Security Protocols and Verification

Attack of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Attack ?

This protocol does not work by itself.

1. $A \rightarrow B : A, \{|N_A, B|\}_{K_{AS}}$
2. $S \rightarrow B : S, \{|N_A, A|\}_{K_{BS}}$

How can S know that it has to send a message to B? How can B decrypt $\{|N_A, B|\}_{K_{AS}}$ without knowing the symmetric key K_{AS}?