Security Protocols and Verification

Design and Analysis of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

Team: **ASKO OM8464A2**

September / November 2025

Contents

1 Attack

1. $A \to I(B) : A, N_A$
2. $I \to B : I, N_I$
3. $B \to I : \{I, N_B, N_I\}_{pub(I)}$
4. $I(B) \to A : \{B, N_B, N_I\}_{pub(A)}$
5. $A \to I(B) : \{K_{AB}, N_B, N_A\}_{pub(B)}$
6. $I \to B : \{K_{IB}, N_B, N_I\}_{pub(B)}$
7.