Topici speciale în logică și securitate I

Protocoale de securitate I

Ioana Leuștean

Master anul II, Sem. I, 2019-2020

Ce este un protocol?

- Un protocol de securitate este un set de reguli și convețiii care determină un schimb de mesaje între doi sau mai mulți agenți, cu scopul de a implementa un serviciu de securitate.
- Un protocol este descris ca o serie de mesaje între agenți.
- Chiar dacă algoritmii criptografici pot fi foarte performanti, dacă protocolul este greșit conceput, comunicarea poate fi în pericol.

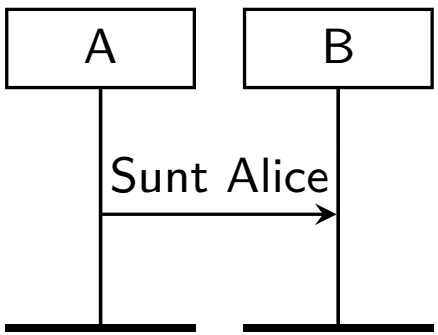
Security protocold are three-line programs
that people still manage to get wrong.- Roger Needham

Modelarea protocoalelor

Notația Alice-Bob

$A \longrightarrow B$: "Sunt Alice"

Message sequence charts MSC



Reguli pentru definirea protocoalelor

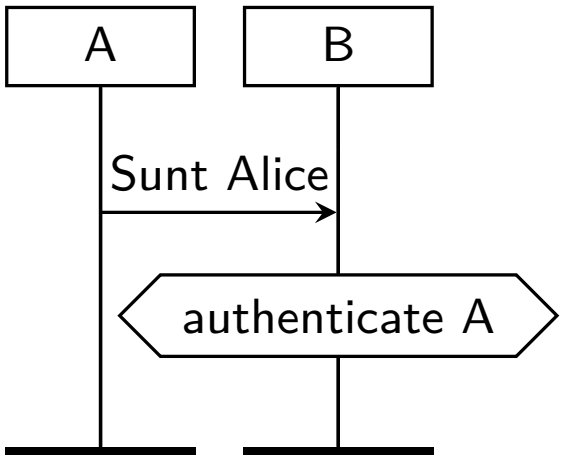
- Un protocol descrie mai multe comportamente, numite *roluri*; fiecare agent execută un rol.
- O *sesiune* este o execuție completă protocolului.
- Toți agenții cunosc protocolul în avans.
- Protocolul este complet și nu este ambiguu.
- Agenții nu au alt canal de comunicare în afara celui descris de protocol.
- Agenții folosesc numai mesajele descrise de protocol.

Modelarea protocoalelor

Notația Alice-Bob

$A \longrightarrow B$: "Sunt Alice"

Message sequence charts MSC



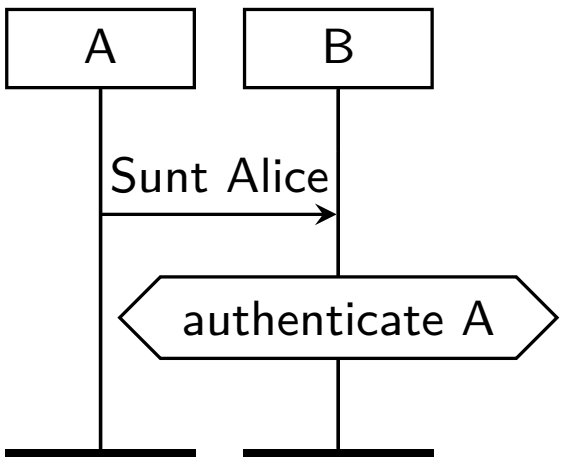
Se poate preciza scopul protocolului: *B știe că vorbește cu A*.

Modelarea protocoalelor

Notația Alice-Bob

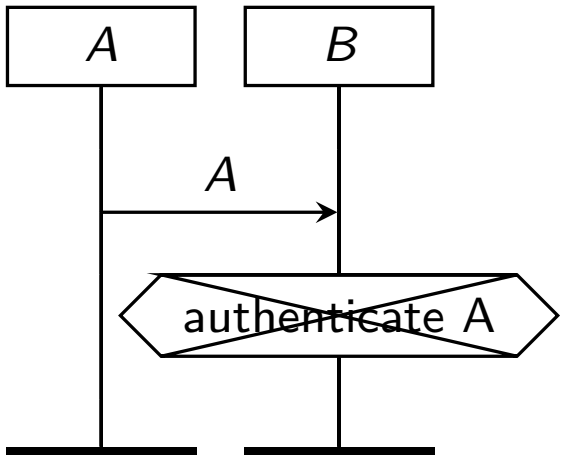
$A \longrightarrow B$: "Sunt Alice"

Message sequence charts MSC

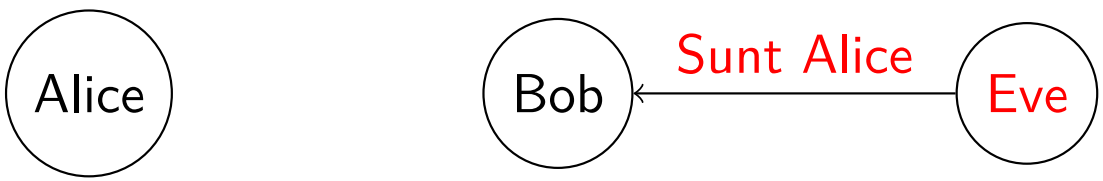


Se poate preciza scopul protocolului: *B știe că vorbește cu A*.
Este corect acest protocol?

Modelarea protocoalelor



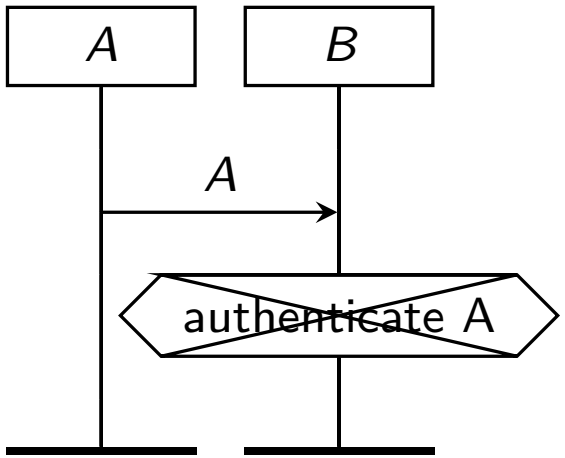
Este posibil ca un adversar să pretindă că este Alice!



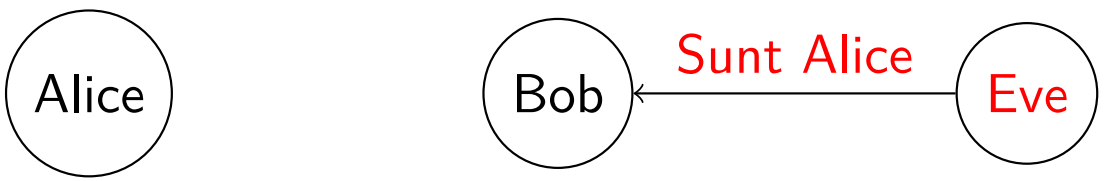
Eve o personifică pe Alice!

$E(A) \longrightarrow B : A$

Modelarea protocoalelor



Este posibil ca un adversar să pretindă că este Alice!



Eve o personifică pe Alice!

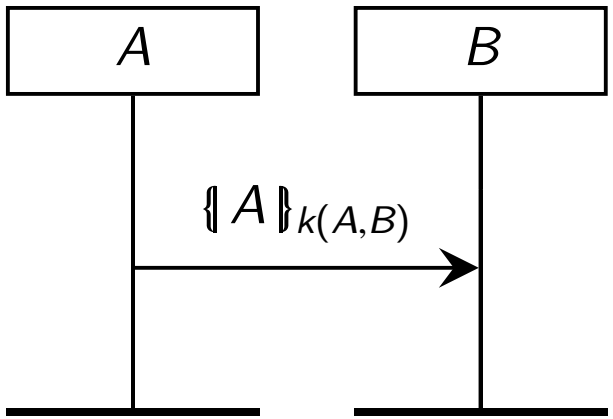
$E(A) \longrightarrow B : A$

Atacatorul are informație completă asupra desfășurării protocolului:

- poate intercepta mesaje,
- poate personifica orice rol.

Modelarea protocoalelor

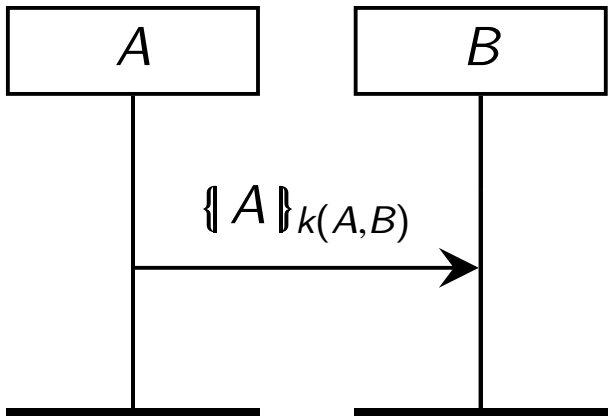
$A \longrightarrow B : \{\!|\, A \,|\!\}_{k(A,B)}$



- Mesajul este criptat cu $k(A, B)$, cheia comuna a lui A și B.

Modelarea protocoalelor

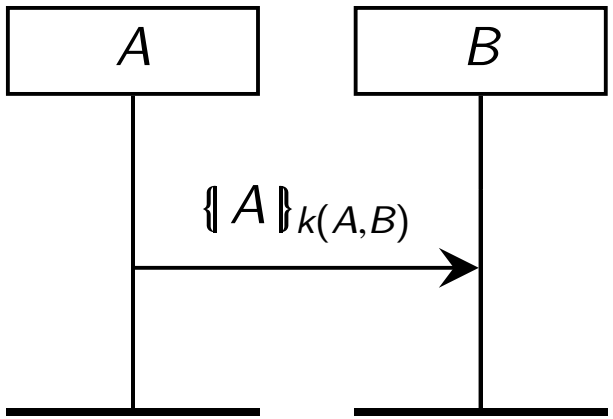
$A \longrightarrow B : \{\!|\, A \,|\!\}_{k(A,B)}$



- Mesajul este criptat cu $k(A, B)$, cheia comuna a lui A și B.
- Atacatorul poate intercepta mesajul criptat $\{\!|\, A \,|\!\}_{k(A,B)}$ dar nu îl poate decripta!

Modelarea protocoalelor

$A \longrightarrow B : \{\!|A|\!\}_{k(A,B)}$



- Mesajul este criptat cu $k(A, B)$, cheia comuna a lui A și B.
- Atacatorul poate intercepta mesajul criptat $\{\!|A|\!\}_{k(A,B)}$ dar nu îl poate decripta!
- În analiza protocoalelor de securitate vom adopta presupunerea "cutiei negre" din punctul de vedere al criptografiei (sau a "criptografiei perfecte"): atacatorul poate descifra un mesaj cifrat numai daca are cheia potrivită.

Modelarea adversarului

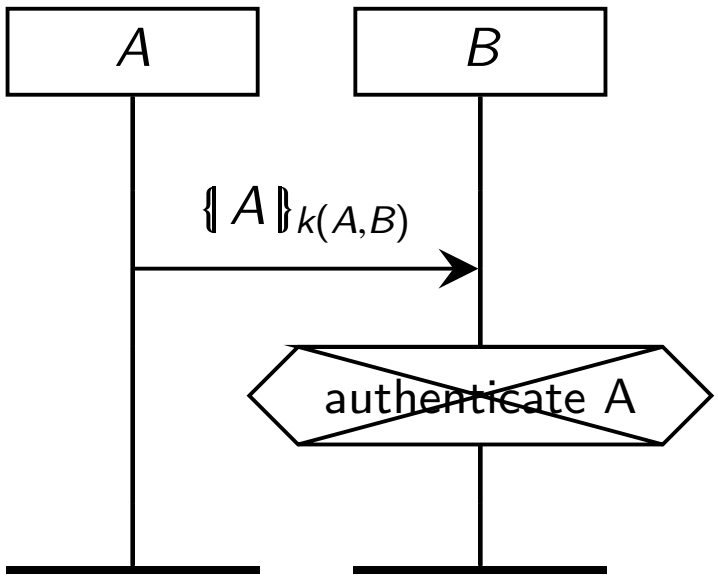
Modelul *Dolev-Yao*

- Adversarul are *informație completă* asupra protocolului:
  - poate să controleze canalele de comunicare,
  - poate să intercepteze mesaje,
  - are memorie nelimitată,
  - poate să personifice agenții,
  - poate să compună mesaje noi (dacă cunoaște toate componentele mesajului),
  - poate juca rolul unui agent legitim,

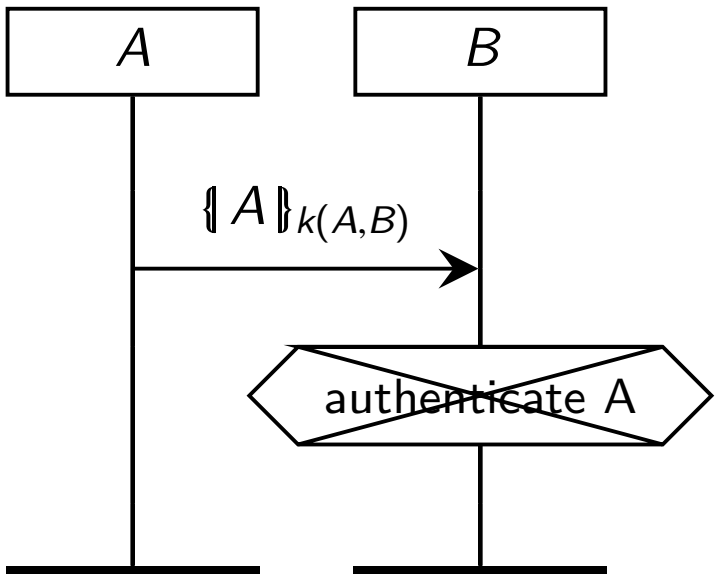
  ...

- Criptografia este *perfectă*:
  atacantul poate decripta un mesaj numai daca știe cheia de criptare.

Modelarea protocoalelor

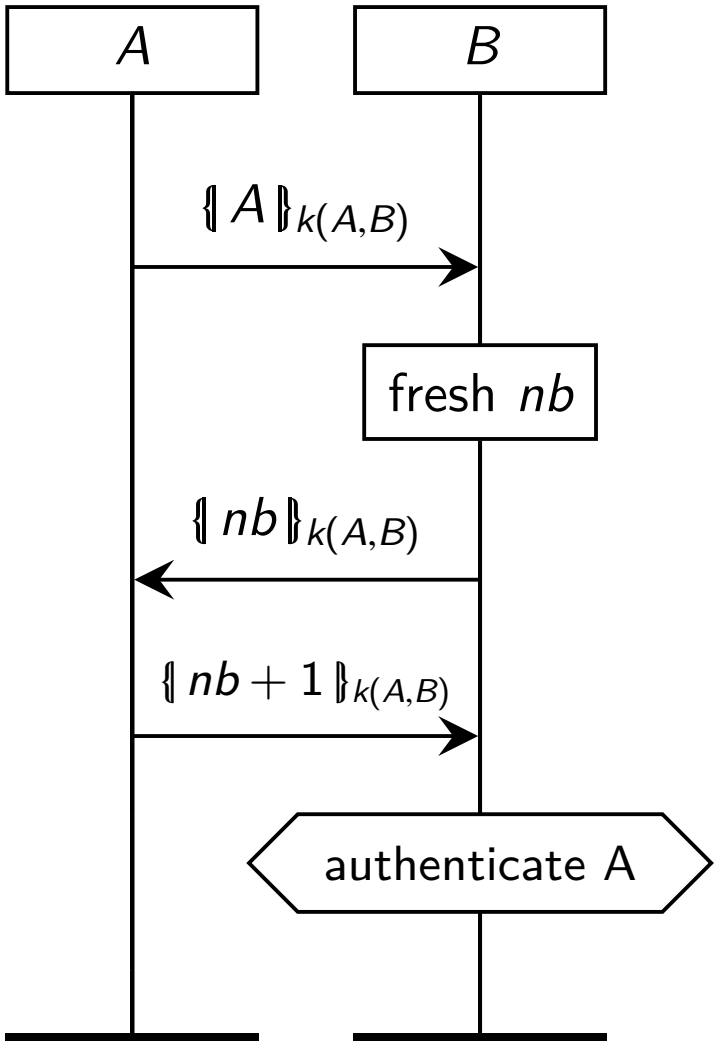


Modelarea protocoalelor



Atacatorul poate să o personifice pe Alice! Cum rezolvăm problema?

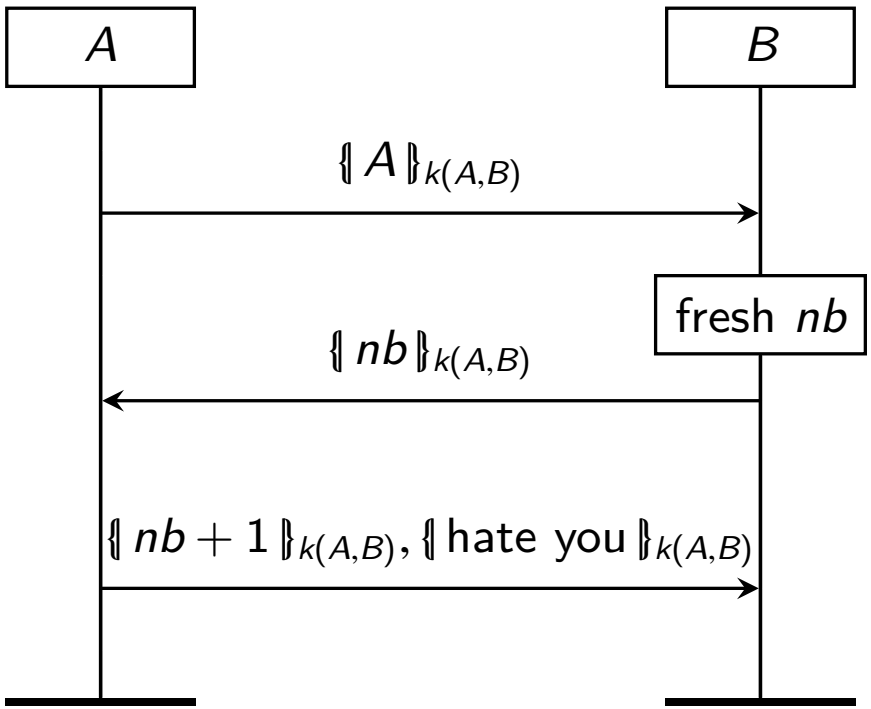
Nonce



- Folosim o valoare *proaspătă* (*nonce* = number used once)!
- Atacatorul poate intercepta mesajul $\{\!| nb |\!\}_{k(A,B)}$ dar nu poate extrage valoarea lui nb deoarece mesajul este mesajul cifrat
- Atacatorul nu poate trimite răspunsul așteptat de Bob.

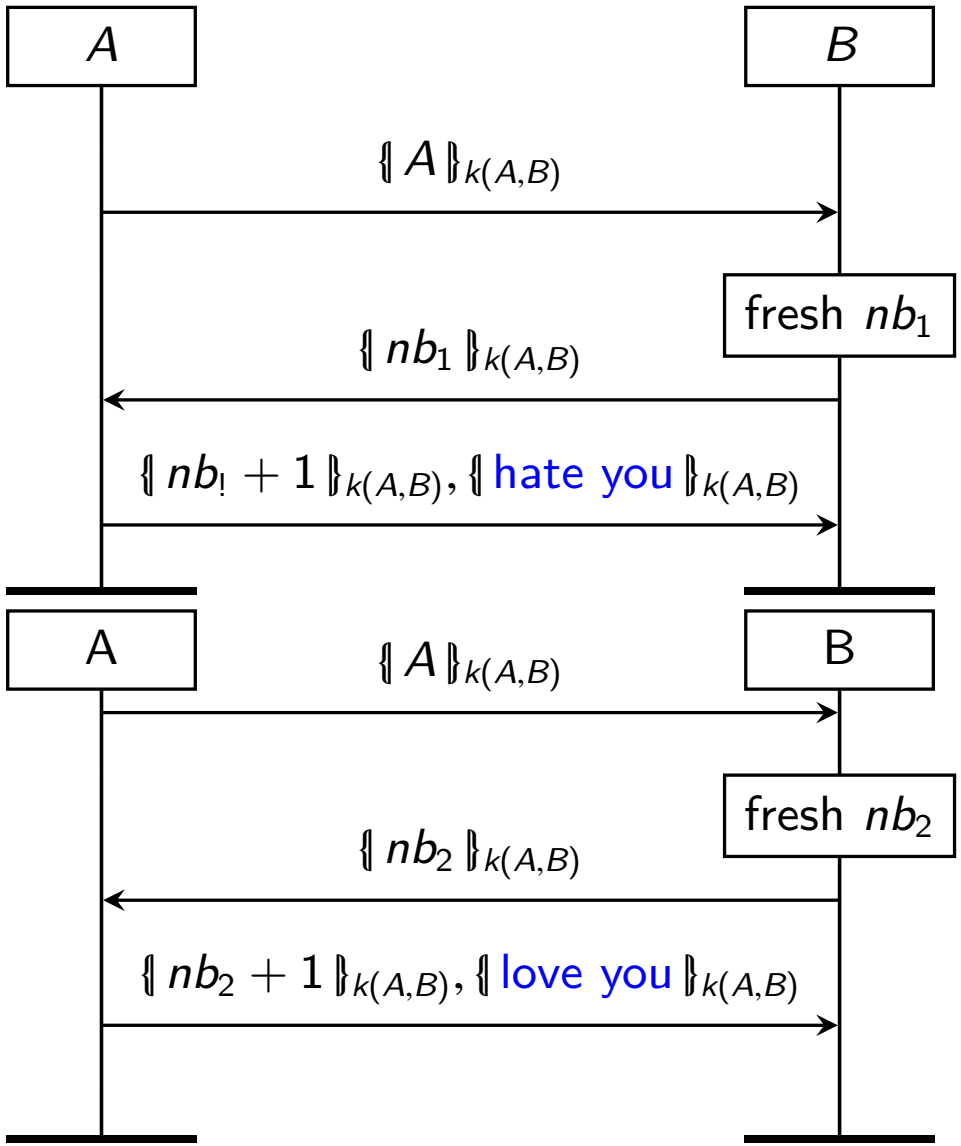
Modelarea protocoalelor

Considerăm următorul protocol:

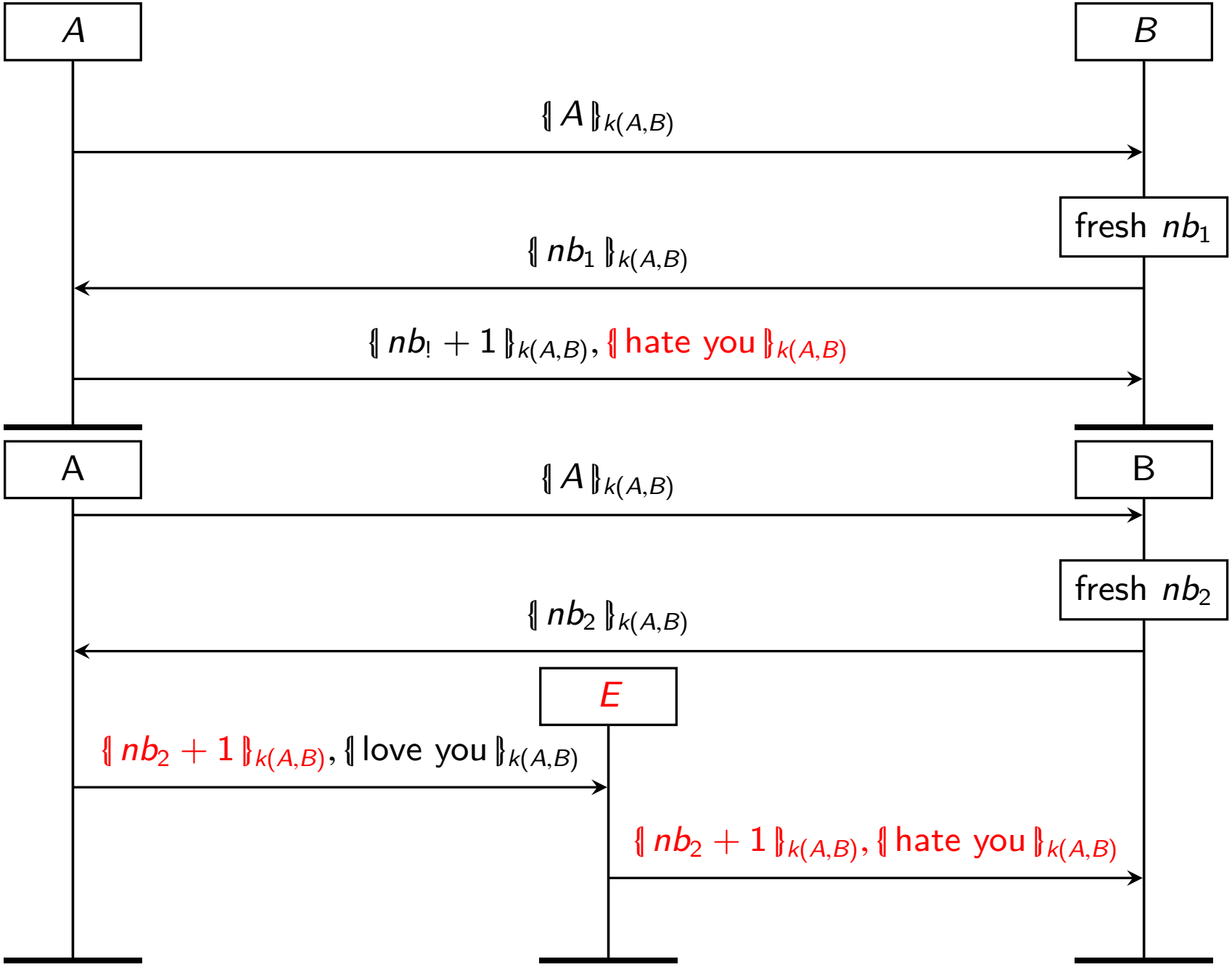


Dacă ne situăm în rolul lui Bob în protcol, ajungem la concluzia că Alice ne urăște în această sesiune!

Modelarea protocoalelor: două sesiuni



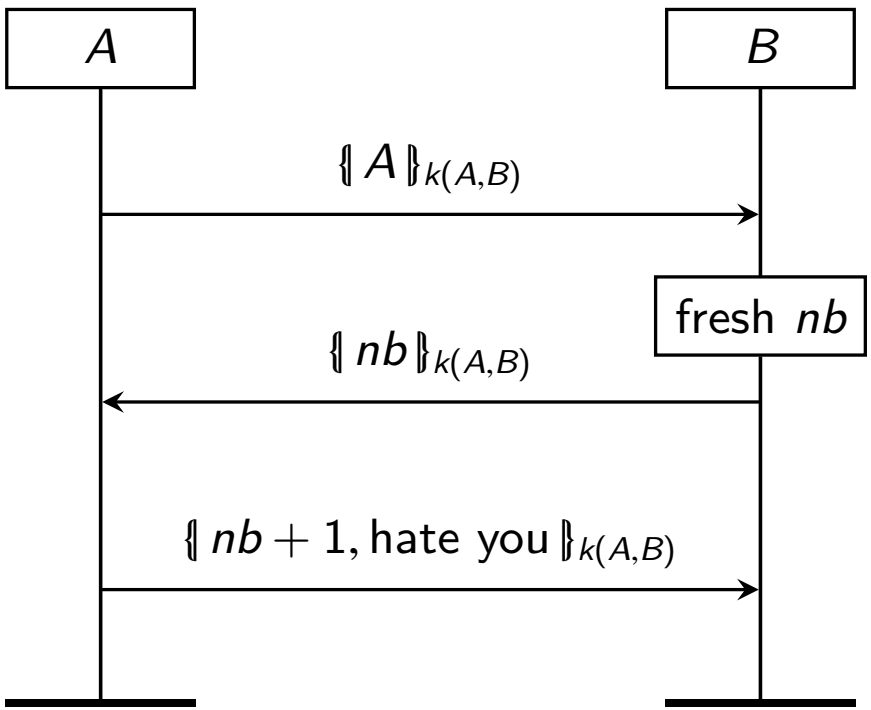
Atac de tip "replay"



Modelarea protocolalelor

- În exemplul anterior, adversarul fabrica un mesaj nou folosind bucăți vechi pe care le-a memorat.

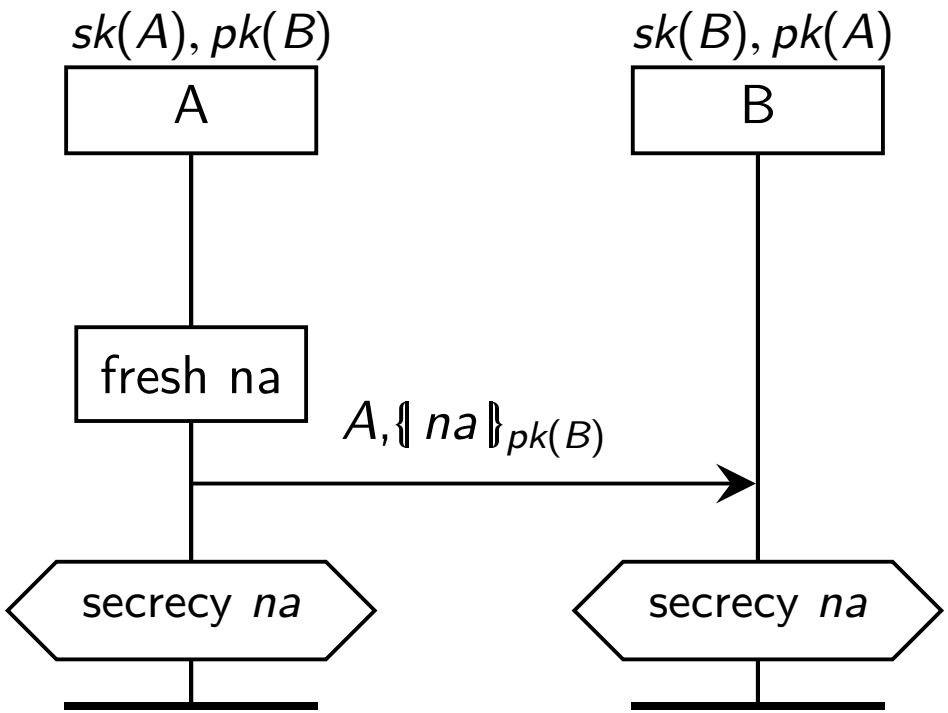
O variantă mai bună a acestui protocol:



Modelarea protocoalelor

- În exemplele anterioare, agenții foloseau un sistem cu chei simetrice.
- În multe protocoale cheia simetrică este un secret stabilit printr-un protocol bazat pe un sistem de criptare cu chei publice.

$A \longrightarrow B : A, \{\!|\, na \,|\!\}_{pk(B)}$



Exemplu

Considerăm următorul protocol:

$A \longrightarrow B : A, B, \{\!|\, A, na \,|\!\}_{pk(S)}$

$B \longrightarrow S : \{\!|\, A, na \,|\!\}_{pk(S)}, \{\!|\, B, na \,|\!\}_{pk(S)}$

Ce este greșit?

Exemplu

Considerăm următorul protocol:

$A \longrightarrow B : A, B, \{\!|\, A, na \,|\!\}_{pk(S)}$

$B \longrightarrow S : \{\!|\, A, na \,|\!\}_{pk(S)}, \{\!|\, B, na \,|\!\}_{pk(S)}$

Ce este greșit?

B nu poate afla na deoarece nu are cheia secretă $sk(S)$,
deci nu poate construi al doilea mesaj.

Exemplu

Considerăm următorul protocol:

$A \longrightarrow B : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

$B \longrightarrow A : \{\!|\, na, nb \,|\!\}_{k(A,B)}$

și următorul atac în care E îl personifică pe B:

$A \longrightarrow E(B) : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

$E(B) \longrightarrow A : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

Ce este greșit în această abordare?

Exemplu

Considerăm următorul protocol:

$A \longrightarrow B : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

$B \longrightarrow A : \{\!|\, na, nb \,|\!\}_{k(A,B)}$

și următorul atac în care E îl personifică pe B:

$A \longrightarrow E(B) : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

$E(B) \longrightarrow A : \{\!|\, A, B, na \,|\!\}_{k(A,B)}$

Ce este greșit în această abordare?

Atacul *nu are sens* deoarece A va detecta o anomalie: mesajul pe care îl primește are o altă structură.

Un atac presupune faptul că agenții onești au schimbat mesaje cu atacatorul fără să detecteze o anomalie!

Analiza formală a protocoalelor

- Am văzut cum analizăm *informal* protocoalele de securitate.
- Scopul *analizei formale* este acela de a defini un model al protocolului și de a-i analiza proprietățile într-o teorie matematică consistentă.
- Protocoalele reale sunt abstractizate, obținându-se modele mai simple. De exemplu protocolul (real) Kerberos are la baza protocolul (academic) Needham-Scroeder.
- Tipuri de modele formale
  - bazate pe logică epistemică, de exemplu BAN logic
  - bazate pe model-checking (tool-uri: Proverif, AVISPA, Scyther, Tamarin, ...)
  - ...

  Noi vom prezenta abordarea din:
  Cas Cremers and Sjouke Mauw. Operational Semantics and Veri cation of Security Protocols. Springer, 2012.

Analiza formală protocoalelor

- Componentele analizei formale
  - specificarea protocolului,
  - modelarea agenților,
  - modelarea comunicării,
  - modelarea adversarilor,
  - modelarea proprietăților de securitate.

- Limbajul formal va fi cel al unei *logici multi-sortate de ordinul I*
  - rolurile și mesajele sunt reprezentate prin termeni,
  - specificarea unui protocol este o mulțime de roluri,
  - cunoștințele adversarului sunt determinate printr-un sistem de deducție,
  - execuția protocolului se definește prin mulțimea urmelor (trace) unui sistem de tranziții etichetat,
  - proprietățile de securitate pot fi formalizate și demonstrate.