L'équipe Proto-Chorale attaque le protocole Protocoolv3

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est de se faire passer pour A aux yeux de B

2 Scénario de l'attaque

A entame une discussion avec C et une discussion avec B :

On considère durant la discussion que tous les messages envoyés de B vers A sont changés de manière à ce que A pense que les messages viennent de C.

- $A \rightarrow C : \{A, K\}_{pub(C)}$
- $C(A) \rightarrow B : \{A, K\}_{pub(B)}$
- $B \rightarrow A : \{\{N\}_{h(K_{pub(A)})}\}_{pub(A)}$
- $A \rightarrow C \rightarrow B : \{N\}_K$
- $B \rightarrow A : \{K\}_{pub(A)}$

A termine en pensant avoir discuté avec C et B termine en pensant avoir discuté avec A.

3 Conclusion

La propriété d'authentification n'est pas respectée.