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 :

$$\textbf{M1.} \quad A \rightarrow S : \{|K, M|\}_{K(A,S)},\ \{|B|\}_{K(A,S)}$$
$$\textbf{M2.} \quad S \rightarrow B : \{|K|\}_{K(B,S)},\ \{|A|\}_{K(B,S)},\ \{M\}_{(pub(B))}$$
$$\textbf{M3.} \quad B \rightarrow A : \{|M+1|\}_{K}$$

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.

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 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 clé symétrique partagée avec le serveur de confiance S.

— **Étape 2 :** S transmet à B la clé de session K et l'identité de A (chiffrés avec la clé symétrique $K(B, S)$). Le nonce de session M est transmis à B chiffré avec la clé publique de B.

— **Étape 3 :** B répond à A en envoyant $M + 1$ chiffré avec la clé de session K, ce qui prouve la possession de K et la fraîcheur de la session.

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.

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

Coût du protocole : 114

— **Étape 1 :** 63 + 12 = 75

— **Étape 2 :** 12 + 12 + 3 = 27

— **Étape 3 :** 12