Exercice 4 – Applications de sécurité

Soit les tables suivantes :

a)

$$(1)\ \mathrm{X} \rightarrow \mathrm{A}:\ M \,\|\, \mathrm{E}_{K_{xa}}\left[ID_X \,\|\, \mathrm{H}(M)\right]$$
$$(2)\ \mathrm{A} \rightarrow \mathrm{Y}:\ \mathrm{E}_{K_{ay}}\left[ID_X \,\|\, M \,\|\, \mathrm{E}_{K_{xa}}\left[ID_X \,\|\, \mathrm{H}(M)\right] \| \, T\right]$$

b)

$$(1)\ \mathrm{X} \rightarrow \mathrm{A}:\ ID_X \,\|\, \mathrm{E}_{KR_x}\left[ID_X \,\|\, \mathrm{E}_{KU_y}\left(\mathrm{E}_{KR_x}[M]\right)\right]$$
$$(2)\ \mathrm{A} \rightarrow \mathrm{Y}:\ \mathrm{E}_{KR_a}\left[ID_X \,\|\, \mathrm{E}_{KU_y}\left[\mathrm{E}_{KR_x}[M]\right] \| \, T\right]$$

notation :

X = sender	M = message
Y = recipient	T = timestamp
A = Arbiter	

1. Modifiez la table a) pour permettre à Y de vérifier la signature.

2. Modifiez la signature digitale de la table b) pour éviter un triple chiffrement du message initial.

3. Il y a 3 façons d'utiliser des nonces.
   Soit N_a un nonce généré par A. A et B partagent la clé K et f() est une fonction d'incrémentation.
   Voici ces 3 usages :
   1. A → B : N_a puis B → A : $E_k(N_a)$
   2. A → B : $E_k(N_a)$ puis B → A : N_a
   3. A → B : $E_k(N_a)$ puis B → A : $E_k(f(N_a))$

   Donnez une situation appropriée à chaque usage.

4. PGP utilise le CFB dans l'algorithme CAST-128 alors que la plupart des autres schémas symétriques utilisent le CBC. Pour rappel :

   CBC : $C_i = E_k[C_{i-1}$ XOR $P_i]$ et $P_i = C_{i-1}$ XOR $D_k[C_i]$
   CFB : $C_i = P_i$ XOR $E_k[C_{i-1}]$ et $P_i = C_i$ XOR $E_k[C_{i-1}]$

   Ces 2 schémas semblent fournir une sécurité égale. Pourquoi PGP utilise-t-il le CFB ?

5. L'architecture d'IPSEC précise que quand on utilise 2 SA en mode transport afin d'employer les protocoles AH et ESP simultanément sur un flux bout à bout, seul l'ordre ESP avant AH est approprié.
   Pourquoi cette approche est-elle recommandée plutôt que AH avant ESP ?