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?
   b. Pour un système à clés asymétrique?
2) En déduire le nombre de clés du système pour chaque cas

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^{ème} bit du message m et k[i] est le i^{ème} bit de la clé K, alors le i^{ème} bit de M⊕K est égal à (M[i] ⊕ K[i])). On note que pour tout X, X⊕X=0, X⊕0=X et X⊕Y=Y⊕X

1) Montrez que le "ou exclusif ⊕ " est une technique de chiffrement symétrique.
2) Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer**?**
3) Soit le protocole décrit par la figure 1 qui exploite le "ou exclusif⊕ " 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 ?
   b) Comment A peut-il déterminer M⊕K_B à partir de M⊕K_A⊕K_B ?
   c) Comment B retrouve t-il M ?
   d) Si tous les messages échangés peuvent être écoutés, ce protocole permet-il la confidentialité?

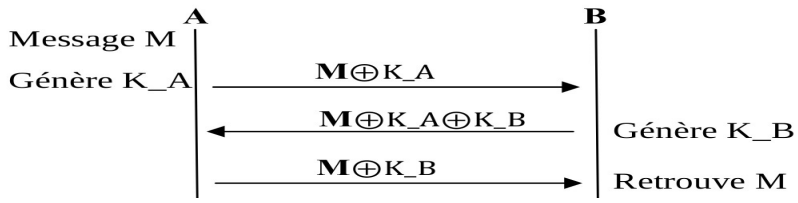

Figure 1: étapes pour l'échange d'un message M Chiffré (symétrique)

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).

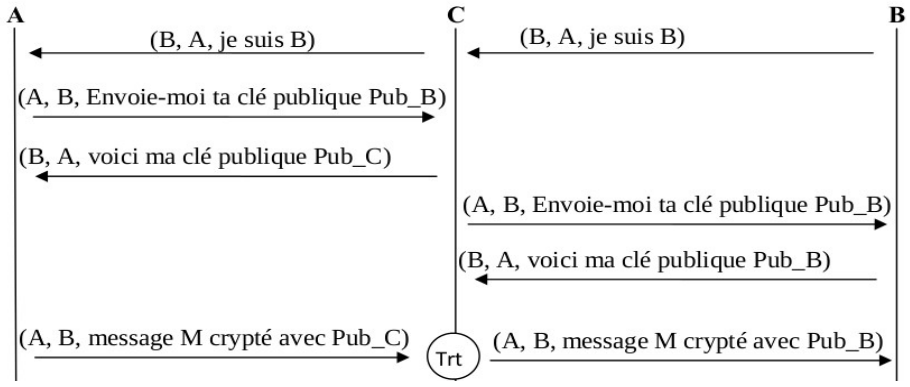

Figure 2: étapes pour l'échange d'un message M chiffré (asymétrique)

1) Quel est le traitement Trt effectué par C.

2) A et B se rendent-ils compte de l'existence de l'intrus C
3) Proposer une solution permettant de remédier à cette attaque

Exercice 4

Soit **M** un message divisé en blocs $\{x_1,x_2,x_3,\ldots x_p\}$chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_1,c_2,c_3,\ldots c_p\}$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 $\mathbf{D_K}$. Montrer que l'opération de déchiffrement est $\mathbf{x_j=C_{j-1}\oplus D_K(C_j)}$ (rappel : A⊕A=0 ; A⊕0=A, A⊕B= B⊕A)
2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ?
3) Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?
4) Peut-on déchiffrer un bloc $\mathbf{c_j}$ en l'absence des autres blocs chiffrés ? Expliquer ?
5) Prenons le cas où $\mathbf{E_K(x)=D_K(x)=K\oplus x}$. 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.
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?
    h. Avec quelle clé B déchiffre KC?
    i. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?

Exercice 5:

Soit **M** un message divisé en blocs $\{x_2,x_3,\ldots x_p\}$chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_2,c_3,\ldots c_p\}$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 $\mathbf{D_K}$ c'est-à-dire que $\mathbf{D_K}(\mathbf{E_K(x))=x}$

1) Donner l'opération de déchiffrement ? (rappel : A⊕A=0 ; A⊕0=A, A⊕B= B⊕A)
2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ?
3) Expliquer ?Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?
4) Peut-on déchiffrer un bloc $\mathbf{c_j}$ en l'absence des autres blocs chiffrés ? Expliquer ?
5) Prenons le cas où $\mathbf{E_K(x)=D_K(x)=K\oplus x}$. 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.
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**.

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		
b) Les blocs sont chiffrés indépendamment les uns des autres		
c) Le déchiffrement d'un bloc nécessite le déchiffrement du bloc précédent		
d) Une erreur de génération d'un bloc chiffré affecte le déchiffrement de tous les blocs		
e) Une erreur de génération d'un bloc chiffré affecte le déchiffrement de tous les blocs suivants		

f) Une erreur de génération d'un bloc chiffré affecte seulement le déchiffrement de ce bloc		
g) La modification de l'ordre des blocs chiffrés affectent l'opération de déchiffrement		
h) Une erreur de transmission d'un bloc chiffré (i) affecte le déchiffrement du bloc (i+2)		
i) Après le chiffrement de tous les blocs, la modification d'un bloc et régénération du cryptogramme correspondant fausse tous les blocs chiffrés suivants		
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		
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		

Algorithm CBC mode of operation

INPUT: k-bit key K; n-bit IV; n-bit plaintext blocks $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; 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 $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; 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 connu par l'opérateur des télécommunication et sauvagardé dans sa carte SIM. A la sortie, sa voix est chiffrée avec cette clé. Elle est ensuite déchiffrée par l'opérateur et chiffré avec la clé symétrique du destinataire.

1) Cette méthode garantit- elle la confidentialité? Expliquer ?
2) Proposer, à l'aide d'un schéma annoté, une solution utilisant le chiffrement asymétrique permettant la confidentialité (sans modifier le système de télécommunication).
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?
4) Proposer une deuxième solution permettant de résoudre les problèmes identifiés au niveau de la question précédente. Expliquer?

Exercice 8: (algorithme RSA)

1) Soit p=23, q=29, e=493 et n=p.q. Calculer d en utilisant l'algorithme d'euclide étendu, puis décrypter le cryptogramme 12.
2) Un Professeur **P** envoie, par mail, les notes de ses étudiants au service examen **SE** de l'école. Les clés publique 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}).
   b. Afin d'assurer la confidentialité, **P** chiffre chaque note avec la clé du **SE**. Donner le message chiffré correspondant à la note 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 ?

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 ?
   b. Quelle clé B doit-il utiliser pour envoyer un message MSG chiffré à A ?
   c. Quelle clé A doit-il utiliser pour décrypter un message provenant de B ?
   d. A peut-il se rendre compte que le message MSG chiffré provient de B ?
   e. Quelles clés A doit-il utiliser pour signer et chiffrer un document pour B ? Quelles clés B doit-il utiliser pour déchiffrer le document et vérifier la signature ?

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.
   b. Par quelle clé privée ont été signés les certificats du CA et du user1
   c. Par quel moyen un utilisateur user2 peut vérifier le certificat de user1 en local (sans faire la vérification chez le CA)
   d. Comment user2 peut s'assurer que la clé publique du CA appartient bien à ce dernier**.**

Exercice 9:

Une chaine de télévision TV1 diffuse des bulletins d'informations destinées au public et des films destinés seulement à ses abonnées. 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 abonnées. 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 payée 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 abonnée 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