14 PRATIQUE PROCÉDURALE 1

Déroulement de l'activité

Description	Début	Fin	Durée

Informations pour la personne tutrice et communication aux étudiantes et aux étudiants

Informations ou directives données aux formateurs dans le guide du formateurs

---

Le contenu du guide de l'étudiante et de l'étudiant pour cette activité suit. Les solutions et les directives y sont ajoutées.

But de l'activité

Le but de cette activité est de se familiariser avec certains algorithmes de chiffrement, la théorie mathématique qui explique leur fonctionnement, et les limites de leur utilisation :

- RSA : système à clé publique
- DH : partage sécuritaire de clé privée
- AES : méthode de chiffrement symétrique

NOTE : Il vous est fortement recommandé de lire les documents qui expliquent RSA, la théorie des nombres et le chiffrement symétrique avant de vous présenter à cette séance.

Pour faire les exercices procéduraux qui suivent, vous devrez faire certains calculs qui pourraient s'avérer exigeants si vous les faites seulement avec un papier et un crayon. Il vous est donc recommandé d'utiliser une calculatrice ou une application logicielle de calcul qui supporte les grands nombres.

14.1 EXERCICES

P1.E1 RSA - Calcul de clé et chiffrement

Soit $p = 5$, $q = 11$,

a. Quel est n ? $n = 5 \times 11 = 55$

b. Est-il possible de trouver une paire de clés avec $e = 59$? Si oui, quel est le d correspondant ? Si vous avez trouvé d, calculez $(d^{-1} \mod \phi(n))$ et $(d^{-1} \mod \lambda(n))$. Expliquez vos résultats. $\phi(n) = 4 \times 10 = 40$, $\lambda(n) = 20$.
Puisque $e = 59$ et $\phi(n)$ sont relativement premiers, alors il existe un inverse multiplicatif de $e \mod \phi(n)$.

On trouve : $d = 19$. Or $d^{-1} = 19$, ce qui veut dire que $e = 59$ est équivalent à $e = 19$ (parce que e et $e \mod \phi(n)$ sont équivalents).
Puisque $e = d = 19$, ce n'est pas vraiment un bon choix de clé, puisque l'encryption et la décryption utilisent le même exposant...

Calculs de l'inverse multiplicatif avec $\phi(n)$:

$$\begin{aligned}
40 &= 1 \times 40 + 0 \times 59 \\
59 &= 0 \times 40 + 1 \times 59 \qquad (40 \div 59 = 0) \\
40 &= 1 \times 40 + 0 \times 59 \qquad (59 \div 40 = 1) \\
19 &= -1 \times 40 + 1 \times 59 \qquad (40 \div 19 = 2) \\
2 &= 3 \times 40 - 2 \times 59 \qquad (19 \div 2 = 9) \\
1 &= -28 \times 40 + 19 \times 59
\end{aligned}$$

Inverse multiplicatif $\mod 40 : 19$ $(-28 \mod 40 = 0$, donc $19 \times 59 \mod 40 = 1)$

Inverse multiplicatif avec $\lambda(n)$:

$$\begin{aligned}
20 &= 1 \times 20 + 0 \times 59 \\
59 &= 0 \times 20 + 1 \times 59 \qquad (20 \div 59 = 0) \\
20 &= 1 \times 20 + 0 \times 59 \qquad (59 \div 20 = 2) \\
19 &= -2 \times 20 + 1 \times 59 \qquad (20 \div 19 = 1) \\
1 &= 3 \times 20 - 1 \times 59
\end{aligned}$$

Inverse multiplicatif $\mod 20 : -1 = 19 (-1 \mod 20 = 19)$

Inverse multiplicatif de 19 (modulo 20) :

$$\begin{aligned}
20 &= 1 \times 20 + 0 \times 19 \\
19 &= 0 \times 20 + 1 \times 19 \qquad (20 \div 19 = 1) \\
1 &= 1 \times 20 - 1 \times 19
\end{aligned}$$

Inverse multiplicatif de $19 \mod 20 = -1 = 19 \mod 20$

c. Est-il possible de trouver une paire de clés où e est un nombre pair ? Pourquoi ? Non, parce que $\phi(n) = (p-1)(q-1)$ est par définition un nombre pair (puisque p et q sont des nombres premiers, que tous les nombres premiers sont impairs (sauf le nombre 2, mais p et q sont grands et donc nécessairement différents de 2), et donc que $p-1$ est un nombre pair), et que e n'aura un inverse multiplicatif que s'il est relativement premier avec $\phi(n)$.

d. Est-il possible de trouver une paire de clés avec $e = 5$, 15, 25 ou 35 ? Si oui, quel est le d correspondant à chacun des e ? Même raison qu'en c. : puisqu'ici $q = 11$, $q-1$ est un multiple de 5, donc $\phi(n)$ est un multiple de 5, et aucun multiple de 5 ne sera relativement premier avec $\phi(n)$.

e. Est-il possible de trouver une paire de clés avec $e = 9$, 11, 19, 21, 29, 31 ou 39 ? Si oui, quel est le d correspondant à chacun des e ? Est-ce que ce sont vraiment des clés de chiffrement ? Pourquoi ? Tous ces nombres sont leurs propres inverses multiplicatifs. Il n'est pas conseillé d'utiliser ce genre de nombre comme clé de chiffrement.

f. Pour $e = 1$, quel est d ? Est-ce qu'ils forment une paire de clés valable ? Pourquoi ? De nouveau, $e = 1$ est son propre inverse multiplicatif. De plus, le message original ne sera pas modifié par l'opération d'encryption ($m^1 = m \ldots$).

g. Est-il possible d'énumérer la liste de paires de clés valables $(n, e), (n, d)$ pour ce n ? Si oui, quelles sont-elles ? Si non, pourquoi ? Après avoir éliminé les nombres pairs, les multiples de 5 et les nombres 1, 9, 11, 19, 21, 29, 31 et 39, il ne reste que $e = 3, 7, 13, 17, 23, 27, 33$ et 37.
On vérifie qu'à ces valeurs de e correspondent les valeurs suivantes de d :
$27, 23, 37, 33, 7, 3, 17, 13$ si on utilise $\phi(n)$.
Si on utilise $\lambda(n) = 20$, on obtient alors : $d = 7, 3, 17, 13, 7, 3, 17, 13$.
Il n'y a donc que les paires de clés $((55, 3), (55, 7))$ et $((55, 13), (55, 17))$ qui sont possibles lorsqu'on fait le calcul avec $\lambda(n)$.
On remarque que ces clés peuvent être dérivées de celles obtenues à l'aide de $\phi(n)$ si on effectue sur ces dernières l'opération $\mod \lambda(n)$.

h. L'une des paires de clés possibles est bâtie à partir de $e = 3$. Que devient le nombre 30 lorsqu'on le chiffre avec la clé publique $(n, 3)$? Peut-on déchiffrer le résultat ? On obtient $c = 30^3 \mod 55 = 50$.
Pour déchiffrer, il s'agit de trouver $50^7 \mod 55$, qui est : 30.
Utiliser la méthode binaire des exposants pour faire le calcul.

i. Avec la même paire de clés, chiffrez le nombre 85. Peut-on déchiffrer le résultat ? Si oui, comment ? Si non, qu'est-il arrivé ? (Vous pouvez aussi essayer de chiffrer/déchiffrer 140 et 195) $85 = 30 \mod 55$. Donc chiffrer 85 revient à chiffrer 30.

On ne pourra déchiffrer le résultat (on obtiendra 30 et non 85). Idem pour 140 et 195 (leur résidu = 30 $\mod 55$)

j. Chiffrez $(m = 54)$ avec $(n, e) = (55, 3)$. Commentez le résultat. On obtient : 54.

Par le binôme de Newton : $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$, d'où :

$$\begin{aligned}(p-1)^e \mod p &= (\text{somme de multiples de } p + (-1)^e) \mod p \\ &= (-1)^e \mod p \\ &= -1 \mod p \\ &= p-1\end{aligned}$$

Aucun des multiples de p n'a de résidu $\mod p$, et puisque e est un nombre impair, alors $(-1)^e = -1$. On ne peut donc chiffrer $(p-1)$, on réobtient exactement le même nombre...

k. Chiffrez $(m = 11,\ 22,\ 33)$ avec $(n, e) = (55, 3)$. Qu'ont en commun les résultats ? Pouvez-vous expliquer pourquoi ? (Indice : le TRC peut s'avérer très utile...) $11^3 \mod 55 = 11$, $22^3 \mod 55 = 33$, $33^3 \mod 55 = 22$

Ces messages sont des multiples de 11 (l'un des deux facteurs de n), et les messages chiffrés sont aussi des multiples de 11. Le TRC nous permet de décomposer un nombre selon les résidus modulo les facteurs de la base. Ici, la base est $55 = 5 \times 11$. On peut donc représenter les nombres 11, 22 et 33 par leurs résidus $\mod 5$ et $\mod 11$:

$11 = (1 \mod 5, 0 \mod 11)$;

$22 = (2 \mod 5, 0 \mod 11)$;

$33 = (3 \mod 5, 0 \mod 11)$.

On peut ensuite faire l'élévation à la puissance 3 des deux résidus :

$11^3 = (1 \mod 5, 0 \mod 11)$;

$22^3 = (2^3 \mod 5, 0 \mod 11) = (3 \mod 5, 0 \mod 11)$

$33^3 = (3^3 \mod 5, 0 \mod 11) = (2 \mod 5, 0 \mod 11)$.

On s'aperçoit que le résidu $\mod 11$ est nul au départ, et donc l'élévation à une puissance conservera un résidu nul $\mod 11$, ce qui implique que le résultat sera un multiple de 11. On observerait une résultat similaire pour 44, et pour tous les multiples de 5, l'autre facteur de n.

l. Prouvez que $a^{(p-1)} \equiv 1(\mod p)$ (où p est un nombre premier) n'est pas vrai si a est un multiple de p (c'est-à-dire, $a = kp$). Puisque a est un multiple de p, $(a \mod p)$ sera nul. Donc $a^x \mod p = 0$ peu importe x.

P1.E2 RSA - Utilisation du théorème du reste chinois (problème de Sun Zi)

Nous avons une certaine quantité d'objets, mais nous n'en connaissons pas le nombre exact :

Si nous les comptons par groupes de 5, il nous en reste 3.
Si nous les comptons par groupes de 7, il nous en reste 0.
Si nous les comptons par groupes de 11, il nous en reste 10.
Enfin, si nous les comptons par groupes de 13, il nous en reste 8.

Combien y a-t-il d'objets ? Comment le tuteur devra-t-il modifier ce problème l'an prochain ? Pourrait-on obtenir le même résultat en n'utilisant que les résidus modulo 5, 7 et 11 ?

Question bonus (demande un peu de réflexion) : l'un des étudiants du cours affirme : "Si cette question est encore là quand elle sera en S3 informatique, ma jeune soeur aura comme paramètres du problème des restes de 5 modulo 7 et de 7 modulo 11". En supposant que les étudiants ont habituellement 20 ans en S3, croyez-vous l'affirmation de cet étudiant ? Si oui, en quelle année est née la soeur de l'étudiant ?

On recherche x tel que :
$x \mod 5 = 3$,
$x \mod 7 = 0$,
$x \mod 11 = 10$,
$x \mod 13 = 8$.

Considérons les 4 produits de 3 facteurs :

$$\begin{aligned} P_5 &= 7 \times 11 \times 13 = 1001 \equiv 1 \pmod 5 \\ P_7 &= 5 \times 11 \times 13 = 715 \equiv 1 \pmod 7 \\ P_{11} &= 5 \times 7 \times 13 = 455 \equiv 4 \pmod{11} \\ P_{13} &= 5 \times 7 \times 11 = 385 \equiv 8 \pmod{13} \end{aligned}$$

P_5 et P_7 sont déjà égaux à $1 \mod 5$ ou $\mod 7$: on peut les utiliser tels quels

$P_{11} = 4 \mod 11$. Il faut donc trouver $4^{-1} \mod 11$, et multiplier le tout par P_{11} :

$$\begin{aligned} 11 &= 1 \times 11 + 0 \times 4 \\ 4 &= 0 \times 11 + 1 \times 4 \\ 3 &= 1 \times 11 - 2 \times 4 \\ 1 &= -1 \times 11 + 3 \times 4 \Longrightarrow 4^{-1} \mod 11 = 3 \end{aligned}$$

On utilisera donc :
$P'_{11} = 3 \times P_{11} = 3 \times 455 = 1365$ (et évidemment, $1365 = 1 \mod 11$)

$P_{13} = 8 \mod 13$. Il faut donc trouver $8^{-1} \mod 13$, et multiplier le tout par P_{13} :

$$\begin{aligned} 13 &= 1 \times 13 + 0 \times 8 \\ 8 &= 0 \times 13 + 1 \times 8 \\ 5 &= 1 \times 13 - 1 \times 8 \\ 3 &= -1 \times 13 + 2 \times 8 \\ 2 &= 2 \times 13 - 3 \times 8 \\ 1 &= -3 \times 13 + 5 \times 8 \Longrightarrow 8^{-1} \mod 13 = 5. \end{aligned}$$

On utilisera donc :
$P'_{13} = 5 \times P_{13} = 1925$ (ici encore, $1925 = 1 \mod 13$)

Donc,

$$\begin{aligned} x &= 3 \times P_5 + 0 \times P_7 + 10 \times P'_{11} + 8 \times P'_{13} \\ &= 3 \times 1001 + 0 \times 715 + 10 \times 1365 + 8 \times 1925 \\ &= 3003 + 0 + 13650 + 15400 \\ &= 32053 \end{aligned}$$

La plus petite solution est $x' = x \mod (5 \times 7 \times 11 \times 13) = 32053 \mod 5005 = 2023$

Extension de la question : Comment modifier les restes de $5, 7, 11$ et 13 pour obtenir 2024 ? 2025 ? -> Ajouter 1 (ou 2) aux résidus.

Autre extension : Pourrait-on obtenir 2023 en n'utilisant que les résidus modulo 5, 7 et 11 ? -> Non, le résultat minimum serait plus petit que $5 \times 7 \times 11 = 385$, qui est plus petit que 2023.
Cependant, on pourrait utiliser le résultat modulo 2, 3, 5, 7, et 11 (résultat maximal = 2310, qui est plus grand que 2023.

Question supplémentaire :
On doit d'abord trouver l'année qui précède 2023 et qui a un reste de 0 mod 7 et de 0 mod 11, c'est-à-dire le multiple de 77 qui est immédiatement inférieur à 2023. Ce nombre est : $2023 - (2023 \mod 77) = 2002$.

Puisque les résidus seront de 5 mod 7 et de 7 mod 11,
ceci implique qu'il faut ajouter 5 X 11 X $11^{-1} \mod 7 + 7$ X 7 X $7^{-1} \mod 11$,
c'est-à-dire 5 X 11 X 2 + 7 X 7 X 8, soit $110 + 393 = 502$.
Puisque $502 \mod 77 = 40$, le tout aura lieu en $2002 + 40 = 2042$.
Puisque la soeur aura 20 ans en 2042, c'est qu'elle est née en 2022.
Elle est née l'an dernier.

P1.E3 RSA - Découverte de clés privées et déchiffrement

a. Soit la clé publique suivante : $(n, e) = (86429, 5)$. Pouvez-vous trouver la clé privée correspondante ? Petit indice : la fonction $f(x) = x^2 + 5$, en commençant avec $x = 1$, pourrait s'avérer utile pour la méthode ρ de Pollard... On utilisera l'algorithme de Pollard, avec $f(x) = x^2 + 5$:
$f(1) = 6$
$f(f(1)) = 41$
$f(f(1)) - f(1) = 35$. Cherchons le PGCD de 35 et 86429 :

86429	
35	$(2469 \times 35 = 86415$, reste $= 14)$
14	$(14 \times 2 = 28$, reste $= 7)$
7	$(7 \times 2 = 14$, reste $= 0)$

Le PGCD est 7, alors $n = 86429 = 7 \times 12347$. D'où $\phi(n) = 6 \times 12346$, et $\lambda(n) = \phi(n)/2 = 37038$.
On trouve $d = e^{-1} \mod \lambda(n)$:

37038	=	$1 \times 37038 + 0 \times 5$	
5	=	$0 \times 37038 + 1 \times 5$	$(37038 \div 5 = 7407$, reste $3)$
3	=	$1 \times 37038 - 7407 \times 5$	$(5 \div 3 = 1$, reste $2)$
2	=	$-1 \times 37038 + 7408 \times 5$	$(3 \div 2 = 1$, reste $1)$
1	=	$2 \times 37038 - 14815 \times 5$	$5^{-1} \mod 37038 = -14815 \mod 37038$

qui donne $d = e^{-1} \mod \lambda(n) = 22223$.

b. Vous interceptez un message chiffré avec la clé précédente. Pouvez-vous le déchiffrer ? Le message chiffré est : 30270 Vous avez une idée : peut-être le message original était-il codé en ASCII, avec des blocs de 8 bits accolés les uns aux autres ? Pour en avoir le coeur net, allez consulter le site suivant : http://www.asciitable.com/ On trouve :
$m = (c^d \mod n) = 30270^{22223} \mod 86429$
$22223 = 16384 + 4096 + 1024 + 512 + 128 + 64 + 8 + 4 + 2 + 1$

w	**Calcul partiel de m^{22223}**	**Calcul effectué**	**Représentation binaire de 22223**
32768	1	$1 \times 1 \times 1 \mod 86429$	0
16384	30270	$1 \times 1 \times 30270 \mod 86429$	1
8192	39071	$30270 \times 30270 \times 1 \mod 86429$	0
4096	75072	$39071 \times 39071 \times 30270 \mod 86429$	1
2048	29381	$75072 \times 75072 \times 1 \mod 86429$	0
1024	79885	$29381 \times 29381 \times 30270 \mod 86429$	1
512	77772	$79885 \times 79885 \times 30270 \mod 86429$	1
256	9706	$77772 \times 77772 \times 1 \mod 86429$	0
128	71768	$9706 \times 9706 \times 30270 \mod 86429$	1
64	32918	$71768 \times 71768 \times 30270 \mod 86429$	1
32	34351	$32918 \times 32918 \times 1 \mod 86429$	0
16	62493	$34351 \times 34351 \times 1 \mod 86429$	0
8	80427	$62493 \times 62493 \times 30270 \mod 86429$	1
4	83934	$80427 \times 80427 \times 30270 \mod 86429$	1
2	38098	$83934 \times 83934 \times 30270 \mod 86429$	1
1	15145	$38098 \times 38098 \times 30270 \mod 86429$	1

$m = 15145 = 59 \times 256 + 41$

$m = 59, 41 =$;) (en ASCII) (c'est un smiley...)

P1.E4 Diffie-Hellman : sécurité de la clé privée partagée

Soit $p = 17$, le nombre premier que nous utiliserons pour faire une échange Diffie-Hellman.

a. Soit $g = 13$. Combien y a-t-il de puissances distinctes de g ? Est-ce que leur nombre est suffisant ? (Utiliser la table des puissances de $g \mod 17$ ci-après). Il y a 4 puissances de $13 \mod 17 : 1, 13, 16, 4$. Non, ce nombre n'est pas suffisant : deux puissances sont toujours connues 1 et 13, alors il ne reste que deux puissances inconnues.

b. Quels sont les meilleurs choix pour g ? Pourquoi ? 3, 5, 6, 7, 10, 11, 12 et 14 sont de bons choix, puisque chacun de ces nombres a $p-1$ puissances distinctes (le maximum).

c. Quelles sont les tailles des cycles des puissances des différents g ? Quel est leur lien avec $p - 1$? Nous pouvons observer des cycles de puissances de longueur 1, 2, 4, 8 et 16. Ce sont tous des facteurs de $p - 1$.

g	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	1	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	1	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	1	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	1	8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	1	9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	1	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	1	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	1	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	1	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	1	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	1	15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

P1.E5 AES - Calcul et utilisation

Pour répondre à cette question, le vidéo suivant (moins de 3 minutes) peut être utile. La description disponible sur wikipédia est aussi intéressante.

a. À quoi sert le "*key schedule*" de Rijndael ?
b. Que représente l'état (*state* en anglais) pendant les calculs AES ?
c. Quelle est la fonction des "tours" de calcul (*rounds* en anglais) ?

P1.E6 RSA - Calcul de p et q à partir de n et phi(n)

On vous donne n et $\phi(n)$. Trouvez p et q. Indice : Travaillez l'équation : $(x-p)(x-q) = 0$, en tentant de remplacer les occurrences de p et q par des fonctions de n et $\phi(n)$. Vous obtiendrez une équation de la forme $x^2+bx+c = 0$, dont les racines seront p et q. Pour vérifier votre solution, calculez p et q pour $n = 218791$ et $\phi(n) = 217800$. $(x-p)(x-q) = x2-(p+q)x+pq = 0$
Puisque $\phi(n) = (p-1)(q-1)$, alors $\phi(n) = pq - p - q + 1 = n - (p+q) + 1$
D'où : $x^2 - (p+q)x + pq = x^2 + (\phi(n) - n - 1)x + n = 0$

La solution de cette équation du 2^e degré est :
$x = \frac{1}{2}(n + 1 - \phi(n) \pm \sqrt{(n + 1 - \phi(n)^2 - 4n)})$
D'où : $x = 331$ et $x = 661$ (avec $n = 218791$ et $\phi(n) = 217800$

Leçon à tirer de cet exercice : à partir de n et $\phi(n)$, on peut retrouver p et q, et donc d. Si $\phi(n)$ est conservé après la génération des clés, il est aussi important de le protéger que p et q : il est équivalent. De même, la connaissance de d, e et n permet de retrouver $\phi(n)$, p et q.