

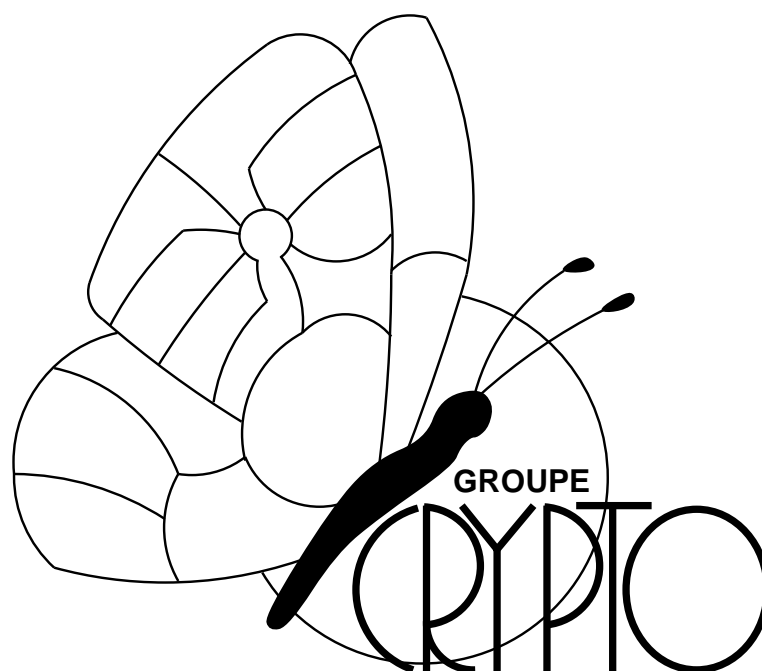


UCL
Université
catholique
de Louvain



Comment jouer à pile ou face sur Internet sans tricher ?

J.-M. Boucqueau, J.-F. Delaigle, J.-F. Dhem, M. Joye,
F. Koeune, H. Massias, P. Mestré et J.-J. Quisquater



<http://www.dice.ucl.ac.be/crypto/>

Technical Report
CG-1997/2

Comment jouer à pile ou face sur Internet sans tricher ?

J.-M. Boucqueau, J.-F. Delaigle, J.-F. Dhem, M. Joye,
F. Koeune, H. Massias, P. Mestré et J.-J. Quisquater

2 octobre 1997

Département d'Électricité (DICE), Université catholique de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium

1 Que signifie travailler modulo un entier ?

Considérons l'ensemble \mathbb{Z} des entiers relatifs. Représentons-le par une droite.

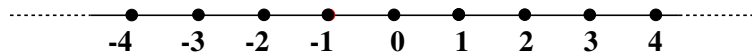


FIG. 1 – *Droite représentant \mathbb{Z} .*

Travailler modulo n revient à enrouler la droite représentant \mathbb{Z} (figure 1) sur un cercle contenant n points (voir figure 2 pour un exemple où $n=5$). Les nombres relatifs sont donc maintenant représentés par n valeurs (voir figure 2 pour l'exemple où $n = 5$). Dans cet exemple, $6=1$, $12=2$, $-17=3$, $24=4$, $45=0$. On note :

$$6 \equiv 1 \pmod{5}, \quad 12 \equiv 2 \pmod{5}, \quad -17 \equiv 3 \pmod{5},$$

et on lit 6 congrue à 1 modulo 5, 12 congrue à 2 modulo 5, -17 congrue à 3 modulo 5. On peut maintenant effectuer les opérations habituelles sur les nombres :

$$4 + 3 \equiv 2 \pmod{5}, \quad 3 \cdot 2 \equiv 1 \pmod{5}.$$

Combien valent 525 ou 637 modulo 5 ?

Pour calculer ceci on enroule la droite représentant \mathbb{Z} sur un cercle contenant 5 points. Comme on vient de voir qu'en effectuant un tour du cercle

CG-1997/2

©1997 by UCL Crypto Group

For more informations, see

<http://www.dice.ucl.ac.be/crypto/techreports.html>

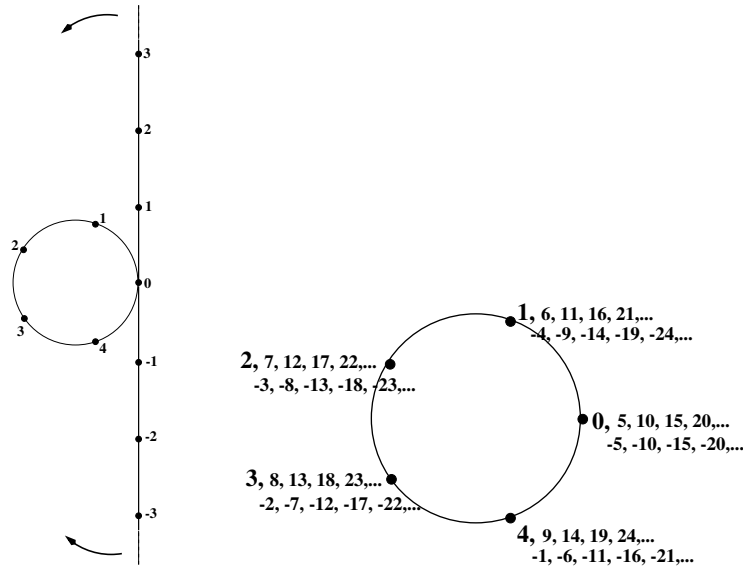


FIG. 2 – Représentation modulo.

la valeur obtenue ne change pas, nous allons compter le nombre de tours nécessaires afin de poser 525 ou 637 sur le cercle. Puis nous regarderons à quelle position du cercle nous sommes arrivés.

Compter le nombre de tours revient à calculer le quotient de la division euclidienne de 525 et de 637 par 5. *Regarder la position* revient à calculer le reste de cette même division.

En définitif, raisonner modulo revient à ne considérer que le reste de la division du nombre que l'on considère par la valeur du modulo. On obtient :

$$525 = 105 \cdot 5 + 0, \quad 637 = 127 \cdot 5 + 2$$

donc

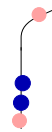
$$525 \equiv 0 \pmod{5}, \quad 637 \equiv 2 \pmod{5}.$$

On peut tout de suite déduire de cette remarque que lorsque l'on considère l'entier x tel que $x \equiv 2 \pmod{5}$, nous savons alors qu'il existe un entier k tel que $x = 2 + 5k$.

1.1 Petit théorème de Fermat

Nous allons fabriquer un collier de p perles avec des perles de 2 couleurs.

Regardons ce qu'il se passe avec $p = 5$.



On enfile 5 perles une à une. Pour la première perle on a le choix entre 2 couleurs, pour la deuxième aussi et ainsi de suite jusqu'à la cinquième. On peut donc fabriquer $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$ colliers différents. Mais attention un collier n'a ni début ni fin et des configurations qui étaient différentes lorsque l'on a construit le collier deviennent identiques lorsque l'on lie les deux extrémités.

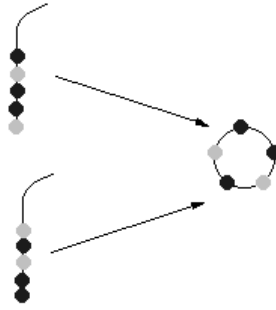


FIG. 3 – Fermeture des colliers.

Comptons maintenant le nombre de configurations différentes et le nombre de fois où chacune est obtenue (voir table 1).

Configuration											
Nombre de fois	1	5	5	5	5	5	5	5	5	5	1

TAB. 1 – Les différentes configurations pour $p = 5$

Nous venons de classer tous les colliers que l'on peut fabriquer et on a compté le nombre de fois qu'ils sont obtenus. On a vu qu'il y a 2^5 colliers possibles, on obtient donc $2^5 = 1 + 5 + 2 \cdot 5 + 2 \cdot 5 + 5 + 1 = 2 + 6 * 5$, et on en déduit ainsi

$$2^5 \equiv 2 \pmod{5}.$$

On peut étendre ceci avec 3 ou 4 couleurs de perles, ou de façon plus générale :

$$\text{pour tout } a, 0 \leq a < 5, a^5 \equiv a \pmod{5}.$$

Définition 1 *Un nombre premier est un entier naturel (différent de 1) qui n'est divisible que par 1 et lui-même.*

Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 23, ...














En généralisant ce que l'on vient de voir à tous les nombres premiers, on obtient le théorème suivant.

Théorème 1 *Pour tout nombre premier p , on a*

$$\text{pour tout entier } a, \text{ avec } 0 \leq a < p, a^p \equiv a \pmod{p}.$$

Attention lorsque p n'est pas premier cette relation n'est pas vérifiée pour tout a . Pour illustrer ceci, fabriquons un collier de 6 perles avec 2 couleurs.

Comme tout à l'heure, étudions les différentes configurations et le nombre de fois où chacune est obtenue (voir table 2).

		
1		1
		
6		6
		
6	6	3
		
6	6	2
		
6	6	3

TAB. 2 – Les différentes configurations pour $p = 6$

En faisant le même raisonnement que précédemment, on obtient donc $2^6 = 1 + 6 + 2 \cdot 6 + 3 + 2 \cdot 6 + 1 + 6 + 2 \cdot 6 + 3 + 2 = 4 + 2 \cdot 3 + 6 \cdot 8$, et on en déduit ainsi

$$2^6 \equiv 10 \pmod{6}$$

ce qui nous donne

$$2^6 \equiv 4 \pmod{6}.$$

Du théorème 1 on déduit le *petit théorème de Fermat*.

Théorème 2 (Petit théorème de Fermat) *Pour tout nombre premier p ,*

$$\text{pour tout } a, 0 < a < p, a^{p-1} \equiv 1 \pmod{p}.$$

Nous venons de voir une illustration de ce théorème. Nous allons maintenant essayer d'en donner une démonstration.

Aperçu de la démonstration sur un exemple

Reprenons notre exemple avec 5. Nous travaillons modulo 5, c'est à dire dans l'ensemble $\mathcal{E} = \{0, 1, 2, 3, 4\}$. On peut alors remarquer que si l'on multiplie chacun de ces éléments par un même autre élément de l'ensemble (excepté 0), on obtiendra tous les éléments de \mathcal{E} . Avec 1 cette remarque est évidente. Regardons maintenant avec 2.

\mathcal{E}	0	1	2	3	4
$\times 2$	0	2	4	1	3

TAB. 3 – Multiplication par un élément

On observe bien que l'on retrouve tous les éléments de \mathcal{E} dans la deuxième ligne. Il est facile de vérifier aussi ceci pour 3 et 4.

Attention cette remarque n'est pas toujours vraie lorsque l'on travaille modulo un nombre qui n'est pas premier.

Nous allons maintenant faire le produit des éléments de l'ensemble excepté 0. Nous savons d'après notre remarque précédente que modulo 5 ce produit est aussi égal au produit des éléments de \mathcal{E} chacun multiplié par 2 puisque ceux sont les deux mêmes ensembles. On obtient alors les congruences suivantes:

$$\begin{aligned}
 1 \cdot 2 \cdot 3 \cdot 4 &\equiv (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdot (2 \cdot 4) \pmod{5} \\
 \iff 1 \cdot 2 \cdot 3 \cdot 4 &\equiv 2^4 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \pmod{5} \\
 \iff 4! &\equiv 2^4 \cdot 4! \pmod{5} \\
 \iff 2^4 &\equiv 1 \pmod{5}.
 \end{aligned}$$

Pour passer de la troisième à la quatrième ligne on divise par $4!$. Il faut tout de même vérifier que $4!$ n'est pas divisible par 5 car sinon on diviserait par 0 ce qui est impossible.

On vient de démontrer le théorème 2 pour $p = 5$ et $a = 2$. Notre remarque était aussi vraie pour $a = 1, 3, 4$; nous venons donc de démontrer le théorème 2 avec $p = 5$.

Généralisation de l'exemple

Il nous est donc maintenant facile de généraliser ceci afin de démontrer le théorème 2 pour tout nombre premier p .

On considère l'ensemble $\mathcal{E} = \{0, 1, \dots, p-1\}$. Nous savons que si on multiplie chacun de ces éléments par un $a \in \mathcal{E}$ mais différent de 0 on obtient encore l'ensemble \mathcal{E} , alors en procédant de même que tout à l'heure on obtient:

$$\begin{aligned}
1 \cdot 2 \cdots p-1 &\equiv (a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \pmod{p} \\
\iff (p-1)! &\equiv a^{p-1} \cdot (p-1)! \pmod{p} \\
\iff a^{p-1} &\equiv 1 \pmod{p}
\end{aligned}$$

La deuxième et la troisième ligne sont équivalentes car $(p-1)!$ n'est pas divisible par p .

Ceci termine donc notre démonstration du théorème 2.

1.2 Test de pseudo-primalité

Grâce au théorème de Fermat, nous obtenons le test de composition suivant.

Test de Fermat : Si un nombre n ne vérifie pas $a^{n-1} \equiv 1 \pmod{n}$ pour un a quelconque tel que $0 < a < n$ alors il n'est pas premier.

Nous disposons donc maintenant d'un outil qui nous permet d'affirmer qu'un nombre n'est pas premier, il s'appelle le *test de Fermat*.

Un entier non premier qui passe le test de Fermat pour un nombre a (que l'on nomme *base* dans ce contexte) est appelé *pseudo-premier* en base a .

Exemple : 341 est pseudo-premier en base 2 car $2^{340} \equiv 1 \pmod{341}$ et pourtant $341 = 11 \cdot 31$.

Un entier n , pseudo-premier en base a pour tous les a premiers avec lui est dit de *Carmichael*. Carl Pomerance a montré en 1993 qu'il en existe une infinité.

Exemple : $n = 561 = 3 \cdot 11 \cdot 17$ est de Carmichael.

1.3 Théorème d'Euler

On peut généraliser le petit théorème de Fermat au produit de deux nombres premiers p et q .

Théorème 3 Soit $n = pq$ avec p et q des nombres premiers alors

$$\text{pour tout } a \text{ premier avec } n, a^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

Il existe encore une généralisation de ce théorème pour n étant un nombre entier naturel quelconque. Mais à ce moment là, la puissance de a devient plus compliquée, c'est $\phi(a)$. ϕ est la fonction d'Euler, elle compte le nombre d'entiers positifs inférieurs à a et premier avec a , c'est à dire n'ayant pas de facteurs communs autres que 1 avec a (par exemple 8 et 15 sont premiers entre eux car $8 = 2^3$ et $15 = 3 \cdot 5$). Quelques valeurs de ϕ :

x	1	2	3	4	5	6	7	8	...
$\phi(x)$	1	1	2	2	4	2	6	4	...

TAB. 4 – Quelques valeurs de la fonction ϕ

Comme on l'a vu précédemment, le théorème 1 est une généralisation du théorème 2. De la même façon, le théorème 3 se généralise en le théorème suivant.

Théorème 4 Soit $n = pq$ avec p et q des nombres premiers alors

$$\text{pour tout entier } a, \text{ avec } 0 \leq a < n, a^{1+(p-1)(q-1)} \equiv a \pmod{n}.$$

2 Algorithme de chiffrement RSA

Le nom de cet algorithme de chiffrement provient des noms de ses inventeurs qui sont Rivest, Shamir et Adleman. Ils l'ont découvert en 1978.

Pour effectuer un chiffrement nous avons besoin d'une clef de chiffrement et d'une autre pour le déchiffrement.

Comme il s'agit d'un algorithme de cryptographie asymétrique à clef publique: il y a une clef publique (qui est connue de tout le monde) pour le chiffrement et une clef secrète pour le déchiffrement. Seule la personne possédant la clef secrète est capable de comprendre le message chiffré.

Si Alice désire qu'on puisse communiquer avec elle de façon secrète, elle se choisit deux grands nombres premiers p et q , puis elle en calcule le produit $n = pq$. Elle choisit ensuite un exposant publique e et elle calcule d tel que

$$ed \equiv 1 \pmod{(p-1)(q-1)}. \quad (1)$$

Elle rend alors publique (n, e) qui forme sa clef publique, elle garde secret d qui forme sa clef secrète.

Supposons que Bob veuille envoyer le message M à Alice. Il calcule le message chiffré $C \equiv M^e \pmod{n}$ et l'envoie à Alice.

Alice calcule alors $C^d \pmod{n}$ c'est à dire $M^{ed} \pmod{n}$. D'après l'équation (1) et la remarque que l'on a fait au paragraphe 1 on sait que ed est égal à $1 + k(p-1)(q-1)$.

On obtient donc

$$\begin{aligned}
 C^d &\equiv M^{ed} \pmod{n} \\
 &\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\
 &\equiv \underbrace{M^{1+(p-1)(q-1)}}_{\equiv M \pmod{n} \text{ d'après le théorème 4}} \cdot M^{(k-1)(p-1)(q-1)} \pmod{n} \\
 &\equiv M^{1+(k-1)(p-1)(q-1)} \pmod{n}.
 \end{aligned}$$

En appliquant encore $k - 1$ fois le théorème 4, on obtient:

$$C^d \equiv M \pmod{n}.$$

Alice a obtenue $C^d \equiv M \pmod{n}$, c'est à dire qu'elle a réussi à retrouver le message M que Bob lui a envoyé.

Exemple: Alice choisit $n = 3 \cdot 11 = 33$ comme module et $e = 3$ comme exposant public. Sa clef secrète est alors $d = 7$ car $3 \cdot 7 \equiv 1 \pmod{2 \cdot 10}$.

Supposons que Bob veuille lui envoyer le message "BONJOUR", il se sert alors du tableau suivant pour transformer les lettres en nombres :

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Bob chiffre le message en élevant chaque lettre à la puissance 3 modulo 20. On peut remarquer que le choix de 1 pour représenter A est très mauvais car le chiffré de A sera lui même.

Pour déchiffrer, il suffit à Alice d'élever chaque nombre chiffré à la puissance sa clef secrète 7 afin de retrouver le message d'origine.

B	O	N	J	O	U	R
02	15	14	10	15	21	18

Chiffrement $\Downarrow x^3 \pmod{33}$

08	09	05	10	09	21	24
H	I	E	J	I	U	X

Déchiffrement $\Downarrow x^7 \pmod{33}$

02	15	14	10	15	21	18
B	O	N	J	O	U	R

Transmission du message chiffré entre Bob et Alice :

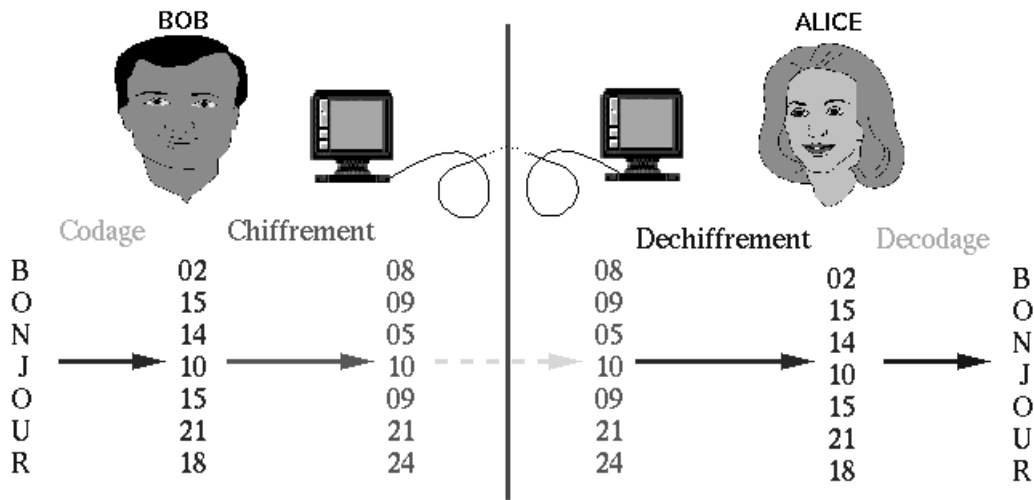


FIG. 4 – Illustration (didactique) du RSA.

On peut remarquer que cet algorithme est basé sur la difficulté de factoriser n . En effet celui qui arrive à factoriser n (retrouver p et q à partir de n) peut retrouver facilement la clef secrète d’Alice connaissant seulement sa clef publique. La factorisation est un problème très difficile si p et q sont très grands. Dans la pratique on utilisera des clefs et des modules ayant au moins 150 chiffres.

Prenons un nouvel exemple

Alice choisit $n = 101 \cdot 113$ (vous pouvez vérifier que 101 et 113 sont bien des nombres premiers). Elle prend $e = 3533$ comme exposant public. Sa clef publique est donc $(11413, 3533)$. Sa clef secrète est alors $d = 6597$ car $3533 \cdot 6597 \equiv 1 \pmod{11200}$.

Bob veut envoyer le message $M = 9726$ à Alice. Il consulte l’annuaire des clefs publiques et trouve $(11413, 3533)$ comme clef pour Alice.

Il calcule donc le message chiffré

$$\begin{aligned}
 C &= 9726^{3533} \pmod{11413} \\
 &= 5761
 \end{aligned}$$

et l’envoi à Alice.

Alice reçoit 5761 et calcule $5761^{6597} \pmod{11413} = 9726$ afin de retrouver le message en clair.

Application à la signature

Le RSA peut aussi être utilisé comme procédé de *signature électronique* d'un document. La signature d'un document permet par exemple à Bob de s'assurer que c'est bien Alice qui lui a envoyé le message qu'il a reçu et pas un fraudeur qui se ferait passer pour Alice.

Comment fonctionne la signature RSA ?

Alice veut envoyer le message M à Bob, mais elle veut aussi que Bob soit sûr que ce message vient bien d'elle. Pour ceci elle va calculer la signature $S = M^d \bmod n$. C'est la seule personne à pouvoir calculer S puisqu'elle est la seule à connaître d .

Elle envoie ensuite (M, S) à Bob.

Bob reçoit (M, S) et pour vérifier que c'est bien Alice qui lui a envoyé M , il consulte l'annuaire des clefs publiques afin d'obtenir la clef publique (n, e) d'Alice.

Il calcule ensuite $S^e \bmod n$ et doit obtenir M si c'est bien Alice qui lui a envoyé le message. La justification de ceci est la même que pour le chiffrement.

3 Jouer à pile ou face sur Internet

Les parents d'Alice ont décidé de déménager. La nouvelle désole Alice et son petit voisin, Bob, avec lequel elle passait des après-midi entières à de passionnantes parties de pile ou face.

Heureusement la cryptographie moderne est à même de leur offrir une solution. Pour jouer à leur jeu favori, Alice et Bob n'auront qu'à se conformer au protocole suivant :

1. Alice génère une paire (clef secrète, clef publique) et envoie la clef publique à Bob.
2. Alice génère les deux messages "pile" et "face", et ajoute à chacun d'eux une même chaîne aléatoire s .
3. Alice chiffre alors les deux messages avec sa clef publique et les envoie, dans un ordre aléatoire, à Bob.
4. Bob choisit un des deux messages au hasard et le renvoie à Alice.
5. Enfin, Alice décode le message reçu, détermine si Bob a gagné et lui envoie sa clef secrète en guise de preuve.

Bob peut-il tricher ?

Pour Bob, il y aurait deux moyens de tricher :

- Essayer de deviner lequel des deux messages reçus correspond à “pile”.
Sans la chaîne aléatoire s , ce serait facile : il suffirait à Bob de chiffrer “pile” avec la clef publique et de voir à quoi correspond le résultat obtenu. La chaîne aléatoire fait en sorte que Bob ne connaît pas exactement le texte clair, ce qui contre cette attaque.
- Jeter les deux messages reçus d’Alice, générer lui-même un message “pile” et l’envoyer à Alice après l’avoir chiffré avec la clef publique.
Ceci aussi est rendu impossible par la chaîne aléatoire s : il suffit à Alice de comparer le message reçu à l’étape 4 avec le message initial pour s’assurer qu’il n’y a pas eu de fraude.

Alice peut-elle tricher ?

Alice pourrait essayer de feinter son ami de l’une des manières suivantes :

- Chiffrer deux fois le message “face”, de sorte que, quoi qu’il choisisse, Bob ne puisse que perdre. Cependant, Bob découvrira la tricherie à l’étape 5, lorsqu’il utilisera la clef secrète pour déchiffrer les deux messages reçus à l’étape 2.
- Tenter, après que Bob ait fait son choix, de construire un message “face” dont le chiffré corresponde au message choisi. A priori, vu que Bob ne sait rien de la séquence aléatoire s , il ne paraît pas trop difficile de construire un message de la forme “face| s ” dont le chiffré corresponde au choix de Bob. Il faut cependant bien noter qu’Alice doit construire, non pas un, mais **deux** messages : le premier ci-dessus et un autre de la forme “pile| s ” dont le chiffré corresponde au message rejeté par Bob (bien sûr, la chaîne s doit être la même pour les deux messages). Sans cela, Bob découvrira la tricherie à l’étape 5. Avec un bon algorithme de chiffrement, Alice est incapable de générer une telle paire.

4 Les fonctions de hachage

Les fonctions de hachage sont classiquement utilisées avant un processus de signature. Pour rappel, signer un message revient à former un autre message qui prouve que l’on est bien l’auteur du premier message (le protocole

de chiffrement RSA peut être adapté très facilement à la signature). Une signature procure une certaine valeur à un message, de la même manière que la signature d'un peintre de renom ou celle sur un chèque. Certaines personnes mal intentionnées aimeraient bien vous faire signer des messages dont vous n'êtes pas l'auteur (c'est à dire faire croire que vous avez signé tel ou tel message), ce qui évidemment peut s'avérer assez gênant. Il faut toujours en tenir compte lorsque l'on élabore un cryptosystème.

En pratique, les algorithmes de signature ne sont pas appliqués au message lui-même. En effet, le message M est souvent trop long pour les algorithmes de signatures classiques.

4.1 Utilité

Il faut éviter de découper en blocs (M_1, M_2, \dots, M_k) de même longueur et signer directement et indépendamment

$$(S(M_1), S(M_2), \dots, S(M_k)).$$

Cela devient vite coûteux en temps de calcul et en communications puisqu'il faut chaque fois transmettre la signature avec le message. Cela ouvre aussi la porte à toutes sortes d'attaques si la chaîne de signature est appliquée sans précaution.

Par exemple, si les signatures ne sont pas reliées entre elles, on peut extraire certaines parties du message M_i et avoir la signature correspondante $S(M_i)$. Un message quelconque sur lequel on appliquerait un schéma de signature lettre par lettre, pourrait être dénaturé par quelqu'un de mal intentionné en lui enlevant quelques lettres ou même en les inversant ou en les répétant.

“Ce prof est vraiment content de nous”

pourrait devenir par exemple

“Ce prof nous ment vraiment”

ou autre chose...

Quand les messages à signer sont longs, il vaut mieux utiliser une fonction de hachage.

4.2 Propriétés des fonctions de hachage

Une fonction de hachage H transforme un message M de longueur quelconque en une version digérée $H(M)$ de *longueur fixe*.

Elle est à *sens unique* : il n'est pas possible d'inverser H ; c'est à dire étant donné un Y , il est impossible de trouver un message M , tel que le hachage de M , $H(M)$, donne Y . Il faut remarque que c'est en général le temps de calcul qui empêche d'inverser H . Supposons par exemple que l'on trouve un document électronique avec dessus la signature d'un montant, S . L'inversion de la signature permet de trouver Y , qui est le haché du montant lui-même, M . Si la fonction H n'était pas à sens unique, il serait possible de trouver un autre montant M' tel que Y soit aussi son haché et donc S en soit une signature valide!

Enfin, elle présente une probabilité très faible de *collision*. Il n'est pas possible de trouver M et M' tels que M est différent de M' et $H(M) = H(M')$.

Les collisions arrivent plus souvent que l'on ne se l'imagine. Un exemple est l'attaque des "anniversaires". Celle-ci découle d'un calcul simple de probabilité mais qui donne un résultat surprenant.

4.3 Le paradoxe des anniversaires

Enoncé : Dans un groupe de 23 personnes choisies aléatoirement, on a au moins une chance sur deux que deux d'entre elles aient leur anniversaire le même jour.

Commentaire : A priori, on serait tenté de penser qu'il faut plus de 23 personnes, puisqu'il y a 365 jours. Il est à noter que l'on écartera les années bissextiles dans la démonstration (ce qui ne change pas grand chose et ne sert qu'à simplifier les calculs, nous sommes désolés pour les gens qui sont nés un 29 février).

Explication : Calculons plutôt la probabilité que k personnes aient leur anniversaire à des jours différents. La première personne peut avoir son anniversaire n'importe quel jour. La seconde a $\frac{364}{365}$ ou $1 - \frac{1}{365}$ chances d'avoir son anniversaire un autre jour, la troisième $\frac{363}{365}$ ou $1 - \frac{2}{365}$ et ainsi de suite...

La probabilité de *non collision* est donc :

$$\left(1 - \frac{1}{365}\right) \left(1 - \frac{2}{365}\right) \left(1 - \frac{3}{365}\right) \cdots \left(1 - \frac{k-1}{365}\right).$$

Pour calculer cette probabilité, on va faire une approximation en utilisant les séries de Taylor. $1 - \frac{l}{365}$ est proche de $e^{-\frac{l}{365}}$. La probabilité approchée de non collision est donc de $e^{-\frac{k(k-1)}{2 \cdot 365}}$ et par conséquent la probabilité que deux personnes aient leur anniversaire le même jour est de $1 - e^{-\frac{k(k-1)}{2 \cdot 365}}$.

Maintenant, quelle valeur doit prendre k pour que la probabilité soit égale à une valeur donnée P ? $1 - e^{-\frac{k(k-1)}{2 \cdot 365}} = P$ nous donne $k = \sqrt{2 \cdot 365 \cdot \ln\left(\frac{1}{1-P}\right)}$.

Donc pour $P = 1/2$, on trouve bien 23. Il ne faut que 23 personnes pour avoir une chance sur deux que deux d'entre elles aient leur anniversaire le même jour.

Conséquence : L'extrapolation de ce paradoxe aux fonctions de hachage conduit à une nouvelle attaque, l'*attaque des anniversaires*. Si le nombre de messages digérés possible n'est pas suffisant, trouver une collision, c'est à dire deux messages ayant le même résultat de hachage est facile. Il faut donc choisir une longueur de messages hachés suffisamment longue, on conseille souvent un minimum de 120 bits.

4.4 Un exemple ludique de collisions

Prenez un jeu de cartes (minimum 52 cartes). Chaque carte vaut ce qui est indiqué sur son recto. Pour les images, le valet vaut un, la dame deux et le roi trois.

Chacun des participants choisit une carte parmi les dix premières.

On remet les dix cartes à leur place au-dessus du paquet. Le principe est alors de parcourir une à une les cartes depuis la première carte jusqu'à la dernière carte du jeu en progressant d'une carte à la suivante selon la valeur de la carte sur laquelle on tombe.

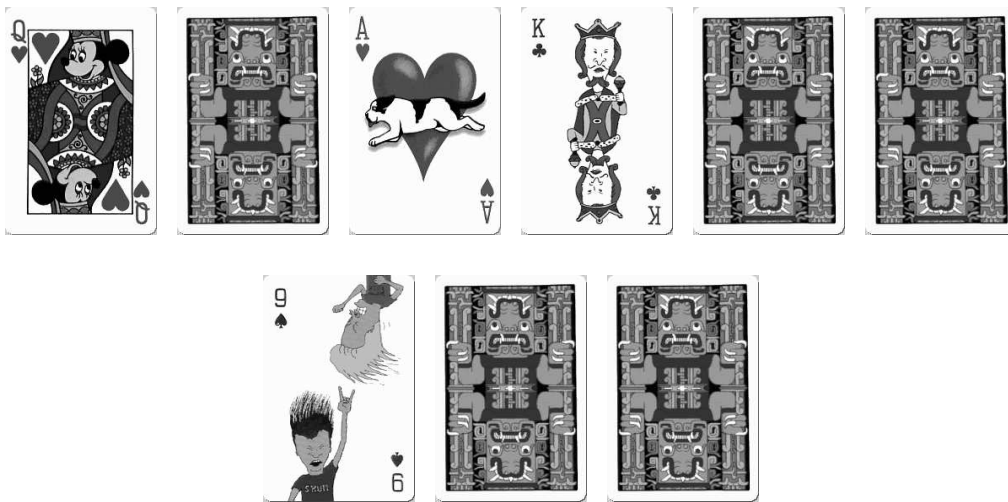


FIG. 5 – *Un autre paradoxe...*

Par exemple, j'ai choisi la dame pour commencer, je compte donc deux cartes (j'en saute une) et tombe ensuite sur l'as. Je passe ainsi à la carte suivante et ainsi de suite jusqu'à ce que l'on sorte du jeu (ici, le neuf de pique

nous fait sortir du jeu). Chaque participant retient la carte qui l'a fait sortir du jeu.

Essayez à plusieurs, vous verrez, *plus de trois quarts des participants finiront avec la même carte*. C'est un exemple de collisions.

La démonstration est laissée bien évidemment aux soins du lecteur...

5 Pile ou face sur Internet : une autre solution

5.1 Le problème

Alice et Bob sont toujours séparés. Leur jeu favori reste le pile ou face. Mais d'où les parents d'Alice se sont installés, l'envoi de messages chiffrés est interdit par la loi.

5.2 Adaptons le jeu

Que faire? Le principe du jeu de pile ou face consiste à ce qu'un des deux joueurs parie sur un événement ayant une probabilité d'1/2. Deux procédures peuvent être envisagées:

1. Il parie avant l'évènement.
2. Il parie après si :
 - (a) Il ne connaît pas le résultat
 - (b) L'autre joueur ne peut plus le modifier ce résultat

5.3 Les fonctions à sens unique

Cette alternative, combinée aux fonctions à sens unique, offre une autre solution à ce problème. Pour rappel, une fonction à sens unique est une fonction facile à calculer dans un sens mais pratiquement impossible à inverser :

- calculer $y = f(x)$ pour x fixé est aisé
- pour y fixé, trouver x tel que $f(x) = y$ est très difficile.

Ces fonctions peuvent être *à trappe* ou pas. Une fonction à sens unique à trappe est une fonction dont l'inversion est rendue aisée par la connaissance d'un secret.

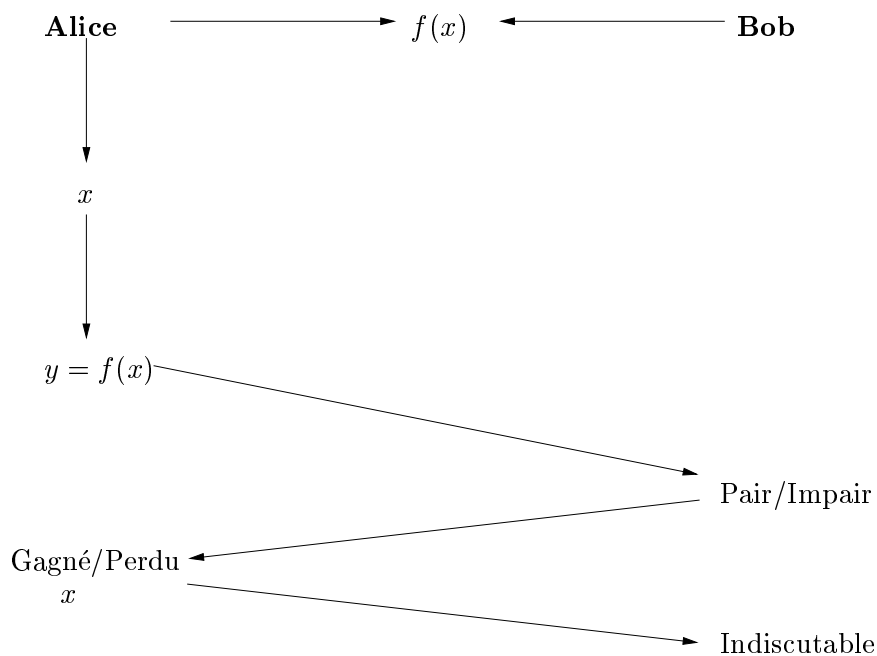
- Casser un vase est une fonction à sens unique.
- Fermer un coffre-fort est une fonction à sens unique à trappe.

5.4 La solution

Alice et Bob choisissent au préalable la fonction qu'ils vont utiliser: f . Elle ne doit pas être à trappe.

1. Alice choisit un nombre aléatoire x .
2. Elle calcule $y = f(x)$
3. Alice envoie y à Bob
4. Bob parie sur la parité de x et envoie sa supposition à Alice
5. Alice annonce le résultat du jeu et envoie x à Bob.

Bob peut vérifier que $y = f(x)$.



6 Zero-knowledge ou prouver une connaissance

6.1 Le Corbeau et le Renard

Maître Corbeau, perché sur son arbre, dit un jour à Maître Renard:

- “Moi, hier, j’ai été manger chez Maître Coq”.

Il faut savoir que Maître Coq est le nom d'un restaurant très sélect. N'y rentre que le gratin de la basse-cour. On comprend la fierté de Maître Corbeau. Pour empêcher les indésirables de rentrer dans le restaurant, la porte ne s'ouvre que si l'on connaît le mot de passe.

– “Je n'en crois rien”,

lui dit Maître Renard.

– “Ce restaurant n'accepte que la crème des crème. Je ne doute pas de ta valeur, Corbeau, mais là, ce serait trop d'honneur. Prouves-moi donc que tu es devenu si important”,

demande le Renard.

Maître Corbeau, trop heureux de pouvoir démontrer qu'il fait partie du gratin, lui répond avec fierté :

– “Et bien, le mot de passe est ”sauce archiduc”.

– “Je te crois et suis heureux de ta réussite”,

dit le Renard, qui quitte le Corbeau en souriant.

Le soir même, quand Maître Corbeau alla dîner chez Maître Coq, il ne trouva que quelques plumes pour tout cuisinier.

On comprend le difficile problème du Corbeau : “Comment prouver qu'il connaît un secret, sans par là même le révéler”.

La cryptographie permet au Corbeau, à la fois d'assouvir son orgueil, sans pour autant mettre en péril la vie de Maître Coq...

6.2 Une définition intuitive du Zero-knowledge (apport nul de connaissances)

Les techniques de Zero-knowledge permettent à Peggy de prouver à Victor, de manière irréfutable, qu'elle connaît un secret, sans donner la moindre information qui permettrait à Victor de déduire ce secret. Encore plus fort, Victor, disposant de la preuve, ne peut l'utiliser pour prouver à Tryphon qu'il connaît lui aussi le secret.

Exemple: l'isomorphisme de graphes

Un graphe est un ensemble de noeuds et d'arêtes. Considérons le graphe $G_1 = (V, E_1)$ donné par

$$G_1 = (\{1, 2, 3, 4, 5, 6, 7\}, \{1 - 2, 2 - 6, 6 - 7, 4 - 3, 4 - 5, 6 - 4, 1 - 7\}).$$

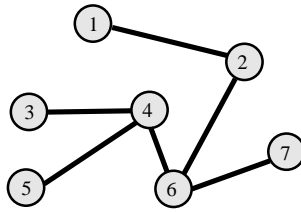


FIG. 6 – Graphe G_1 .

Définition 2 Deux graphes $G_1(V_1, E_1)$ et $G_2(V_2, E_2)$ sont isomorphes si et seulement si il existe une bijection $B : V_1 \rightarrow V_2$ telle que $\{u, v\}$ appartient à E_1 si et seulement si $B(u), B(v)$ appartient à E_2 .

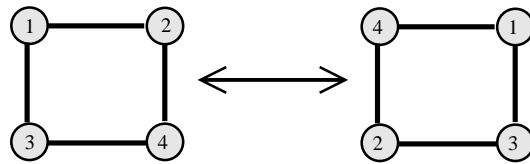


FIG. 7 – Isomorphisme entre deux graphes.

6.3 La question facile

Soit un graphe $G_1 = (V, E_1)$ donné par

$$G_1 = (\{1, 2, 3, 4, 5, 6, 7\}, \{1 - 2, 2 - 6, 6 - 7, 4 - 3, 4 - 5, 6 - 4, 1 - 7\})$$

trouver un graphe $G_2 = (V, E_2)$ isomorphe à G_1 .

On choisit une permutation des noeuds, $\{5, 7, 4, 3, 6, 1, 2\}$, et on applique cette permutation à G_1 . On obtient

$$G_2 = (\{1, 2, 3, 4, 5, 6, 7\}, \{1 - 2, 1 - 3, 3 - 4, 3 - 6, 2 - 5, 5 - 7, 7 - 1\}).$$

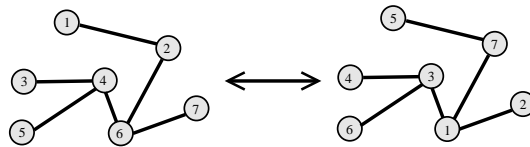


FIG. 8 – Construction d'un graphe isomorphe à un autre.

6.4 La question difficile

Soit 2 graphes avec n noeuds, sont-ils isomorphes ?

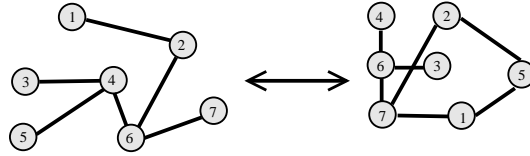


FIG. 9 – Trouver un isomorphisme.

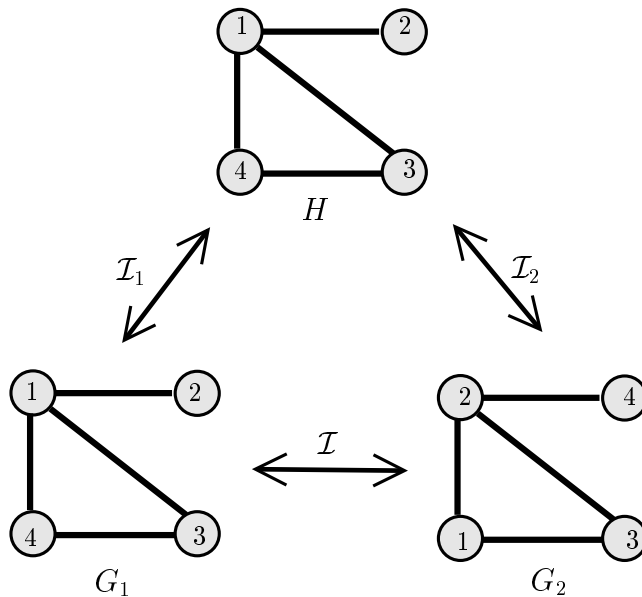
Si n est grand, le problème est très difficile.

6.5 Le protocole Zero-Knowledge

Peggy et Victor connaissent deux graphes, G_1 et G_2 .

Peggy prétend connaître un isomorphisme \mathcal{I} entre ces deux graphes. Victor voudrait vérifier cette connaissance de Peggy. Mais Peggy ne veut pas donner son isomorphisme. Voici comment Peggy va convaincre Victor sans révéler son secret.

1. Peggy, qui construit un graphe H isomorphe à G_1 , à l'aide d'un isomorphisme qu'elle a choisi \mathcal{I}_1 . Connaissant \mathcal{I} , Peggy peut calculer l'isomorphisme entre H et G_2 .



2. Peggy envoie le graphe H à Victor.
3. Victor choisit un des deux graphes initiaux G_1 ou G_2 et demande à Peggy de lui donner l'isomorphisme entre H et son choix.
4. Peggy envoie \mathcal{I}_1 ou \mathcal{I}_2 suivant la demande de Victor.

Propriétés

- Victor n'apprend rien.

En effet, après la preuve, Victor connaît un isomorphisme entre H et soit G_1 , soit G_2 , mais pas les deux. Mais cela, Victor aurait pu le calculer sans effort. Ce que Victor ne peut pas calculer, c'est deux isomorphismes, l'un entre H et G_1 et l'autre entre H et G_2 .

- Peggy, si elle ne connaît pas i , à une chance sur deux de pouvoir répondre à la demande de Victor.

En effet, ne connaissant pas i , Peggy n'a d'autre solution que de deviner la question de Victor. Elle choisit par exemple de calculer H par rapport à G_2 , si Victor demande i_2 , elle pourra répondre, mais s'il demande \mathcal{I}_1 , elle sera démasquée. La probabilité de pouvoir tricher est donc $1/2$.

En répétant le protocole, on rend la probabilité de tricher aussi petite que l'on veut. En répétant le protocole m fois, la probabilité de pouvoir tricher devient $1/2^m$.

Table des matières

1	Que signifie travailler modulo un entier?	1
1.1	Petit théorème de Fermat	2
1.2	Test de pseudo-primalité	6
1.3	Théorème d'Euler	6
2	Algorithme de chiffrement RSA	7
3	Jouer à pile ou face sur Internet	10
4	Les fonctions de hachage	11
4.1	Utilité	12
4.2	Propriétés des fonctions de hachage	12
4.3	Le paradoxe des anniversaires	13
4.4	Un exemple ludique de collisions	14
5	Pile ou face sur Internet : une autre solution	15
5.1	Le problème	15
5.2	Adaptons le jeu	15
5.3	Les fonctions à sens unique	15
5.4	La solution	16
6	Zero-knowledge ou prouver une connaissance	16
6.1	Le Corbeau et le Renard	16
6.2	Une définition intuitive du Zero-knowledge (apport nul de connaissances)	17
6.3	La question facile	18
6.4	La question difficile	19
6.5	Le protocole Zero-Knowledge	19