L'équipe Proto-Chorale attaque le protocole AzoteV3

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

1. $A \rightarrow C : A, \{N_a\}_{pub(C)}$
2. $C \rightarrow B : A, \{N_a\}_{pub(B)}$
3. $B \rightarrow A : h(N_a), \{N_b\}_{pub(A)}$ C modifie les entêtes pour que A pense que ça vient de lui
4. $A \rightarrow C \rightarrow B : \{\{secret\}_{N_b}\}_{N_a}$
5. $B \rightarrow A : \{secret\}_{pub(A)}$. C modifie les entêtes pour que A pense que ça vient de lui

3 Conclusion

La propriété d'authentification n'est pas respectée.