TD Cryptographie et ACL

Exercice 1 cryptographie symétrique

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 a pu récupérer deux blocs consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Montrer que cet attaquant 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 **sécurisé et authentifié**. 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.
    a. Avec quelle clé A doit chiffrer K ?
    b. Avec quelle clé B déchiffre KC ?
    c. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?

Exercice 2 : chiffrement RSA

Question 1 : Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes:

Les deux nombres premiers p = 3 et q = 11
e = 7
Le message M = 5

Question 2 : Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35.
Que vaut M ?
Quelle est la clé privée de cet utilisateur ?

Exercice 4 : *ACL étendue*

```
Router(config-if)#  access-group 101 in
Router(config)#     interface ethernet 0
Router(config)#     access-list 101 deny tcp 192.168.10.0     0.0.0.255 any neg 80
```

(Ca veut dire interdire tout segment TCP, sauf celui qui est à destination du port 80)

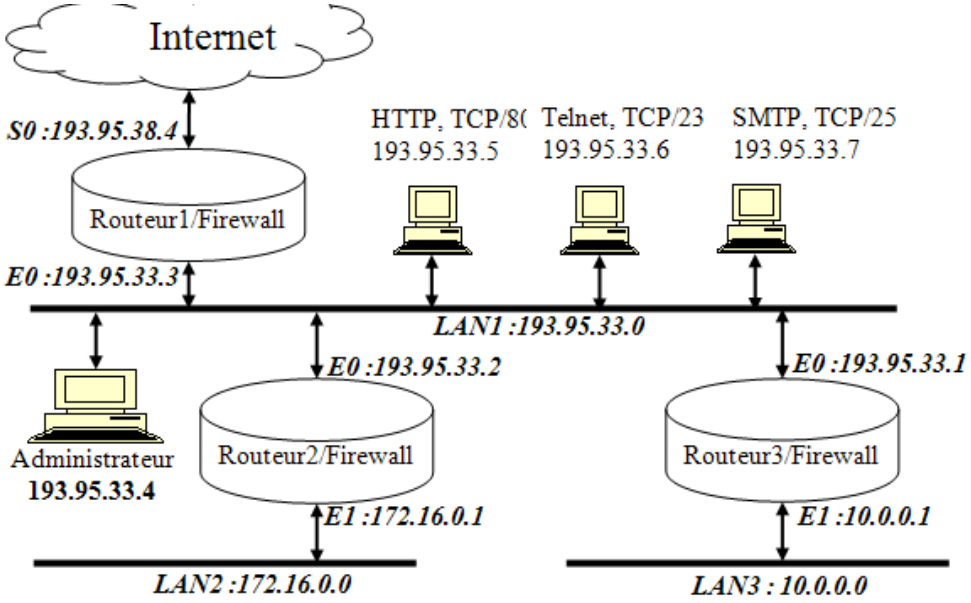
```
Router(config)#     access-list 101 deny tcp 192.168.10.0 0.0.0.255 any neg 21
Router(config)#     access-list 101 permit ip any any
```

1. Quel est l'effet de cette ACL ?

2. En devinant l'intention de l'administrateur, proposez une ACL correcte

Exercice 3 : Filtrage

Soit l'architecture du réseau suivant :



1) Considérons les politiques de sécurité suivantes :
   P1 : Permettre aux utilisateurs externes d'accéder aux serveurs HTTP et SMTP du LAN1.
   P2 : Permettre aux utilisateurs du LAN2 d'accéder aux serveurs du LAN3
   P3 : Permettre aux utilisateurs du LAN1 d'accéder à Internet

Ecrire les règles à implémenter pour chaque politique. Il faut préciser les routeurs dans lesquels on doit implémenter chaque politique ?

Règle	Adr IP Source	Adr IP destination	Protocole	Port source	Port dest	Action

2) Préciser les numéros de ports utilisés (port source et port destination) permettant à l'administrateur d'envoyer un trafic ICMP sur les machines internes (LAN1, LAN2 et LAN3) ? Expliquer ?
3) Doit-on considérer l'état du bit ACK lors de l'implémentation de règles de filtrage du service TFTP (Trivial File Transfer Protocol) qui fonctionne au dessus d'UDP ?
4) Soient les deux politiques suivantes et les règles de filtrage correspondantes :
   - Politiques :
   - Permettre au LAN3 d'accéder aux serveurs du LAN1 fonctionnant au dessus de TCP
   - Interdire l'accès du LAN3 au serveur Telnet du LAN1
     - Règles de filtrages

règle	Routeur	@IP source	@IP dest	Port source	port dest	protocole	ACK=1	Action
1	Routeur3	LAN3	LAN1	>1023	tous	TCP	*	Autoriser
2	Routeur3	LAN1	LAN3	tous	>1023	TCP	oui	Autoriser
3	Routeur3	LAN3	.33.6	>1023	23	TCP	*	Bloquer

   a. Est-ce que ces règles permettent à un utilisateur du LAN3 d'accéder au serveur Telnet du LAN1? Expliquer
   b. En déduire les règles permettant de répondre aux deux politiques spécifiées ? (les écrire)

Exercice 1:

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⊕A=0 ; A⊕0=A, A⊕B= B⊕A)

$c_j=E_K(C_{j-1}\oplus x_j) \Rightarrow D_K(c_j)= D_K(E_K(C_{j-1}\oplus x_j))$
$\Rightarrow D_K(c_j)= C_{j-1}\oplus x_j$
$\Rightarrow C_{j-1}\oplus D_K(c_j)= C_{j-1}\oplus C_{j-1}\oplus x_j$
$\Rightarrow C_{j-1}\oplus D_K(c_j)= x_j$

2) Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ?
   ⇒ **Non, selon la formule $x_j=C_{j-1}\oplus D_K(C_j)$, le chiffrement de x_j nécessite C_{j-1}**
3) Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?
   ⇒ **Oui, x_j ne dépend pas de x_{j-1}**
4) Peut-on déchiffrer un bloc **c_j** en l'absence des autres blocs chiffrés ? Expliquer ?
   ⇒ **Non, selon la formule $x_j=C_{j-1}\oplus D_K(C_j)$, le déchiffrement de c_j nécessite C_{j-1}**
5) Prenons le cas où **$E_K(x)=D_K(x)=K\oplus x$.** Supposons qu'un attaquant a pu récupérer deux blocs consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Montrer que cet attaquant peut en déduire la clé de chiffrement K.
   Dans ce cas : $c_j=K\oplus C_{j-1}\oplus x_j \Rightarrow K= c_j\oplus C_{j-1}\oplus x_j$
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 **sécurisé et authentifié**. 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.
   a. Avec quelle clé A doit chiffrer K ? ⇒ **avec la clé publique de B**
   b. Avec quelle clé B déchiffre KC ? ⇒**avec sa clé privée**
   c. Expliquer pourquoi cette méthode n'est pas authentifiée et proposer une solution ?
      ⇒ **Rien ne garantit l'appartenance de la clé publique de B à B.**
      Solution : certification de la clé publique de B.

Exercice 2 : chiffrement RSA

Question 1 : Effectuer le chiffrement et le déchiffrement en utilisant l'algorithme RSA pour les valeurs suivantes:
Les deux nombres premiers p = 3 et q = 11
e = 7
Le message M = 5
⇒ N=pq=3*11=33 et φ=(p-1)(q-1)=2*10=20
⇒ e.d=1 mod φ ⇒ 7*d=1mod 20 ⇒d=3
Chiffrement : $C=M^e \bmod N=5^7 \bmod 33 = 14$
Déchiffrement : $M= C^d \bmod N \Rightarrow M=C^3 \bmod 33=14^3 \bmod 33 =5$

Question 2 : Soit un système à clé publique utilisant le RSA, vous interceptez le texte chiffré C=10 envoyé par un utilisateur dont la clé publique est e = 5 et n = 35.
Que vaut M ?
Quelle est la clé privée de cet utilisateur ?

⇒ N=35 ⇒ p*q=35 ⇒ p=5 et q= 7 ou p=7 et q=5 ⇒ φ=(p-1)(q-1)=6*4=24
⇒ e.d=1 mod φ ⇒ 5*d=1mod 24 ⇒d=5
⇒ $M= C^d \bmod N \Rightarrow M= 10^5 \bmod 35 =5$

Exercice 3 : *ACL étendue*

Router(config-if)# access-group 101 in
Router(config)# interface ethernet 0
Router(config)# access-list 101 deny tcp 192.168.10.0 0.0.0.255 any neg 80
(Ca veut dire interdire tout segment TCP, sauf celui qui est à destination du port 80)

Router(config)# access-list 101 deny tcp 192.168.10.0 0.0.0.255 any neg 21
Router(config)# access-list 101 permit ip any any

1. Quel est l'effet de cette ACL ?

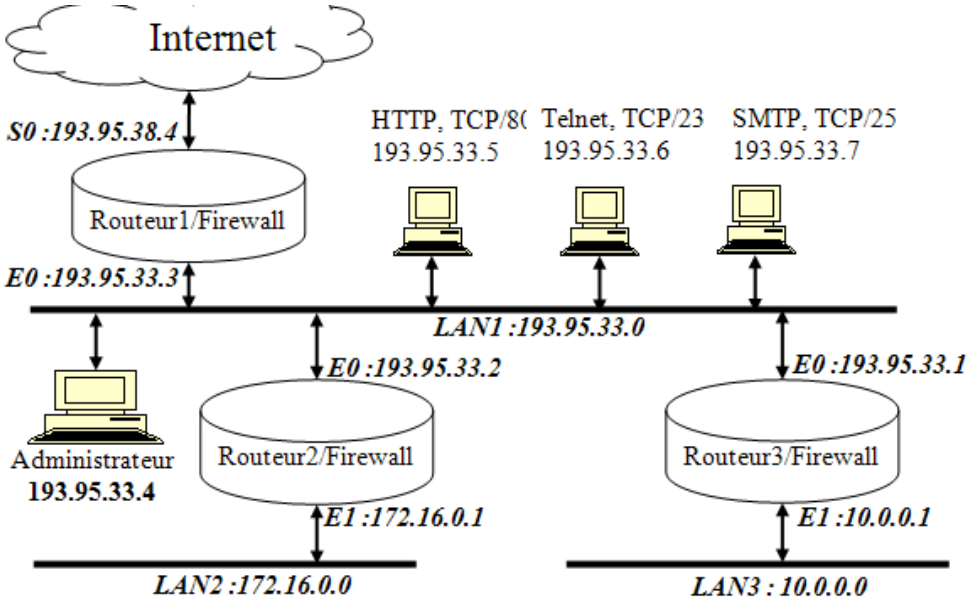
 Cette ACL permet d'interdire tout segment TCP (y compris ceux à destination du port 21), sauf celui à destination du port 80. Le reste du trafic est autorisé.

2. En devinant l'intention de l'administrateur, proposez une ACL correcte

 L'administrateur veut autoriser l'accès http (TCP/80) et FTP (TCP/21) ainsi que tout autre trafic différent de TCP (**tout autre trafic TCP sera interdit)**

Exercice 4 : Filtrage

Soit l'architecture du réseau suivant :



1) Considérons les politiques de sécurité suivantes :

P1 : Permettre aux utilisateurs externes d'accéder aux serveurs HTTP et SMTP du LAN1. **routeur1**

P2 : Permettre aux utilisateurs du LAN2 d'accéder aux serveurs du LAN3 **routeur2 et routeur 3**

P3 : Permettre aux utilisateurs du LAN1 d'accéder à Internet

Ecrire les règles à implémenter pour chaque politique. Il faut préciser les routeurs dans lesquels on doit implémenter chaque politique ?

Règle	Adr IP Source	Adr IP destination	Protocole	Port source	Port dest	Action
1	*	193.95.33.7	TCP	>1023	25	accepter
2	193.95.33.7	*	TCP	25	>1023	accepter
3	*	193.95.33.5	TCP	>1023	80	accepter
4	193.95.33.5	*	TCP	80	>1023	accepter
5	LAN2	LAN3	*	>1023	*	accepter
6	LAN3	LAN2	*	*	>1023	accepter
7	LAN1	*	*	>1023	*	accepter
8	*	LAN1	*	*	>1023	accepter

2) Préciser les numéros de ports utilisés (port source et port destination) permettant à l'administrateur d'envoyer un trafic ICMP sur les machines internes (LAN1, LAN2 et LAN3) ? Expliquer ?

 Pas de numéro de port car ICMP est un protocole de niveau 3 encapsulé dans IP.

3) Doit-on considérer l'état du bit ACK lors de l'implémentation de règles de filtrage du service TFTP (Trivial File Transfer Protocol) qui fonctionne au dessus d'UDP ?

 Non, le bit ACK est spécifique à TCP (il n' y a pas de bit ACK dans UDP)

4) Soient les deux politiques suivantes et les règles de filtrage correspondantes :

- Politiques :
  - Permettre au LAN3 d'accéder aux serveurs du LAN1 fonctionnant au dessus de TCP
  - Interdire l'accès du LAN3 au serveur Telnet du LAN1
- Règles de filtrages

règle	Routeur	@IP source	@IP dest	Port source	port dest	protocole	ACK=1	Action
1	**Routeur3**	**LAN3**	**LAN1**	**>1023**	**tous**	**TCP**	*****	**Autoriser**
2	**Routeur3**	**LAN1**	**LAN3**	**tous**	**>1023**	**TCP**	**oui**	**Autoriser**
3	**Routeur3**	**LAN3**	**.33.6**	**>1023**	**23**	**TCP**	*****	**Bloquer**

a. Est-ce que ces règles permettent à un utilisateur du LAN3 d'accéder au serveur Telnet du LAN1? Expliquer ?

 Oui, la machine .33.6 fait partie du LAN1et les deux première règles permettent aux utilisateurs du LAN3 d'accéder aux serveurs du LAN1 peu importe le numéro de port (tous les ports destination sont permis)

b. En déduire les règles permettant de répondre aux deux politiques spécifiées ? (les écrire)

 Garder les mêmes règles et mettre à jour seulement le port destination dans la première règle pour avoir « tous sauf 23 »
 Une deuxième réponse pourrait être le ré-ordonnancement des règles en mettant la règle 3 en premier puis la règle 1 puis la règle 2.