L'équipe Proto-Chorale attaque le protocole A-TeamV3

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de l'attaque est de se faire passer pour A aux yeux de B.

2 Scénario de l'attaque

C entame une discussion avec B en se faisant passer pour A :

1. $C(A) \rightarrow B : \{A, A\}_{pub(B)}$ C se fait passer pour A.
2. $B \rightarrow A : \{B\}_{N_b}, \{A\}_{N_b}, \{N_b\}_{pub(A)}$ Ce message sera **bloqué** et jamais reçu par A.
3. $C(A) \rightarrow B : \{A\}_{N_b}$ C peut utiliser une partie du message qu'il aura intercepté pour finir la conversation.

3 Conclusion

La propriété d'authentification n'est pas respectée, puisque B pense avoir parlé avec A alors que A n'a jamais initié de conversation avec B.