

TD Cryptographie

Exercice 1:

Soit un système de communication à N nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés.

- 1) Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication sécurisée entre chaque paire de nœuds:
 - a. Pour un système à clés symétrique? ==> **N-1 clés**
 - b. Pour un système à clés asymétrique? ==> **2 clés: chaque nœud stocke sa clé publique et sa clé privée. La clé publique peut être sauvegardé dans un annuaire.**
- 2) En déduire le nombre de clés du système pour chaque cas
 - a. Pour un système à clés symétrique? ==> **$N(N-1)/2$ clés**
 - b. Pour un système à clés asymétrique? ==> **$2N$ clés**

Exercice 2 :

Soit **M** un message et **K** une clé aussi longue que **M**. On note **C=M⊕K** le message **M** chiffré avec **K**. Si $m[i]$ est le $i^{\text{ème}}$ bit du message **m** et $k[i]$ est le $i^{\text{ème}}$ bit de la clé **K**, alors le $i^{\text{ème}}$ bit de **M⊕K** est égal à $(M[i] \oplus K[i])$.

On note que pour tout X, $X \oplus X = 0$, $X \oplus 0 = X$ et $X \oplus Y = Y \oplus X$

- 1) Montrez que le "ou exclusif \oplus " est une technique de chiffrement symétrique.

==> **On chiffre et on déchiffre avec la même clé K : $C=M \oplus K \implies C \oplus K = M \oplus K \oplus K = M$**
- 2) Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer?

==> **C'est inadéquat car il faut changer la clé pour chaque message et il faut la transmettre au destinataire dans un canal sécurisé.**
- 3) Soit le protocole décrit par la figure 1 qui exploite le "ou exclusif \oplus " pour le chiffrement d'un message **M**. Quand **A** veut envoyer un message **M** à **B**, il génère une clé **K_A** aussi longue que **M**. **B** génère aussi une clé **K_B** aussi longue que **M**.
 - a) Comment **B** peut-il déterminer la taille de la clé **K_B** ? ==> **même taille que $M \oplus K_A$**
 - b) Comment **A** peut-il déterminer $M \oplus K_B$ à partir de $M \oplus K_A \oplus K_B$? ==> **$M \oplus K_A \oplus K_B \oplus K_A = M \oplus K_B$**
 - c) Comment **B** retrouve t-il **M** ? ==> **$M \oplus K_B \oplus K_B = M$**
 - d) Si tous les messages échangés peuvent être écoutés, ce protocole permet-il la confidentialité? ==> **non, un ou exclusif entre les trois message donnera M**



Figure 1: étapes pour l'échange d'un message **M** Chiffré (symétrique)

Exercice 3:

La figure 1 présente l'échange de messages entre 3 entités **A**, **B** et **C** (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format des messages suivant: (source, destination, message).

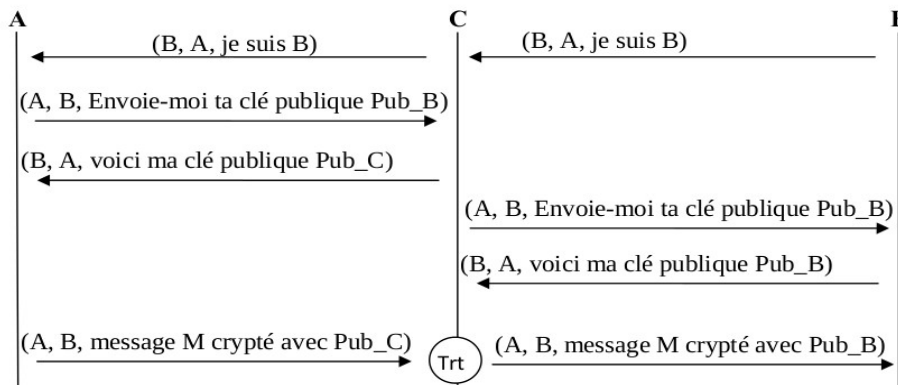


Figure 2: étapes pour l'échange d'un message M chiffré (asymétrique)

- 1) Quel est le traitement Trt effectué par C. ==> **déchiffrement avec Pub_C puis chiffrement avec Pub_B**
- 2) A et B se rendent-ils compte de l'existence de l'intrus C ==> **non**
- 3) Proposer une solution permettant de remédier à cette attaque ==> **utiliser l'authentification par certificat qui assure l'appartenance d'une clé publique à une entité**

Exercice 4

Soit M un message divisé en blocs $\{x_1, x_2, x_3, \dots, x_p\}$ chacun de taille n bits et soit K une clé de même taille que les blocs (n bits). Soit $\{c_1, c_2, c_3, \dots, c_p\}$ les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:

$C_0 = IV$ (valeur initiale) ; pour i de 1 à p , $c_j = E_K(C_{j-1} \oplus x_j)$

- 1) La fonction E_K est inversible et son inverse est D_K . Montrer que l'opération de déchiffrement est $x_j = C_{j-1} \oplus D_K(C_j)$ (rappel : $A \oplus A = 0$; $A \oplus 0 = A$, $A \oplus B = B \oplus A$)
On a $c_j = E_K(C_{j-1} \oplus x_j) \implies D_K(c_j) = D_K(E_K(C_{j-1} \oplus x_j)) \implies D_K(c_j) = C_{j-1} \oplus x_j \implies C_{j-1} \oplus D_K(c_j) = C_{j-1} \oplus C_{j-1} \oplus x_j \implies C_{j-1} \oplus D_K(c_j) = 0 \oplus x_j \implies x_j = C_{j-1} \oplus D_K(C_j)$
- 2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ?
==> selon la formule de chiffrement $c_j = E_K(C_{j-1} \oplus x_j)$, pour chiffrer x_j on doit avoir c_{j-1} . Donc on doit chiffrer x_{j-1} d'abord, qui ne peut se faire qu'après le chiffrement de x_{j-2} . Par récurrence, pour chiffrer x_j , on doit chiffrer tous les blocs précédents
- 3) Peut-on déchiffrer un bloc quelconque c_j sans déchiffrer les blocs qui le précèdent ? Expliquer ?
==> Oui car, selon la formule de déchiffrement $x_j = C_{j-1} \oplus D_K(C_j)$, on n'a besoin que de C_{j-1} .
- 4) Peut-on déchiffrer un bloc c_j en l'absence des autres blocs chiffrés ? Expliquer ?
==> non car, selon la formule de déchiffrement $x_j = C_{j-1} \oplus D_K(C_j)$, on a besoin de C_{j-1} .
- 5) Prenons le cas où $E_K(x) = D_K(x) = K \oplus x$. Supposons qu'un attaquant peut sniffer tous les cryptogrammes et qu'il a réussi à décrypter un bloc c_j (par cryptanalyse), montrer qu'il peut en déduire la clé de chiffrement K .
==> la formule de chiffrement $c_j = E_K(C_{j-1} \oplus x_j)$ devient équivalente à $c_j = K \oplus C_{j-1} \oplus x_j \implies c_j \oplus C_{j-1} \oplus x_j = K$
- 6) Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K doit être échangée d'une façon **sécurisée et authentifiée**. Pour cela A et B font appel au chiffrement asymétrique. A calcule la clé K , la chiffre pour obtenir KC et l'envoi à B.
 - g. Avec quelle clé A doit chiffrer K ? ==> **avec la clé publique de B**
 - h. Avec quelle clé B déchiffre KC ? ==> **avec sa clé privée**
 - i. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?
==> A ne peut pas prouver que la clé publique de B qu'il a utilisé appartient bien à B. De même, B ne peut pas prouver que KC vient réellement de A. Une solution pourrait être l'utilisation de certificats.

Exercice 5:

Soit M un message divisé en blocs $\{x_2, x_3, \dots, x_p\}$ chacun de taille n bits et soit K une clé de même taille que les blocs (n bits). Soit $\{c_2, c_3, \dots, c_p\}$ les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:

$C_0 = IV0$ (valeur initiale) ; $C_1 = IV2$ (valeur initiale) ; pour j de 2 à p , $c_j = E_K(C_{j-2} \oplus C_{j-1} \oplus x_j)$

La fonction E_K est inversible et son inverse est D_K c'est-à-dire que $D_K(E_K(x)) = x$

- 1) Donner l'opération de déchiffrement ? (rappel : $A \oplus A = 0$; $A \oplus 0 = A$, $A \oplus B = B \oplus A$) \implies **On a**
 $c_j = E_K(C_{j-2} \oplus C_{j-1} \oplus x_j) \implies D_K(c_j) = D_K(E_K(C_{j-2} \oplus C_{j-1} \oplus x_j)) \implies D_K(c_j) = C_{j-2} \oplus C_{j-1} \oplus x_j \implies$
 $C_{j-2} \oplus C_{j-1} \oplus D_K(c_j) = C_{j-2} \oplus C_{j-1} \oplus C_{j-2} \oplus C_{j-1} \oplus x_j \implies C_{j-2} \oplus C_{j-1} \oplus D_K(c_j) = C_{j-2} \oplus C_{j-2} \oplus C_{j-1} \oplus C_{j-1} \oplus x_j \implies$
 $C_{j-2} \oplus C_{j-1} \oplus D_K(c_j) = 0 \oplus 0 \oplus x_j \implies C_{j-2} \oplus C_{j-1} \oplus D_K(c_j) = x_j$
- 2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? \implies **non, selon la formule de chiffrement pour chiffrer x_j on doit avoir C_{j-1} et C_{j-2}**
- 3) Peut-on déchiffrer un bloc quelconque c_j sans déchiffrer les blocs qui le précèdent ? Expliquer ? **Oui car, selon la formule de déchiffrement, on n'a besoin que de C_{j-1} et C_{j-2}**
- 4) Peut-on déchiffrer un bloc c_j en l'absence des autres blocs chiffrés ? Expliquer ? \implies **non car, selon la formule de déchiffrement on a besoin de C_{j-1} et C_{j-2}** .
- 5) Prenons le cas où $E_K(x) = D_K(x) = K \oplus x$. Supposons qu'un attaquant peut sniffer tous les cryptogrammes et qu'il a réussi à décrypter un bloc c_j (par cryptanalyse), montrer qu'il peut en déduire la clé de chiffrement K. \implies la formule de chiffrement $c_j = E_K(C_{j-2} \oplus C_{j-1} \oplus x_j)$ **devient équivalente à**
 $c_j = K \oplus C_{j-2} \oplus C_{j-1} \oplus x_j \implies c_j \oplus C_{j-1} \oplus C_{j-2} \oplus x_j = K$
- 6) Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K est fixée par l'une des deux entités puis transmise à la deuxième entité. Proposer une solution permettant aux deux entités d'échanger la clé K d'une façon **sécurisée et authentifiée**. \implies **voir ex4 6)**

Exercice 6:

Comparer les deux modes de chiffrement symétrique CBC et ECB en se limitant aux critères suivants:

Critères	CBC	ECB
a) Deux blocs identiques (en utilisant la même clé K) donnent deux cryptogrammes identiques	F	V
b) Les blocs sont chiffrés indépendamment les uns des autres	F	V
c) Le déchiffrement d'un bloc nécessite le déchiffrement du bloc précédent	F	F
d) Une erreur de génération d'un bloc chiffré affecte le déchiffrement de tous les blocs	F	F
e) Une erreur de génération d'un bloc chiffré affecte le déchiffrement de tous les blocs suivants	F	F
f) Une erreur de génération d'un bloc chiffré affecte seulement le déchiffrement de ce bloc	V	V
g) La modification de l'ordre des blocs chiffrés affecte l'opération de déchiffrement	V	F
h) Une erreur de transmission d'un bloc chiffré (i) affecte le déchiffrement du bloc (i+2)	F	F
i) Après le chiffrement de tous les blocs, la modification d'un bloc et régénération du cryptogramme correspondant fausse tous les blocs chiffrés suivants	V	F
j) Après le chiffrement de tous les blocs, la modification d'un bloc et régénération du cryptogramme correspondant fausse le déchiffrement de tous les blocs chiffrés suivants	F	F
k) Après le chiffrement de tous les blocs, la modification d'un bloc et régénération du cryptogramme correspondant fausse seulement le bloc déchiffré suivant, lors de l'opération de déchiffrement	V	F

Algorithm CBC mode of operation

INPUT: k -bit key K ; n -bit IV ; n -bit plaintext blocks x_1, \dots, x_t .

SUMMARY: produce ciphertext blocks c_1, \dots, c_t ; decrypt to recover plaintext.

1. Encryption: $c_0 \leftarrow IV$. For $1 \leq j \leq t$, $c_j \leftarrow E_K(c_{j-1} \oplus x_j)$.
2. Decryption: $c_0 \leftarrow IV$. For $1 \leq j \leq t$, $x_j \leftarrow c_{j-1} \oplus E_K^{-1}(c_j)$.

Algorithm ECB mode of operation

INPUT: k -bit key K ; n -bit plaintext blocks x_1, \dots, x_t .

SUMMARY: produce ciphertext blocks c_1, \dots, c_t ; decrypt to recover plaintext.

1. Encryption: for $1 \leq j \leq t$, $c_j \leftarrow E_K(x_j)$.
 2. Decryption: for $1 \leq j \leq t$, $x_j \leftarrow E_K^{-1}(c_j)$.
-

Exercice 7:

On utilise pour les réseaux mobiles un système de chiffrement à clés symétriques pour la transmission de la voix. Chaque utilisateur possède une clé symétrique connue par l'opérateur des télécommunications et sauvegardée dans sa carte SIM. À la sortie, sa voix est chiffrée avec cette clé. Elle est ensuite déchiffrée par l'opérateur et chiffrée avec la clé symétrique du destinataire.

- 1) Cette méthode garantit-elle la confidentialité? Expliquer? ==> **non car l'opérateur télécom peut lire les messages échangés**
- 2) Proposer, à l'aide d'un schéma annoté, une solution utilisant le chiffrement asymétrique permettant la confidentialité (sans modifier le système de télécommunication). ==> **soit: K1S la clé symétrique partagée entre le client 1 et le serveur, K2S la clé symétrique partagée entre le client 2 et le serveur. Les clients 1 et 2 maintiennent la paire de clés publique/privée (pub1, priv1) et (pub2, priv2) respectivement. La solution est la suivante: le client 1 chiffre sa voix avec pub2 avant de la chiffrer avec K1S. Le client 2 déchiffre la voix reçue avec priv2 après l'avoir déchiffré avec K2S.**
- 3) En pratique, le temps qui sépare l'envoi et la réception de la voix ne doit pas dépasser, en général, 250 ms. Quels problèmes peuvent surgir si nous adoptons la solution de la question précédente? ==> **perte d'interactivité car le chiffrement asymétrique est très lent.**
- 4) Proposer une deuxième solution permettant de résoudre les problèmes identifiés au niveau de la question précédente. Expliquer? ==> **mettre en place une clé symétrique entre les deux clients (en utilisant le chiffrement asymétrique) et l'utiliser pour chiffrer la voix avant de la chiffrer avec la clé partagée avec le serveur.**

Exercice 8: (algorithme RSA)

- 1) Soit $p=23$, $q=29$, $e=493$ et $n=p \cdot q$. Calculer d en utilisant l'algorithme d'Euclide étendu, puis décrypter le cryptogramme 12. ==> $\varphi = (p-1)(q-1) = 616$
Essayer de trouver la relation suivante $e \times d + \beta \times \varphi = 1$
 $616 = ? \cdot e + ?$ ==> $616 = 1 \cdot 493 + 123$
==> $493 = 4 \cdot 123 + 1$, on a atteint un reste égal à 1 ==> on remonte

 $1 = 493 - 4 \cdot 123$
 $1 = 493 - 4(616 - 1 \cdot 493)$
 $1 = 5 \cdot 493 - 4 \cdot 616$ ==> $d=5$
- 2) Un professeur P envoie, par mail, les notes de ses étudiants au service examen SE de l'école. Les clés publiques de P et SE sont ($e_P=3, n_P=55$) et ($e_{SE}=3, n_{SE}=33$) respectivement.
 - a. Déterminer la clé privée (d_P) de P et celle de SE (d_{SE}). ==> **Pour P , on détermine p et q , $n=p \cdot q=55$ donc $p=11$ et $q=5$ ou l'inverse. Puis on suit la même méthode que 1), on trouve $d_P=27$. Pour SE , on trouve $d_{SE}=7$.**
 - b. Afin d'assurer la confidentialité, P chiffre chaque note avec la clé du SE . Donner le message chiffré correspondant à la note 12? ==> **soit m la note, $C = m^{e_{SE}} \bmod n_{SE}$ on trouve $C=12$.**
 - c. Pour assurer l'authenticité et la confidentialité, P signe chaque note puis il la chiffre avec la clé du SE . SE reçoit le message 23. Donner la note correspondante? ==> Soit m la note. P signe m et

obtient: $S = m^e \bmod n_p$ Puis chiffre S avec la clé publique de SE $CS = S^{e_{SE}} \bmod n_{SE} = 23$

Pour retrouver la note, on doit tout d'abord retrouver S: $S = CS^{d_{SE}} \bmod n_{SE} ==>$
 $S = 23^7 \bmod 33 = 23$ puis $m = S^d \bmod n_p = 23^{27} \bmod 55 = 12$

Algorithm Key generation for RSA public-key encryption

SUMMARY: each entity creates an RSA public key and a corresponding private key.
Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q , each roughly the same size.
 2. Compute $n = pq$ and $\phi = (p - 1)(q - 1)$. (See Note 8.5.)
 3. Select a random integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
 4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
 5. A 's public key is (n, e) ; A 's private key is d .
-

Algorithm RSA public-key encryption

SUMMARY: B encrypts a message m for A , which A decrypts.

1. *Encryption.* B should do the following:
 - (a) Obtain A 's authentic public key (n, e) .
 - (b) Represent the message as an integer m in the interval $[0, n - 1]$.
 - (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).
 - (d) Send the ciphertext c to A .
 2. *Decryption.* To recover plaintext m from c , A should do the following:
 - (a) Use the private key d to recover $m = c^d \bmod n$.
-

- 3) Soit A et B deux entités désirant échanger des messages chiffrés en utilisant l'algorithme RSA. A détient la clé publique $\{n_A, e_A\}$ et la clé privée $\{d_A, n_A\}$. B détient la clé publique $\{n_B, e_B\}$ et la clé privée $\{d_B, n_B\}$.
- a. Quel est le service de sécurité assuré par le schéma décrit ci-dessus? ==> **confidentialité**
 - b. Quelle clé B doit-il utiliser pour envoyer un message MSG chiffré à A? ==> **$\{n_A, e_A\}$**
 - c. Quelle clé A doit-il utiliser pour décrypter un message provenant de B? ==> **$\{d_A, n_A\}$**
 - d. A peut-il se rendre compte que le message MSG chiffré provient de B? ==> **non**
 - e. Quelles clés A doit-il utiliser pour signer et chiffrer un document pour B? ==> **pour signer: $\{d_A, n_A\}$, pour chiffrer $\{n_B, e_B\}$**
 - f. Quelles clés B doit-il utiliser pour déchiffrer le document et vérifier la signature? ==> **pour déchiffrer $\{d_B, n_B\}$, pour vérifier la signature $\{n_A, e_A\}$**
- 4) Une autorité de certification CA a généré un certificat pour soi même et un certificat pour un utilisateur user1
- a. Justifier par un exemple d'attaque le besoin d'utiliser les certificats pour la délivrance des clés publiques. ==> **voir l'attaque au niveau de l'ex3.**
 - b. Par quelle clé privée ont été signés les certificats du CA et du user1? ==> **par la clé privée du CA**
 - c. Par quel moyen un utilisateur user2 peut vérifier le certificat de user1 en local (sans faire la vérification chez le CA) ==> **par la clé publique du CA**
 - d. Comment user2 peut s'assurer que la clé publique du CA appartient bien à ce dernier. ==> **en utilisant le certificat du CA.**

Exercice 9:

Une chaîne de télévision TV1 diffuse des bulletins d'informations destinées au public et des films destinés seulement à ses abonnés. Chaque abonné doit payer un tarif mensuel au début de chaque mois pour pouvoir regarder les films. TV1 possède une paire de clés : clé publique et clé privée.

- 1) Sachant que des attaquants peuvent utiliser la fréquence de TV1 pour diffuser des bulletins d'informations au nom de TV1, donner une méthode permettant au public de s'assurer que les bulletins d'informations proviennent réellement de TV1 ?
- 2) Sachant que des attaquants peuvent modifier le contenu des bulletins d'informations en transit, donner une solution à ce problème ?
- 3) Pour s'assurer que les films ne soient regardés que par les abonnés. Le propriétaire de TV1 a proposé de chiffrer les films avec la clé publique de chaque abonné : chaque abonné recevra le film chiffré avec sa clé publique et peut le déchiffrer avec sa clé privée. Montrer que cette solution est inadéquate ?
- 4) Etant convaincu des limites de la solution proposée en 3) le propriétaire de TV1 fait appel à un spécialiste de sécurité qui lui propose de chiffrer les films avec une clé symétrique KSYM. Chaque abonné ayant payé son abonnement mensuel courant obtient une copie de cette clé. Proposer une méthode permettant de distribuer KSYM d'une façon sécurisée ?
- 5) Pour renforcer la sécurité de son système, la clé KSYM peut être mise à jour avant la fin du mois (dans le cas où la clé est divulguée à des personnes non abonnés). Donner une méthode pratique permettant la mise à jour de KSYM d'une façon sécurisée.
- 6) Pour des questions de traçabilité (pour savoir qui est en train de donner KSYM à des personnes non abonnés), chaque abonné obtient plusieurs sous clés qui dépendent de son identité. Ces sous clés seront introduits au module spécifique de déchiffrement qui va les combiner pour obtenir KSYM (sans la divulguer à l'abonné) et informer les propriétaires de TV1 automatiquement que les sous clés viennent d'être utilisées.
 - a. Montrer comment peut-on détecter que le même sous ensemble de clés a été utilisé plusieurs fois.
 - b. Cette méthode est-elle efficace dans le cas où l'abonné ré-initialise son appareil de réception et introduit les sous clés de nouveau