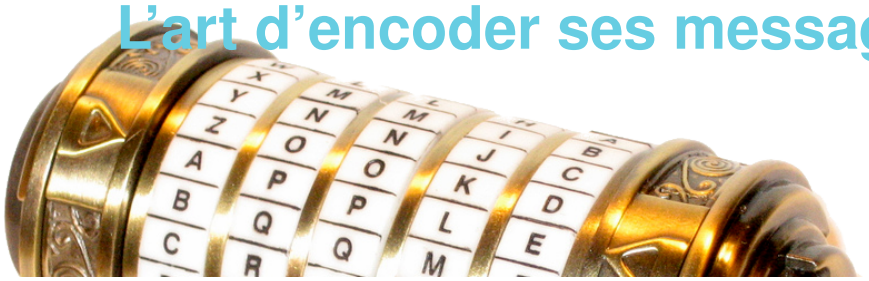
printemps des sciences '16
les sciences à portée de main

L'art d'encoder ses messages



Autre exemple de chiffrement : Vigenère

- Le chiffrement de César est très vulnérable :
  1. il y a peu de clés,
  2. une analyse fréquentielle triviale brise le code.
- Solutions possibles :
  1. augmenter le nombre de clés,
  2. un caractère ne doit pas être toujours codé de la même façon.
- Le chiffrement de Vigenère pallie à ces défauts.
  - Tient bon jusque fin du XVIII^{e} siècle.
  - Une partie du chiffrement des japonais durant la seconde guerre mondiale repose sur ce chiffrement.
- Idée : César à décalage variable.

Vigenère : cryptanalyse

- Ici, on ne peut plus tester toutes les clés.
  - Il y a trop de possibilités, les tester prendrait trop de temps.
- On sait que Vigenère est un « César à décalage variable ».
- On veut se ramener à cet algorithme simple.
- On doit trouver la longueur de la clé.
- Si on trouve cette longueur, on peut appliquer César sur des sous-morceaux de texte.

Exemple

- Si la clé est de longueur 4, on fait 4 analyses fréquentielles :
  1. la première sur le texte composé des caractères en positions $1, 5, 9, 13, \ldots$,
  2. la deuxième sur le texte composé des caractères en positions $2, 6, 10, 14, \ldots$,
  3. la troisième sur le texte composé des caractères en positions $3, 7, 11, 15, \ldots$,
  4. la quatrième sur le texte composé des caractères en positions $4, 8, 12, 16, \ldots$
- Si le texte est suffisamment long, les résultats seront probants.
- Ces quatre analyses fréquentielles vont fournir le texte d'origine, sans connaître la clé.

Comment trouver la longueur de la clé ?

- Repérer des répétitions dans le texte.
  - Choisir une courte longueur (p. ex., 3) pour les répétitions.
- Ces répétitions peuvent arriver dans deux cas de figure.
  1. Du hasard. Dans un tel cas, on ne peut tirer aucune information de la répétition.
  2. Un même morceau de texte clair a été codé par un même morceau de clé.
- Si le texte est suffisamment long,
  - le risque de répétitions dues au hasard est minimisé,
  - la probabilité d'avoir d'autres répétitions augmente.
- Quelle information peut-on tirer d'une répétition de type « même bout de texte codé par le même bout de clé » ?

Vigenère : l'algorithme

- La clé est un mot, par exemple : « HECM ».
- Les lettres de la clé dénotent chacune un décalage.
  1. « HECM » = $(8, 5, 3, 14)$.
  2. La première lettre du texte est décalée de 8,
  3. la deuxième lettre du texte est décalée de 5,
  4. la troisième lettre du texte est décalée de 3,
  5. la quatrième lettre du texte est décalée de 14,
  6. la cinquième lettre du texte est décalée de 8, etc.
- César : Vigenère avec des clés de longueur 1.
- Une analyse de fréquence « basique » ne sert à rien car une lettre n'est pas toujours encodée par un même caractère.

Exemple

- Avec la clé « INFO », on encode de la façon suivante

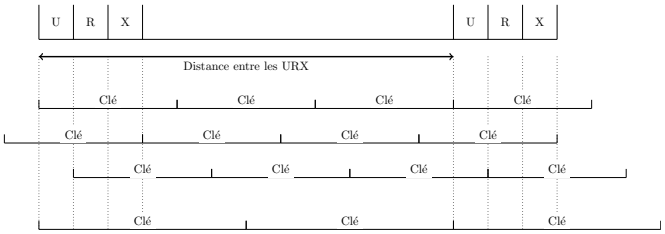
	Texte clair																									
clé	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

- Exemple de chiffrement

Texte clair	JOURNEE MATH SCIENCES
Clé	INFOINF OINF OINFOINF
Texte chiffré	RBZFVRJ AIGM GKVJBKRX

Exploiter les répétitions

- Si la distance entre deux répétitions vaut k, alors la longueur de la clé divise k.
- On a « recopié » la clé un nombre entier de fois entre les répétitions.



- Ici, exemple avec une distance de 12 et des clés de longueur 4 et 6.
- Fonctionne aussi avec 3, ainsi que 1, 2 et 12.

Les répétitions en pratique

Texte clair	MES EXPOSES SONT TOUJOURS LIMPIDES ET MES DIX ETUDIANTS COMPRENNENT TOUT
clé	INF OINFOIN FOIN FOINFOIN FOINFOIN FO INF OIN FOINFOINF OINFOINFOIN FOIN
Texte chiffré	URX SFCTGMF XCVG YCCWTIZF QWUCNRMF JH URX RQK JHCQNOVGX QWZUFMASSVG YCCG

- Distance entre les URX : 32, distance entre les YCC : 44
- On choisit le diviseur commun le plus grand entre les distances : $PGCD(32, 44) = 4$.
- On a trouvé la longueur de la clé ! Il n'y a plus qu'à appliquer 4 analyses fréquentielles.
- Essayez l'exemple interactif !

heb

esi

La sécurité à l'ESI

- Trois bacheliers (3 ans) centrés sur du développement informatique soigné.
- Diplôme « orienté pratique », professionnalisant.
- Trois finalités répondant aux sensibilités des étudiants :
  - informatisation des organisations,
  - informatisation des réseaux et télécommunications,
  - informatisation des processus industriels.
- Cours contextualisés pour les thématiques connexes.
- Plusieurs thématiques de sécurité au sein de certains cours.
- Un cours « Éléments de sécurité » en 3^{e} industrielle.
- Les stages en entreprise peuvent être liés à la sécurité (stage à la police, etc.)
- Une année de spécialisation en sécurité en horaires adaptés, avec étalement possible.
- Ouverture d'un Master (2 ans) en cybersécurité en 2016-2017, en co-diplomation avec des universités et hautes-écoles.