R4.Cyber.10 - Cryptographie

Définition

La cryptographie est la science qui vise à protéger l'information en la rendant illisible à toute personne qui n'a pas les moyens de la déchiffrer.

Principe de Kerkoffs

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Crypter ou hacher ?

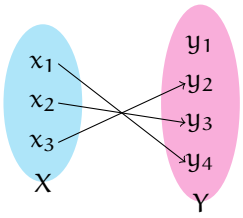
Définition

Soit $f : X \to Y$ une application.

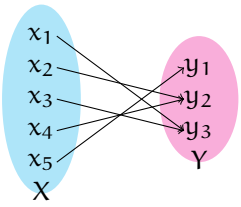
Injection (hacher). $\forall x, x'\ f(x) = f(x') \Rightarrow x = x'$

Surjection. $\forall y \in Y,\ \exists x \in X,\ f(x) = y$

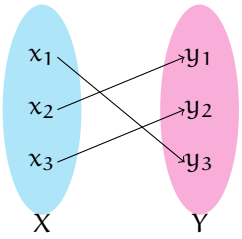
Bijection (crypter). $\forall y \in Y,\ \exists! x \in X,\ f(x) = y$



Injection



Surjection



Bijection

Chiffrement de César

La fonction de chiffrement est

$$C(x) \equiv_{26} x + 7$$

Cara	R	E	S	E	A	U	X
x	17	4	18	4	0	20	23
+7	24	11	25	11	7	27	30
%26	24	11	25	11	7	1	4
Cara	Y	L	Z	L	H	B	E

La réciproque est la fonction de déchiffrement.

$$D(x) \equiv_{26} x - 7$$

Cara	Y	L	Z	L	H	B	E
x	24	11	25	11	7	1	4
x − 7	17	4	18	4	0	−6	−3
%26	17	4	18	4	0	20	23
Cara	R	E	S	E	A	U	X

Le 7 est appelé la **clef** de chiffrement.

Inverse modulaire

Définition

L'inverse d'un nombre modulaire x est un nombre modulaire y tel que $xy \equiv 1$.

Exemple : $3 \times 9 \equiv_{26} 1$ donc $\frac{1}{3} \equiv_{26} 9$ et $\frac{1}{9} \equiv_{26} 3$.

Pour déterminer l'inverse modulaire d'un entier, on applique l'algorithme d'Euclide étendue. Détaillons un exemple et cherchons l'inverse de 382 modulo 2365. On va commencer par réaliser des divisions euclidienne successives. On initialise dans ce tableau en plaçant les valeurs données.

a	b	r	q
2365	382		

On réalise une division euclidienne en notant le reste et le quotient.

a	b	r	q
2365	382	73	6

On va ensuite, sur la ligne suivante, décaler les valeurs

a	b	r	q
2365	382	73	6
382	73		

On réalise à nouveau une division et ce jusqu'à ce que le dernier des reste soit 0

a	b	r	q
2365	382	73	6
382	73	17	5
73	17	5	4
17	5	2	3
5	2	1	2
2	1	0	2

Si le dernier b n'est pas 1 alors l'inversion n'est pas possible

Dans notre exemple, puisque le dernier $b = 1$, on en déduit qu'il existe un inverse modulaire. Pour le trouver nous allons rajouter au tableau deux colonnes u et v. On va remplir ce tableau par le bas en initialisant u et v par 0 et 1 respectivement.

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3		
5	2	1	2		
2	1	0	2	0	1

On va remplir la ligne du dessus. On va mettre la valeur de v dans la nouvelle case de u. Pour la nouvelle valeur de v on va mettre $-q \times u_{NEW} + u_{OLD}$ où u_{NEW} représente le nouveau u (ici 1) et u_{OLD} l'ancienne valeur (ici 0).

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3		
5	2	1	2	1	−2
2	1	0	2	0	1

On recommence : à la ligne de dessus, on place l'ancienne valeur de v comme nouvelle valeur de u et pour la nouvelle valeur de v le résultat de $-q \times u_{NEW} + u_{OLD}$. Ici $u_{NEW} = -2$ et $u_{OLD} = 1$.

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3	−2	7
5	2	1	2	1	−2
2	1	0	2	0	1

On peut vérifier qu'à chaque ligne $au + bv = 1$ (par exemple, notre dernier calcul permet d'aboutir à $17 \times (-2) + 5 \times 7 = 1$).

On réitère pour aboutir à :

a	b	r	q	u	v
2365	382	73	6	157	−972
382	73	17	5	−30	157
73	17	5	4	7	−30
17	5	2	3	−2	7
5	2	1	2	1	−2
2	1	0	2	0	1

Nous avons donc trouvé : $2365 \times 157 + 382 \times (-972) = 1$. Pour finir -972 est l'inverse modulaire de 382. On peut choisir un représentant positif : $-972 \equiv_{2365} -972 + 2365 = 1393$ et on peut donc conclure que l'inverse de 382 modulo 2365 est 1393.

Chiffrement affine

La fonction de chiffrement est

$$C(x) \equiv_{26} 3x+1$$

Cara	R	E	S	E	A	U	X
x	17	4	18	4	0	20	23
3x	51	12	54	12	0	60	69
3x+1	52	13	55	13	1	61	70
%26	0	13	3	13	1	9	18
Cara	A	N	D	N	B	J	S

La réciproque est la fonction de déchiffrement. L'inverse de 3 modulo 26 est 9 car $3 \times 9 \equiv_{26} 1$

$$D(x) \equiv_{26} 9(x-1)$$

Cara	A	N	D	N	B	J	S
x	0	13	3	13	1	9	18
x−1	−1	12	2	12	0	8	17
9(x−1)	−9	108	18	108	0	72	153
%26	17	4	18	4	0	20	23
Cara	R	E	S	E	A	U	X

Le couple $(3,1)$ est appelé la **clef** de chiffrement.

Algorithme d'exponentiation modulaire rapide

§
Écrire n en binaire : $n = \sum_{i=0}^{k} a_i 2^i$

```
Pour i de 0 à k
          Si i=0
               poser x[0] = x modulo m
          Sinon
               x[i] = x[i-1]*x[i-1] modulo m
          Fin Si
Fin pour
res = 1
Pour i de 0 à k
          Si a_i=1
               res = res*x[i] modulo m
          Fin Si
Fin pour
Renvoyer res
```

Par exemple calculons 19^{19} modulo 2017.

Ecriture binaire. La première étape consiste à écrire 19 en binaire ce qui se fait par division euclidienne successive. On trouve $19 = (10011)_2$.

Calcul des puissances de puissance de 2. On représente la situation dans un tableau

k	0	1	2	3	4
2^k					
mod					

où la dernière ligne est la seconde ligne modulo $m = 2017$. Le tableau va jusqu'à $k = 4$ car c'est la plus grande puissance de 2 qui apparait dans l'écriture binaire de 19. On l'initialise de la sorte

k	0	1	2	3	4
2^k	19				
mod	19				

On prend la valeur de la dernière ligne de la colonne k que l'on met au carré et que l'on inscrit dans à la seconde ligne de la colonne k+1 et on calcul la réduction modulo m à la dernière ligne.

k	0	1	2	3	4
2^k	19	361			
mod	19	361			

On itère le processus.

k	0	1	2	3	4
2^k	19	361	130321		
mod	19	361	1233		

k	0	1	2	3	4
2^k	19	361	130321	1520289	
mod	19	361	1233	1488	

k	0	1	2	3	4
2^k	19	361	130321	1520289	2214144
mod	19	361	1233	1488	1495

Conclusion. Les puissances de 2 apparaissant dans l'écriture binaire de 19 sont 0, 1 et 4 on a donc $19^{19} \equiv_{2017} 19 \times 361 \times 1495 \equiv_{2017} 808 \times 1495 \equiv_{2017} 1794$

RSA

Liste de nombres premiers inférieur à 100

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Définition

Soient $p < q$ deux nombres premiers. Notons $n = pq$ et $\varphi(n) = (p-1)(q-1)$ et choisissons un nombre e inversible modulo $\varphi(n)$. On note $d \equiv_\varphi \frac{1}{e}$.

Fonction de chiffrement. $C(M) \equiv_n M^e$.

Fonction de déchiffrement. $D(M) \equiv_n M^d$.

Exemple

Dans le système RSA, on dispose de la clef publique $(1147, 743)$ ainsi que du message 25. Pour chiffrer ce message il faut calculer 25^{743}. L'écriture binaire de 743 est $(1011100111)_2$. Appliquons l'algorithme d'exponentiation modulaire rapide :

k	0	1	2	3	4	5	6	7	8	9
25^{2^k}	25	625	390625	416025	657721	240100	142129	1098304	390625	416025
mod 1147	25	625	645	811	490	377	1048	625	645	811

Ainsi $25^{743} \equiv_{1147} 25 \times 625 \times 645 \times 377 \times 1048 \times 625 \times 811 \equiv_{1147} 67$ qui est donc me message crypté.