Un peu de cryptographie et cryptanalyse...

Vocabulaire :

Quand on veut savoir en sciences de quoi parle tel ou tel domaine souvent l'étymologie peut nous aider :

1. *crypto* = caché en grec
2. *graphie* = écriture en grec
3. *analyse* = "casser"

D'où *cryptographie*= art ou science de transformer des textes "en clair" en des textes "cachés" , on dit aussi "chiffrés" et *cryptanalyse*= art de "déchiffrer " des textes "chiffrés"

A quoi sert la cryptographie ?

Dans le passé, cela a servi à "cacher" les communications entre les militaires d'un même pays ou politiques d'un même parti. De nos jours la cryptographie sert en plus à protéger les informations contenues sur les cartes vitales, à protéger le commerce en ligne, les communications entre téléphones mobiles, les mots de passe sur un ordinateur, les communications wi-fi etc...

Le contexte général est le suivant :

Deux entités A pour Alice et B pour Bob communiquent en présence d'un observateur éventuel ou cryptanaliste Oscar.

Exemples pour A : un sous-marin , une ambassade, une entreprise, un ordinateur personnel...

Exemples pour B : l'état-major du sous-marin, le ministère, le siège administratif de l'entreprise, un serveur...

$A \rightarrow$ message en clair $M \rightarrow$ cryptogramme ou message chiffré $C \rightarrow$ déchiffrement $M \longrightarrow B$

$\uparrow$

O observateur

1 Cryptographie à clef secrète : séance 1

Histoire

1. Chiffrement par décalage ou chiffrement de César

   Alphabet clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ

   Alphabet chiffré :DEFGHIJKLMNOPQRSTUVWXYZABC

   Quel est la logique de l'alphabet chiffré ?Puis on va remplacer chaque lettre du message en clair par celle correspondante dans l'alphabet chiffré.

   Chiffrer le message suivant :"Bientôt les vacances".

   Quel problème apparaît ?

2. Cryptanalyse du chiffrement par décalage :

   Il semble que ce soit un scientifique arabe Al-Kindi (IX siècle) qui eut l'idée pour déchiffrer un message chiffré par substitution, **chaque lettre de l'alphabet est remplacé par une autre** :

   "Si nous savons dans quelle langue est écrite le message chiffré, il nous suffit de comparer les fréquences d'apparition des lettres de l'alphabet chiffré à celles de l'alphabet clair dans la langue du message

   Par exemple en Français la lettre E est la plus fréquente avec une fréquence approximative de 15 %, si dans le message chiffré la lettre Z est la plus fréquente , il y a de fortes chances que le Z remplace le E.

   Tableau de fréquences :

Lettres	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Fréq(%)	9,5	1	2,5	3,5	15	1	1	0,8	8,5	1	0	5,5	3,5	7	5	2,8	1	6,5	8	7	6

Lettres	V	W	X	Y	Z
Fréq(%)	2	0	...	...	...

   A vous de jouer. Déchiffrer :

   Message crypté : HJXFW FZWFNY JYJ HTSYJSY IJ ATZX !

   Quel problème statistique pose cette méthode de déchiffrement ? Dans quelle mesure un échantillon ressemble à une population ?

   Quel problème poserait le chiffrement du roman , *La disparition*, de Georges Perec, où ne figure aucune lettre e ?

3. Chiffrement avec une clé :

   Combien y -a-t-il de possibilités de chiffrer par décalage ? Si on décide de permuter toutes les lettres de l'alphabet, il y a $26 ! = 26 \times 25 \times ... \times 3 \times 2 \times 1$ possibilités soit environ 10^{26} possibilités

   Un exemple de chiffrement avec une clé : On choisit un mot ou une phrase clé par exemple "JULES CESAR " on supprime les blancs et les lettres répétées et on obtient"JULESCAR" c'est la **clé** que l'on place en tête de l'alphabet chiffré ainsi on a :

   Alphabet clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ

   Alphabet chiffré :JULESCARTVWXYZBDFGHIKMNOPQ

Quel est la logique de la clé ? Chiffrer le message suivant :"Bientôt les vacances".

Plus généralement la clé est une des 26 ! permutations possibles.

Proposer votre clé est chiffrer le message ci-dessus avec

4. Cryptanalyse d'un chiffrement monoalphabétique par substitution

   Message crypté 1 :MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ KPJABT HYJHUBT LZA ULBAYVU

   Message crypté 2 : BAELXEJ JCKJ ZA JANBH HSXGXWXL XMXPJ LCEEA XK GCP JGCPH DPOH. FKXEL AOOA AKJ JAGNPEA O'SPHJCPH LA NX'GKD OA HXMAJPAG,AOOA HA OAMX, YXPHX OA HCO LAMXEJ OA HCKMAGXPE AJ OKP LPJ : "IGXEL GCP, LABKPH NPOOA AJ KEA EKPJH RA J'XP GXZCEJA OAH OAIAELAH LAH GCPH BXHHAH BKPH-RA NA BAGNAJJGA LA HCOOPZPJAG KEA DXMAKG LA MCJGA NXRAHJA ?"
   ABPOCIKA-ZCEJAH LAH NPOOA AJ KEA EKPJH

5. Chiffrement de Vigenère

   A la fin du XV ième siècle le match est nul entre la cryptographie et la cryptanalyse, autrement dit aucune méthode de chiffrement n'est véritablement sûr. Blaise de Vigenère, né en 1523, un diplomate français eut alors l'idée du chiffrement **polyalphabétique**.

   Carré de Vigenère :(fourni en annexe) : est constitué d'un tableau 26 x 26 où à la ligne k avec $1 \leq k \leq 26$ se trouve l'alphabet clair décalé de k crans

   Exemple de chiffrement avec le carré de Vigenère :

   Soit le message en clair "Envoyer troupes nord ville" avec la clé "Rouge" . On écrit au-dessus du message en clair la clé "en boucle", afin d'associer à chaque lettre du message en clair une lettre de la clé.

   Ainsi à la première lettre du message E est associé la lettre R qui définit la ligne 17 du carré de Vigenère, on va donc utiliser alphabet chiffré à la ligne 17 pour chiffrer la lettre E, on obtient ainsi la lettre V.

   Finir de chiffrer le message.

   Clé : ROUGEROUGEROUGEROUGERO

   Clair ENVOYERTROUPESNORDVILLE

   Crypté VB

   Exercice Vous avez reçu le message crypté suivant :"SMMYKMYTJ" par le carré de Vigenère et la clé RIME. Déchiffrer le.

6. Cryptanalyse du chiffre de Vigenère

   Le E dans le chiffrement ci-dessus ne sera pas codé de la même façon et pourra soit être remplacé par soit V (ligne 17) soit S (ligne 14) soit Y (ligne 20) soit K (ligne 6) soit I (ligne 4), ce qui rend inutilisable la méthode des fréquences .

   Charles Babbage (qui parait -il eut l'idée des ordinateurs) a réussi la cryptanalyse du chiffre de Vigenère au XIX ième siècle en cherchant la clé c'est à dire les lignes du carré de Vigenère.

7. Le Chiffrement, une histoire d'Hommes originaux et tenaces et de machines originales

   D'autres techniques de chiffrement ont existé parallèlement à ceux que l'on a vu précédemment (voir le livre Histoire des codes secrets de Simon Singh) et avec l'apparition de nouveaux moyens de communication (télégraphie) le besoin de mécaniser la cryptographie se fit sentir (et par voie de conséquence de mécaniser la cryptanalyse).

2 Cryptographie à clef publique : séance 2

Jusqu'à présent pour échanger des messages cryptés l'émetteur et le récepteur devaient partager un secret. C'est le principe de Kerckhoffs(1883) :"La sécurité d'un système de cryptement ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clé."Aussi les gouvernements ont fait beaucoup d'efforts pour l'acheminement des clés.

Jusqu'au jour où quelques individus ont remis en cause le principe de Kerckhoffs.

1. Dieu bénit les fous : "*Comme nous, Ralph était un peu fou. Il faut être fou pour mener jusqu'au bout une recherche originale, et seuls des fous la poursuivront envers et contre tout. Vous avez une première idée, vous vous enthousiasmez, et ça ne marche pas. Alors vous passez à l'idée numéro 2, vous vous enthousiasmez, et ça ne marche pas. Alors vous avez l'idée 99, vous vous enthousiasmez, et ça ne marche pas. Seul un fou sera encore enthousiaste à sa centième idée, et il faudra peut-être avoir essayé cent voies avant que l'une conduise quelque part. A moins d'être assez fou pour retrouver à chaque fois tout votre enthousiasme, vous vous découragerez, et n'aurez pas l'énergie de mener les choses jusqu'au bout. Dieu bénit les fous.*"(Martin Hellman, professeur d"informatique à l'université de Stanford - Californie (1975))
   Whitfield Diffie, Ralph Merkle et Martin Hellman sont les co-inventeurs de la cryptographie à clef publique en 1976.
2. Une anecdote : Alice envoit un message à Bob. Elle met le message dans un coffret qu'elle ferme avec son cadenas dont elle a la clé et elle seule, puis l'envoie à Bob. Lorsque le coffret arrive à Bob celui -ci ajoute son propre cadenas et renvoie la boîte à Alice. Cette dernière retire **son** cadenas et retourne le coffret à Bob. Maintenant Bob peut ouvrir le coffret puisqu'il a **la** clé du cadenas.
3. Conséquences : Tester l'anecdote précédente : Prendre pour Alice le chiffrement "$x+3$" et pour Bob le chiffrement "$x+5$" le message d'Alice est "rdv a midi place du marché".
   Qu'observez vous ?Quelle est la différence entre la situation avec les cadenas et celle ci-dessus ?
4. Pour chiffrer avec une clé publique tout en résistant aux tentatives d'Oscar pour déchiffrer Diffie et Hellman cherchèrent des fonctions mathématiques *à sens unique*.
   Inverser les fonctions f, g, h définies par $f(x) = 2x + 1$ sur $\mathbb{R}$, puis $g(x) = (x-1)^2$ sur $[1; +\infty[$ puis $h(x) = \dfrac{1}{x-1}$ sur $[1; +\infty[$
   Une fonction à sens unique est inversible mais *concrètement* difficilement inversible, c'est à dire que le temps mis pour obtenir la valeur de l'antécédent à partir d'une valeur donnée, sera "très grand".
5. Le Protocole de Diffie-Hellman (1976)
   Alice et Bob vont utiliser une méthode traditionnelle de chiffrement à clé secrète S mais **ils veulent que cette clé ne soit pas acheminée mais déduite par eux seuls par calcul.**
   a) Alice et Bob se mettent d'accord **publiquement** sur un "grand" nombre premier p (ici on prendra $p = 7$) et une racine primitive modulo p soit r (ici $r = 3$)
   b) Alice choisit un nombre a **secret**, connu d'elle seule. Choisissez $a =$ .... (de 1 à 6). Et elle transmet à Bob et à qui veut l'entendre le nombre $\alpha = r^a \mod p$.
      Que vaut ici $\alpha = 3^a \mod 7 =$.....?
   c) Bob choisit de même un nombre b **secret** et connu de lui seul,et transmet à Alice $\beta = r^b \mod p$. Choisir une valeur pour b. $b =$ .....
      $\beta =$ .....

d) Ici est le coeur du protocole : **la clé secrète** S **est** $S = \alpha^b \bmod p = \beta^a \bmod p$
$\alpha^b \bmod 7 =$ ..... et $\beta^a \bmod 7 =$ .....
Autrement dit Alice prend ce que lui a envoyé Bob , c'est à dire β et l'élève à la puissance "le nombre secret" d'Alice et obtient la clé secrète S qui servira à chiffrer.
De même Bob prend ce que lui a envoyé Alice, c'est à dire α et l'élève à la puissance "le nombre secret" de Bob et obtient ô miracle mathématique le même nombre S

e) Oscar a peut-être intercepté les valeurs de p puis r puis r^a puis r^b mais il arrivera difficilement à obtenir a à partir de α ou b à partir de β, parce que l'exponentiation modulaire est une fonction à sens unique.

f) Inconvénient : Le chiffrement ne peut commencer que lorsque la clé S est connu ce qui nécessite une communication préalable entre les deux personnes ce qui n'est pas toujours possible. Le chiffrement est symétrique.

6. Le cryptosystème RSA (Rivest, Shamir, Adleman) (1977). Chiffrement asymétrique et à clé publique

a) Alice et Bob ont chacun leurs clés publiques P_A et P_B et leurs clés secrètes S_A et S_B. Ces clés sont des **paires** d'entiers.

b) Les clés d'Alice (et de même pour Bob) définissent des fonctions $P_A()$ et $S_A()$ à sens unique, **commutatives** c'est à dire :

$$S_A(P_A(M)) = P_A(S_A(M)) = M$$

c) Supposons que Bob veuille envoyer un message M chiffré à Alice. Il se procure la clé publique d'Alice P_A comme un numéro de téléphone dans un annuaire.

d) Bob calcule le texte chiffré $C = P_A(M)$ et envoie C à Alice.

e) Lorsque Alice reçoit C elle calcule $S_A(C) = S_A(P_A(M)) = M$ et elle a accès au texte en clair M.