L'équipe Proto-Chorale attaque le protocole Azote

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de l'attaque est d'envoyer à B K_{bc} en se faisant passer pour A

2 Scénario de l'attaque

1. $C \rightarrow B : A, \{B, K_{bc}\}_{K_{cs}}$. B ne connait ni la clé de chiffrage ni le contenu chiffré. Il semble discuter normalement avec A.
2. $B \rightarrow S : A, \{B, K_{bc}\}_{K_{cs}}, \{Nb\}_{K_{bs}}$ Ce message sera bloqué par C.
3. $C \rightarrow S : C, \{B, K_{bc}\}_{K_{cs}}, \{Nb\}_{K_{bs}}$ Avec cette modification, le serveur peut traiter les informations pour B et C sans problème.
4. $S \rightarrow B : \{K_{bc}\}_{K_{bs}}$
5. $S \rightarrow C : \{Nb\}_{K_{cs}}$
6. $C \rightarrow B : \{Nb\}_{K_{bc}}$ C assure ici à B qu'il est bien A. La propriété d'authentification est donc non-respectée.