Description du protocole « Semi-Croustillant »

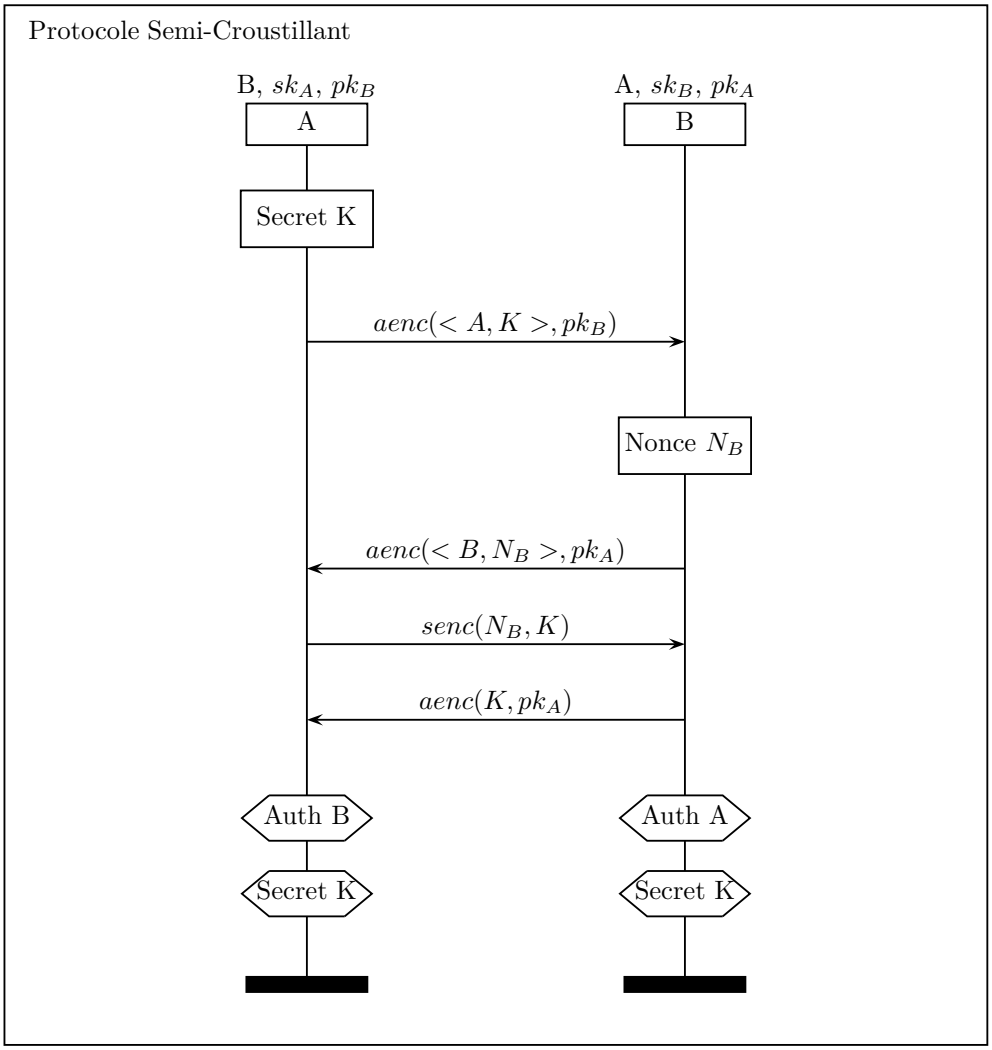
Benoît Fournier
Grégory Martin

30 novembre 2017

1 Description du protocole

Version 2017.11.30

$$A \to B : aenc(< A, K >, pk_B)$$
$$B \to A : aenc(< B, N_B >, pk_A)$$
$$A \to B : senc(N_B, K)$$
$$B \to A : aenc(K, pk_A)$$



Connaissances Initiales

Au début on suppose :
— L'agent A connaît la clef publique de B et connaît la clef privée de A.
— L'agent B connaît la clef publique de A et connaît la clef privée de B.

Valeurs générés au cours du protocole

— K est le secret frais généré par A.
— N_B est le nonce généré par B.

Détail du protocole

Etape 1 : A envoie à B l'information K ainsi que son identifiant A, le tout chiffré avec la clé publique de B.

Etape 2 : B génère un nonce nommé N_B.

Etape 3 : B envoie un message composé de son identité et du nonce N_B, chiffrant le message avec la clef publique de A.

Etape 4 : A envoie un message de confirmation d'identité à B en lui renvoyant le nonce N_B, chiffré symétriquement avec le secret K.

Etape 5 : B confirme à A le secret partagé, envoyant ce secret K chiffré asymétriquement avec la clef publique de A.

Propriétés de sécurité

— Confidentialité : Les deux agents A et B sont les seuls à connaître K.
— Authentification : Si B termine en pensant avoir reçu K de A alors A a effectivement envoyé K à B. Si A termine en ayant envoyé K à B alors B a bien reçu K.

Poids du protocole

Message 1 : 1+50+1+1+1=54
Message 2 : 1+50+1+1+1=54
Message 3 : 1+1+1=3
Message 4 : 1+1+1=3
— Poids total : 114