratique.
Lorsque les senouilles sont terminées, les nouilliculteurs, qui sont encore entachés de superstition, consultent les présages ; ils prennent une petite taupe et la font courir dans l'herbe. Si elle fait : « ouh ! », c'est que la récolte sera bonne ; si elle ne fait pas « ouh ! » c'est que la récolte sera bonne tout de même, mais comme cela les croyances sont respectées, et tout le monde sera content.
Au mois d'août vient alors le temps de la moisson. Celui qui n'a pas vu moissonner les nouilles n'a rien vu. Les paysans mettent les nouilles joyeusement en gerbes, les gerbes en bottes, et les bottes en meule.
La nouille, encore à l'état brut, est alors expédiée à l'usine et passée immédiatement au laminouille qui lui donne l'aspect définitif que nous lui connaissons. Le laminouille est une machine extrêmement perfectionnée, qui marche au guignolet-cassis et qui peut débiter jusqu'à 80 kilomètres de nouilles à l'heure.
À la sortie du laminouille, la nouille est automatiquement passée au vernis cellulosique qui la rend imperméable et souple ; elle est ensuite hachée menue à la hache d'abordage et râpée.
On verse alors la nouille dans un grand récipient placé sur un réchaud à alcool à haute tension. Puis on verse dans le fût du récipient : du sel, du thym, du sucre, de la magnésie bismurée, du riz, du vin blanc et des piments rouges. On mélange lentement ces ingrédients avec la nouille à l'aide d'une cuiller à pot et on laisse mitonner à petit feu pendant 21 jours.
La confiture de nouilles est alors virtuellement terminée. Lorsque les 21 jours sont écoulés, on saisit le récipient très délicatement, avec d'infinies précautions et le maximum de prudence, et on balance le tout par la fenêtre parce que c'est pas bon !

Voilà, Mesdames, Mesdemoiselles, Messieurs, en résumé l'histoire de la confiture de nouilles, c'est une industrie dont la prospérité s'accroît d'année en année, elle fait vivre des milliers d'artisans, des ingénieurs, des chimistes, des huissiers et des fabricants de lunettes. Sa réputation est universelle et en bonne ambassadrice, elle va porter dans les plus lointaines contrées de l'univers, et par-delà les mers océanes, la bonne parole et le renom de notre industrie républicaine, une, indéfectible et démocratique.