

# Modeli apstraktne kriptografije i protokoli (1)

Neva Slani

3. srpnja 2004.

Tema seminara su apstraktni modeli kriptografskih protokola. Izložena su tri modela: model transformacije multiskupova (*multiset rewriting*), model niti (*strands*), model struna (*cords*).

Kako se specificira protokol unutar pojedinog modela pokazano je na primjeru Dolev-Yao protokola javnog ključa.

Detaljnije je predstavljen model transformacija multiskupova. Akcije agenata protokola opisuju se pravilima prijelaza. Model daje dinamički opis razvoja protokola: djelovanjem pravila prijelaza na multiskup  $S$  dobija se novi multiskup  $S'$ , koji opisuju novonastalo stanje protokola. Djelovanje uljeza, zlonamjernog agenta koji ometa komunikaciju poštenih sudionika protokola, također je opisano pravilima prijelaza.

Spomenuti su osnovni rezultati dokazani u modelu vezani za sigurnost protokola, a tiču se pitanja složenosti (traženja napada na neki protokol).

## Literatura:

I. Cervesato, N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov.

*A comparison between strand spaces and multiset rewriting for security protocol analysis.* In *Software Security – Theories and Systems*, Mext-NSF-JSPS International Symposium, ISSS 2002.

N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. *Multiset rewriting and the complexity of bounded security protocols.* Technical report, 2002.