Protocoles de sécurité et vérification
Description du protocole proposé
Membres du groupe : Aymane OUKHATOU, Erika BUREI ALVES, Fahd TOUSSI

Chronos Protocol

Le protocole est décrit comme suit :

M1. $A \rightarrow S : ID_A,\ \{|K, M|\}_{K(A,S)},\ \{|B|\}_{K(A,S)}$

M2. $S \rightarrow B : ID_S,\ \{|K|\}_{K(B,S)},\ \{|A|\}_{K(B,S)},\ \{M\}_{pub(B)}$

M3. $B \rightarrow A : ID_B,\ \{|M+1|\}_K$

Connaissances initiales : Chaque agent X partage une clé symétrique $K(X, S)$ avec le serveur de confiance S. Les agents connaissent également les clés publiques $pub(C)$ des autres agents. Chaque participant possède aussi un identifiant ID_X unique et public, envoyé en clair au début de chaque message afin d'indiquer l'origine de l'envoi.

Valeurs générées lors de l'exécution :

— K est une clé de session générée par A.

— M est un nonce de session aléatoire, unique et limité dans le temps.

Description du protocole :

— **Étape 1 :** A envoie à S son identifiant ID_A, la clé de session K et l'identificateur de session M, chiffrés avec la clé symétrique partagée $K(A, S)$. A envoie aussi l'identité du destinataire B, chiffrée avec la même clé symétrique. L'identifiant ID_A permet au serveur S de reconnaître immédiatement l'expéditeur et donc de sélectionner la bonne clé $K(A, S)$ pour le déchiffrement. À la réception, le serveur S vérifie que le nonce M n'a jamais été utilisé auparavant. Si M existe déjà dans sa base de sessions actives, la requête est rejetée.

— **Étape 2 :** Après la vérification du nonce M, le serveur S envoie à B son identifiant ID_S, la clé de session K et l'identité de A (chiffrées avec la clé symétrique $K(B, S)$). Le nonce de session M est transmis à B chiffré avec la clé publique de B. L'identifiant ID_S permet à B de reconnaître l'origine du message comme venant du serveur de confiance et d'utiliser la clé $K(B, S)$ appropriée. Le serveur enregistre ensuite la session M dans sa base de données pour éviter toute réutilisation future.

— **Étape 3 :** B répond à A en envoyant son identifiant ID_B et le message $\{M + 1\}_K$, chiffré avec la clé de session K. L'identifiant ID_B permet à A d'identifier l'origine du message et de savoir qu'il doit être déchiffré avec la clé de session K. Cette étape prouve que B possède bien la clé K et confirme la fraîcheur de la session. À la réception, A vérifie que la valeur de M utilisée dans la réponse correspond bien au même nonce de session que celui envoyé initialement

Propriétés de sécurité :

— **Secret.** La clé de session K n'est connue que par A, B et le serveur S honnête.

— **Authentification.** La réponse $\{M+1\}_K$ prouve à A que B possède bien la clé K. À propos des identifiants ID_X, leur présence permet simplement d'indiquer l'origine des messages. Une éventuelle modification d'un ID_X par un adversaire n'affecterait pas la sécurité du protocole, car le contenu chiffré resterait incohérent et ne pourrait pas être déchiffré avec la clé appropriée.

— **Fraîcheur.** L'utilisation d'un nonce M aléatoire, unique et limité dans le temps empêche les attaques par rejeu.

Coût du protocole : 117

— **Étape 1 :** $1 + 63 + 12 = 76$

— **Étape 2 :** $1 + 12 + 12 + 3 = 28$

— **Étape 3 :** $1 + 13$