# Информациска безбедност

Предавање 4:
**Автентикациски протоколи**

Проф. д-р Весна Димитрова

# Протоколи

- Протоколи се правила кои мора да се следат и да се извршуваат во одреден редослед
- Кај компјутерските мрежи, протоколи се правила кои се следат во мрежните комуникациски системи
  - HTTP, FTP, TCP, UDP, PPP и многу други.
- Безбедносни протоколи се правила за комуникација кои се следат во безбедносна апликација

# Протоколи

- Протоколите треба да бидат многу прецизни
  - ако направиме навидум незначителна промена, таа може да направи значителна промена во протоколот
- Безбедносните протоколи може да имаат сериозни безбедносни пропусти
  - дури и самиот протокол да нема недостатоци, може неговата имплементација да има

# Протоколи

- Еден безбедносен протокол мора да исполнува одредени барања
  - ефикасни, лесни за користење, лесни за спроведување, флексибилни, исплатливи и широко употребливи
- Идеален безбедносен протокол треба да продолжи да работи и кога напаѓачот активно се обидува да го сруши и кога околината во која работи е променета
  - тешко е да се заштитиме од непознатото

# Протоколи

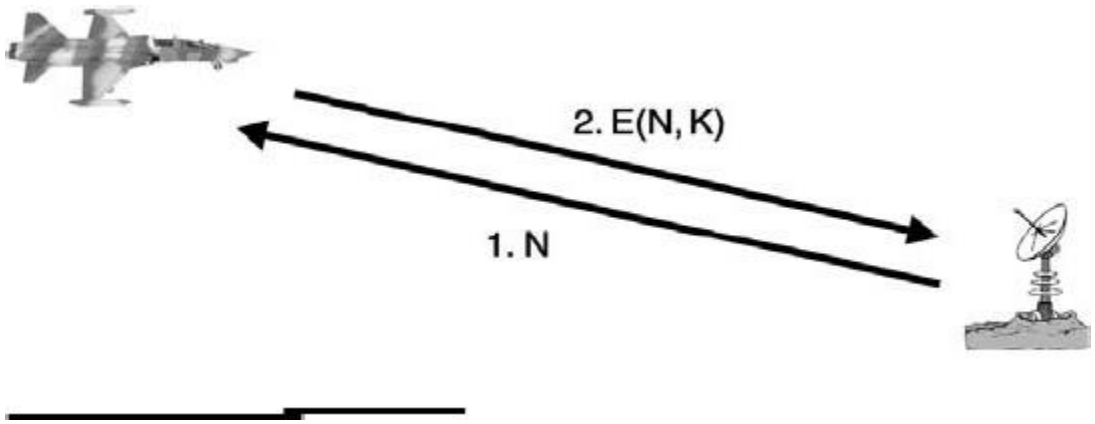
- Најпознатите сериозни безбедносни предизвици
  - протоколите се користат во средини за кои тие не беа првично наменети
- Безбедносните протоколи мора да работат
  - без разлика што напаѓачот активно се обидува да ги пробие и
  - без разлика што околината во која работи се менува

# Едноставни безбедносни протоколи

- Примери:
  - влез во обезбедена зграда
    - Внеси картичка во читач
    - Внеси PIN
    - Дали PIN-от е во ред?
      - Да – дозволен влез
      - Не – недозволен влез
  - подигнување пари од банкомат
    - слично на влез во обезбедена зграда

# Едноставни безбедносни протоколи

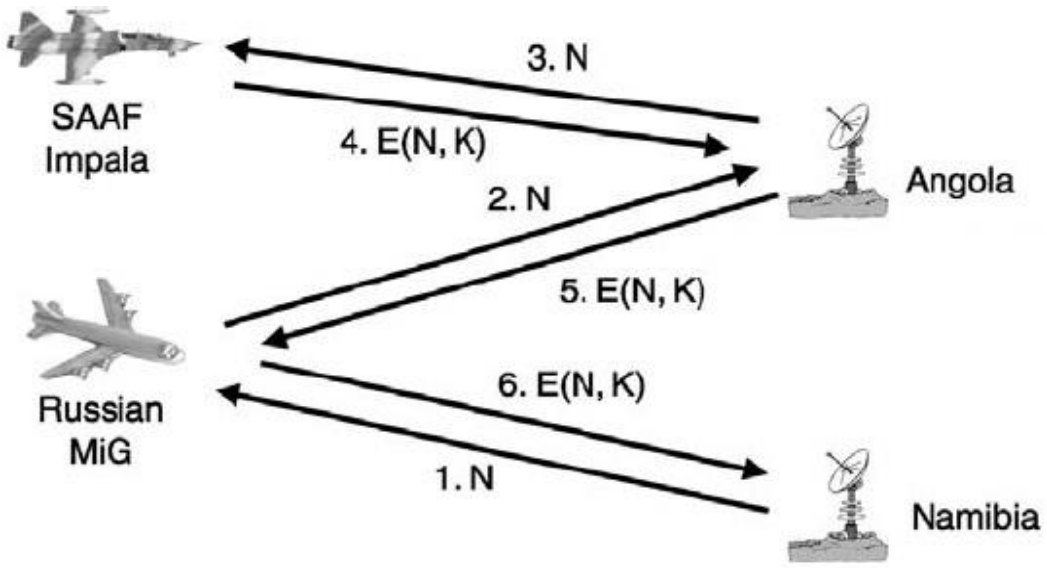
- Безбедносен протокол во војска
  - дизајниран да спречи “пријателски инциденти”




Идентификување на пријател или непријател

# Едноставни безбедносни протоколи

- Слабост на протоколот




MiG in the Middle

# Автентикациски протоколи

- Взаемна автентикација:
  - Боб да го провери идентитетот на Алис и
  - Алис да го провери идентитетот на Боб
    - користејќи автентикациски протокол најчесто со симетричен клуч кој генерално се користи како сесиски клуч, кој е клуч за доверливост или заштита на интегритетот (или двете) за тековната сесија
- Безбедносниот протокол може да има други барања
  - протоколот да користи јавни клучеви или хаш функции
  - во некои ситуации може да се бара приватност и анонимност или веродостојно спречување

# Автентикациски протоколи

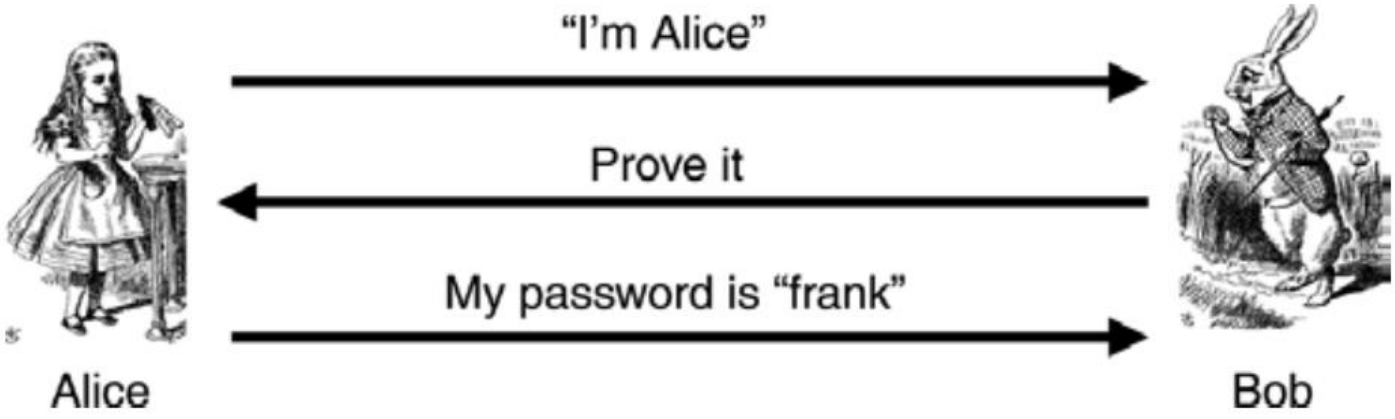
- Автентикацијата кај самостојни компјутерски систем е јасна и едноставна
- Автентикација на мрежа бара многу внимание при креирање на протоколот
  - Напаѓачот, Trudy, може пасивно да ги следи и чита пораките, да ги препраќа пораките, но, може активно да напаѓа, да додава информации, да брише или да ги менува пораките

# Автентикациски протоколи

- Видови автентикациски протоколи:
  - Едноставна автентикација (Simple authentication)
  - Едноставна автетикација со хаш (Simple authentication with a hash)
  - Генерички автентикациски протокол (Generic authentication protocol)
  - Предизвик-одговор автентикација (Challenge-response)

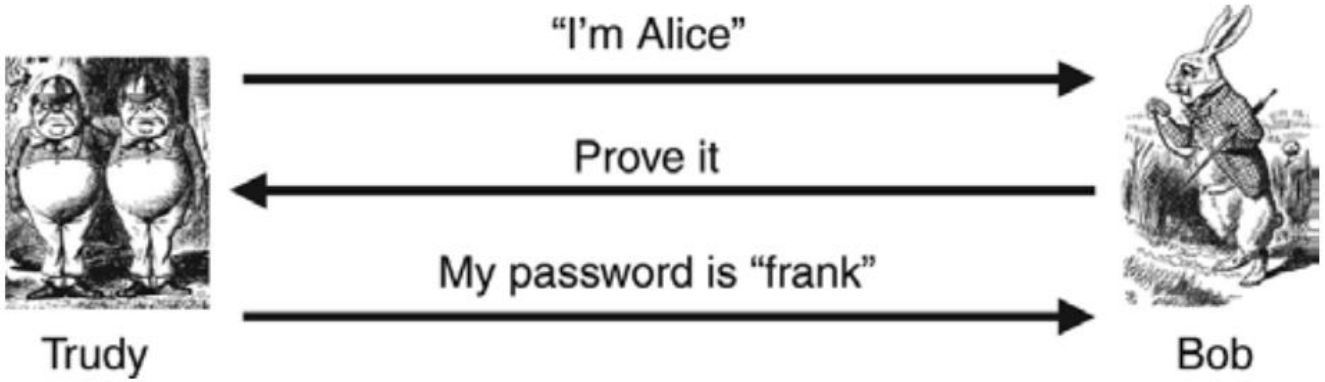
# Автентикациски протоколи

- Едноставен автентикациски протокол
  - нема взаемна автентикација



# Автентикациски протоколи

- Недостатоци на протоколот
  - ако Труди може пасивно да ги набљудува пораките кои се праќаат, таа подоцна може да ги препрати пораките за да го убеди Боб дека таа е Алис

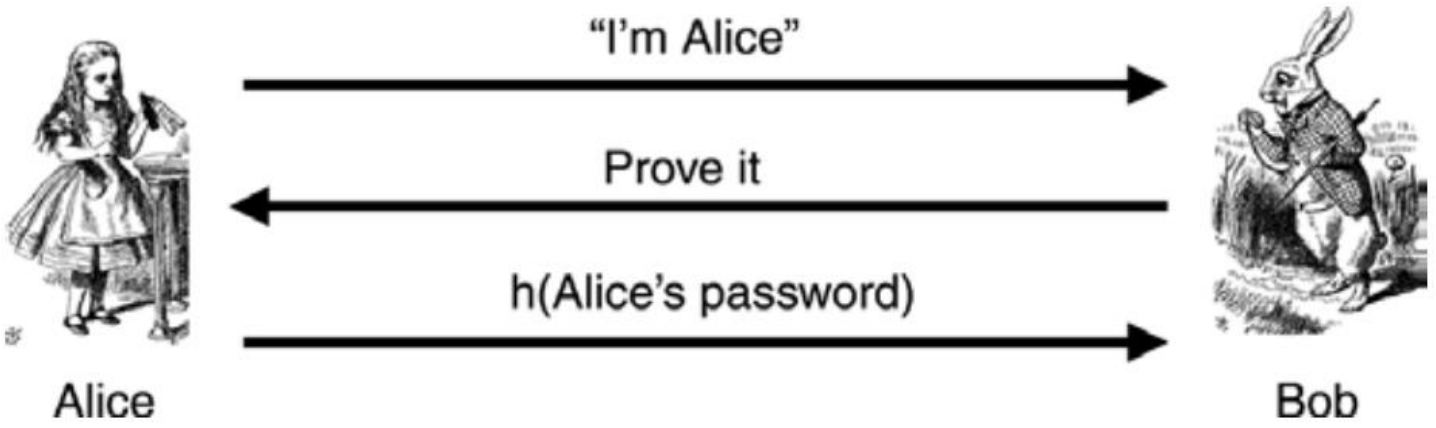


# Автентикациски протоколи

- Недостатоци на протоколот
  - Алис ја праќа лозинката незаштитена
    - ако Труди пасивно ја набљудува набљудува лозинката на Алис, таа може да се претстави како Алис на сите места каде што Алис ја користи лозинката “frank”
  - Боб треба да ја знае лозинката на Алис, со цел да ја идентификува
  - неефикасен, бидејќи истиот ефект може да се постигне со една порака од Алис до Боб
  - не обезбедува меѓусебна идентификација

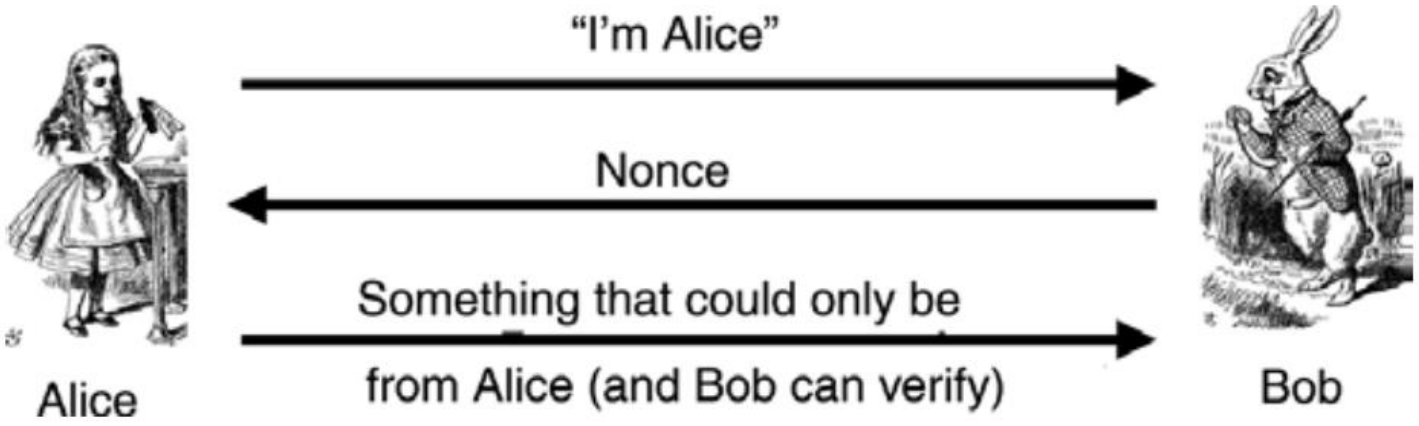
# Автентикациски протоколи

- Автентикациски протокол со хаш
  - Недостатоци на протоколот
    - Труди повторно може пасивно да ги набљудува пораките кои се праќаат, и подоцна да ги препрати пораките за да го убеди Боб дека таа е Алис



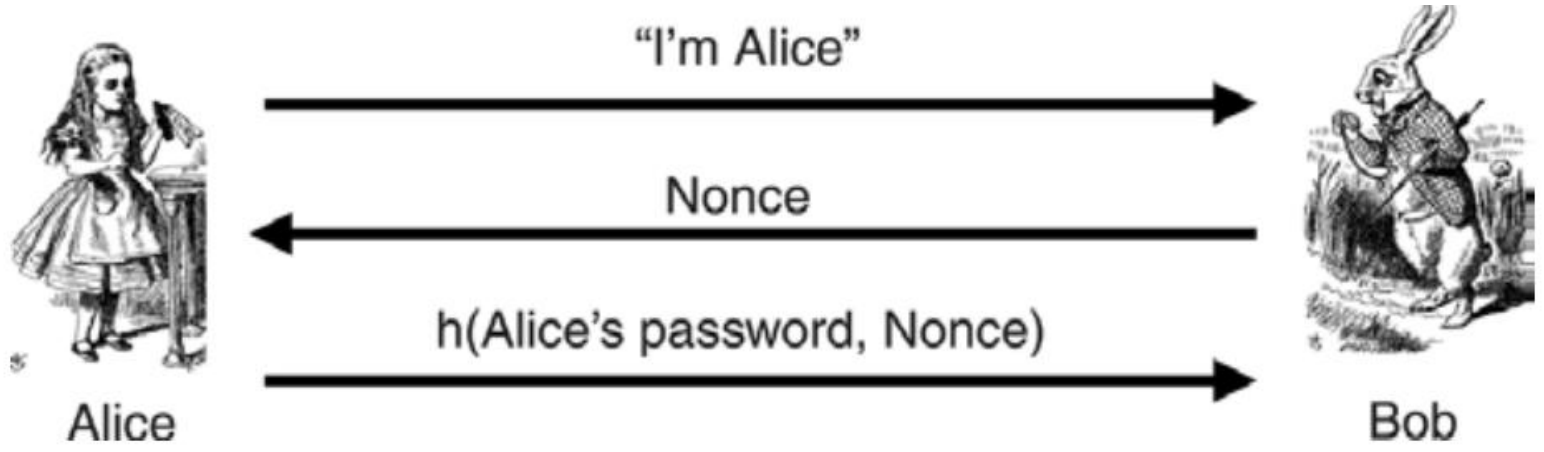
# Автентикациски протоколи

- Генерички автентикациски протокол
  - Спречува напад со препраќање



# Автентикациски протоколи

- Предизвик-одговор автентикациски протокол
  - Отпорен на нападот со препраќање
  - Недостаток
    - Боб мора да ја знае лозинката на Алис



# Автентикација со користење симетричен клуч

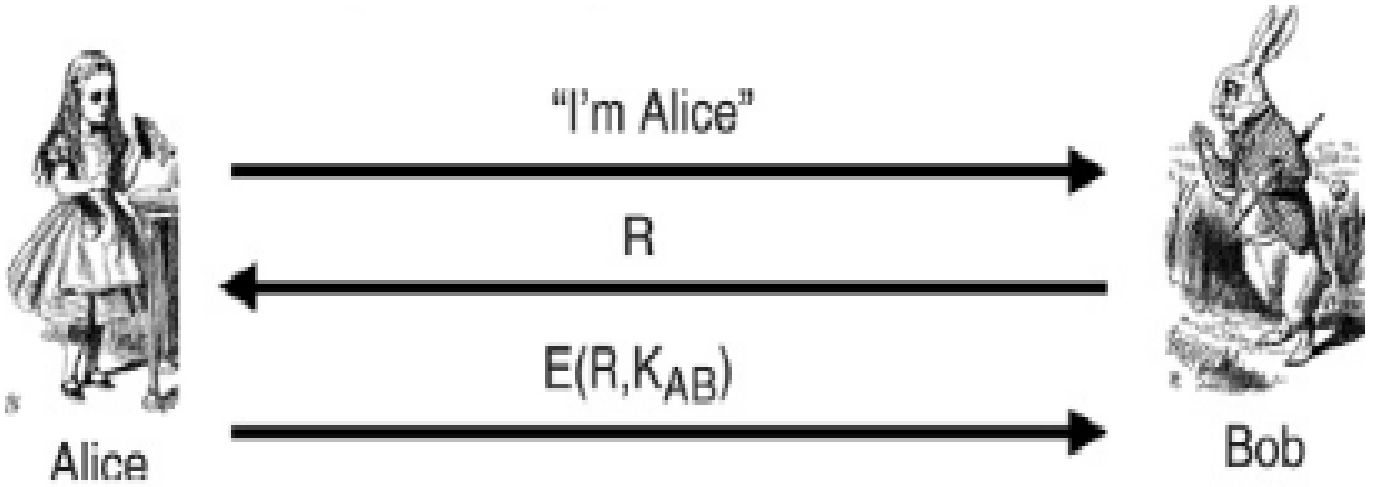
- Alice и Bob користат симетричен клуч $\mathbf{K_{AB}}$
- Автентикацијата ќе биде извршена знаејќи го овај симетричен клуч
- Во процесот на автентикација
  - клучот $\mathbf{K_{AB}}$ не треба да и биде познат на Trudy
  - мора да бидеме заштитени од напад со препраќање

# Автентикација со користење симетричен клуч

- Автентикацискиот проткол со симетричен клуч е аналоген на challenge-response protocol
- Наместо  хаширање на nonce со лозинка се врши шифрирање на nonce **R** со клучот $\mathbf{K_{AB}}$.

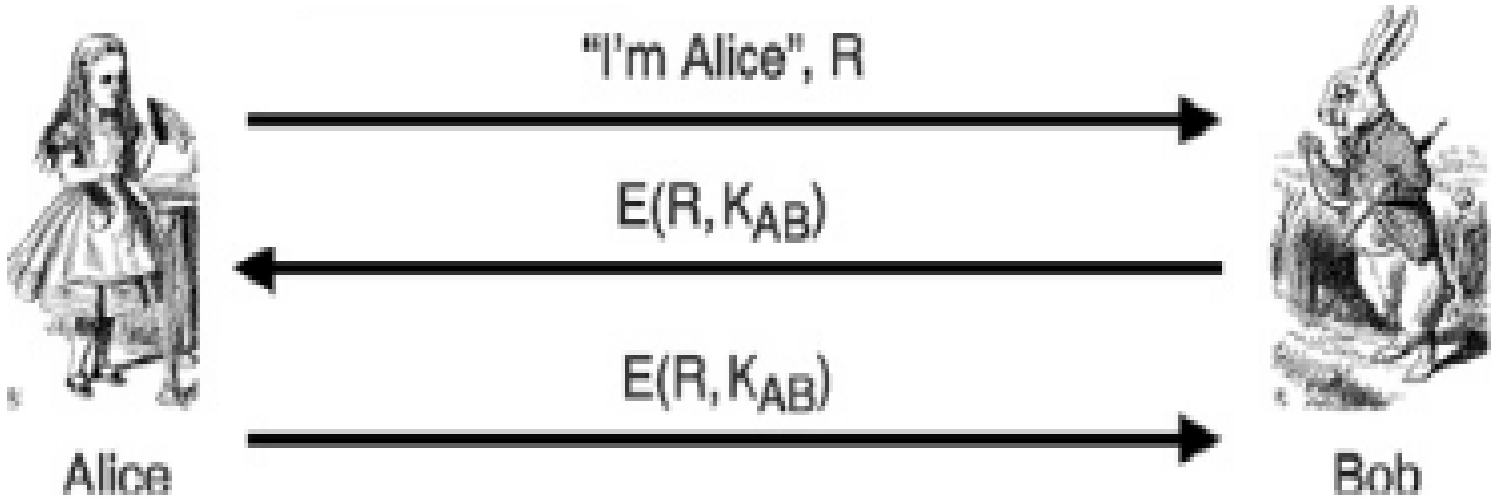
# Автентикација со користење симетричен клуч

- Автентикацискиот протокол му дозволува на Bob да ја автентицира Alice и да спречи напад со препраќање
- Протоколот нема взаемна автентикација



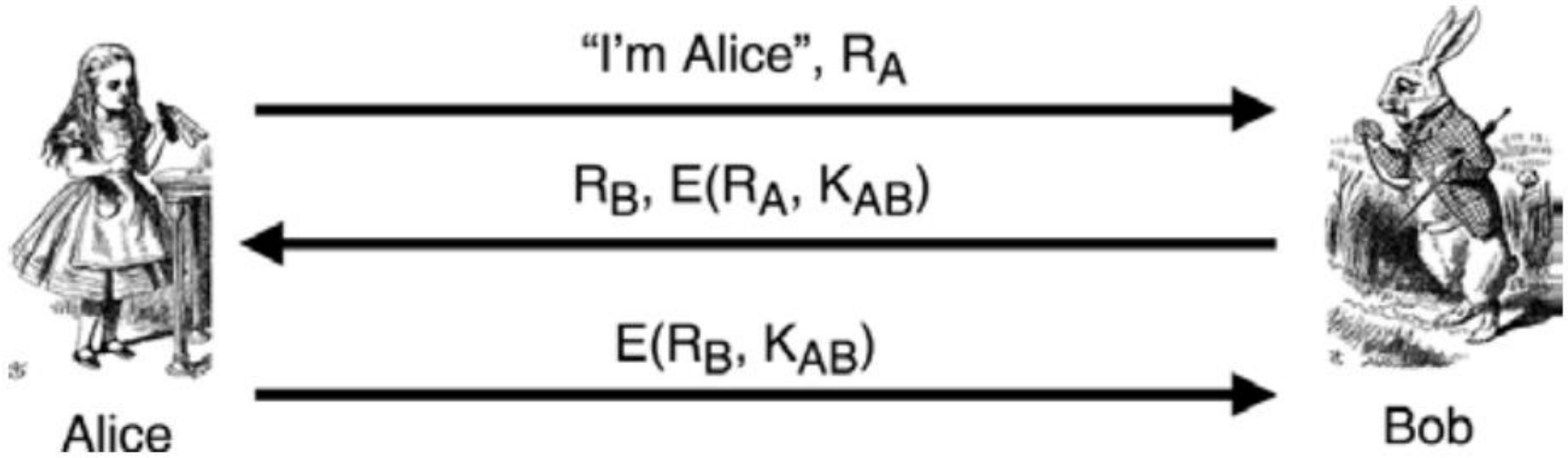
# Автентикација со користење симетричен клуч

- Взаемна автентикација?
- Овој проткотол е ефикасен
- Користи симетричен клуч, но тоа е недостаток.



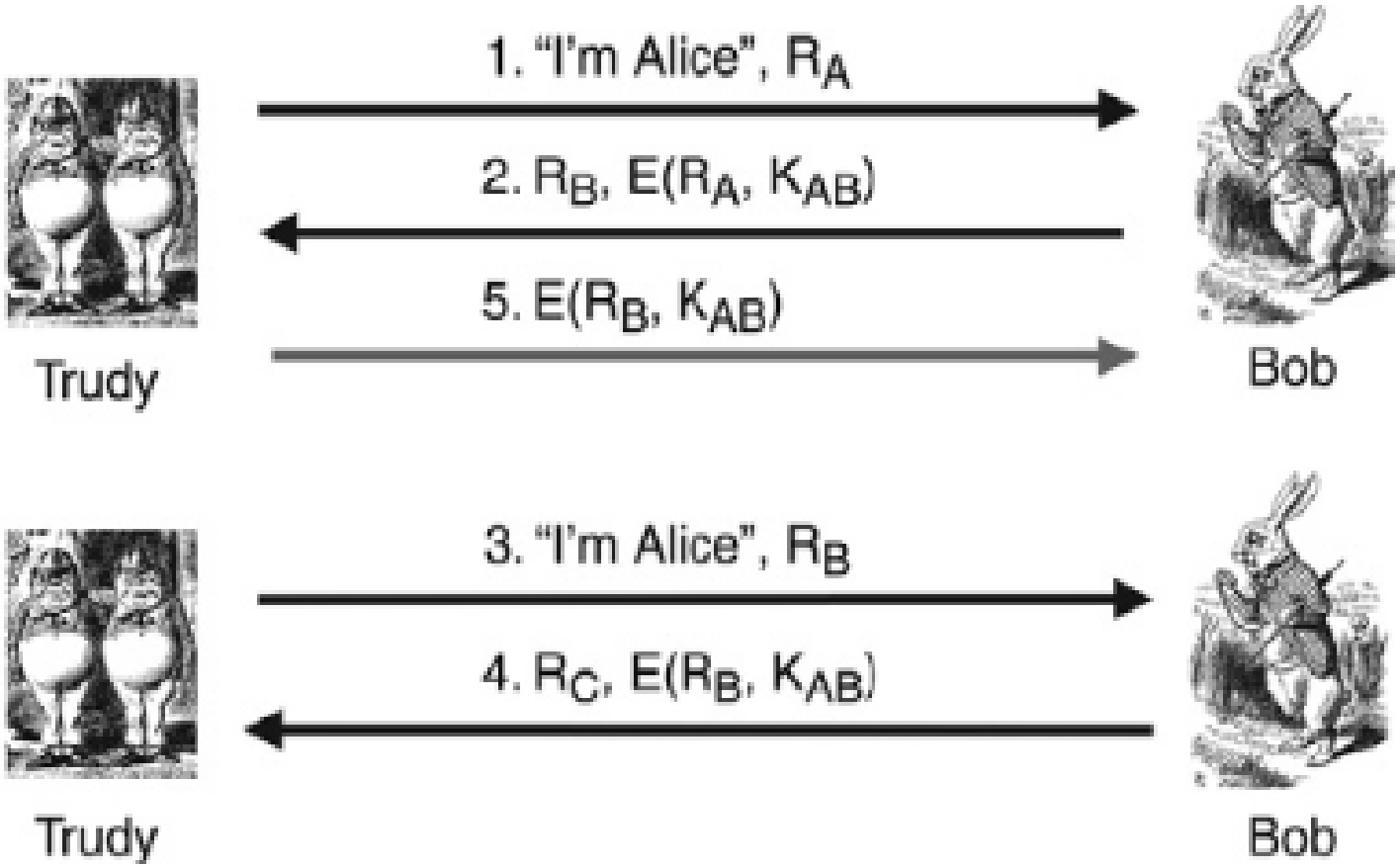
# Автентикација со користење симетричен клуч

- Безбедна взаемна автентикација?



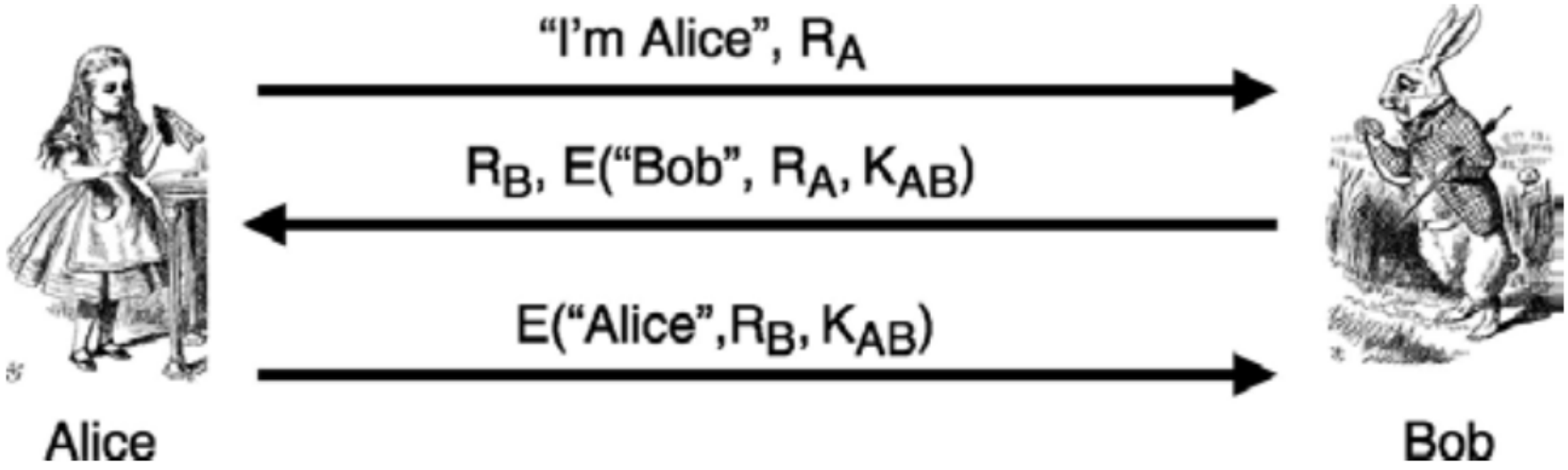
# Автентикација со користење симетричен клуч

- Напад: Man-in-the –middle



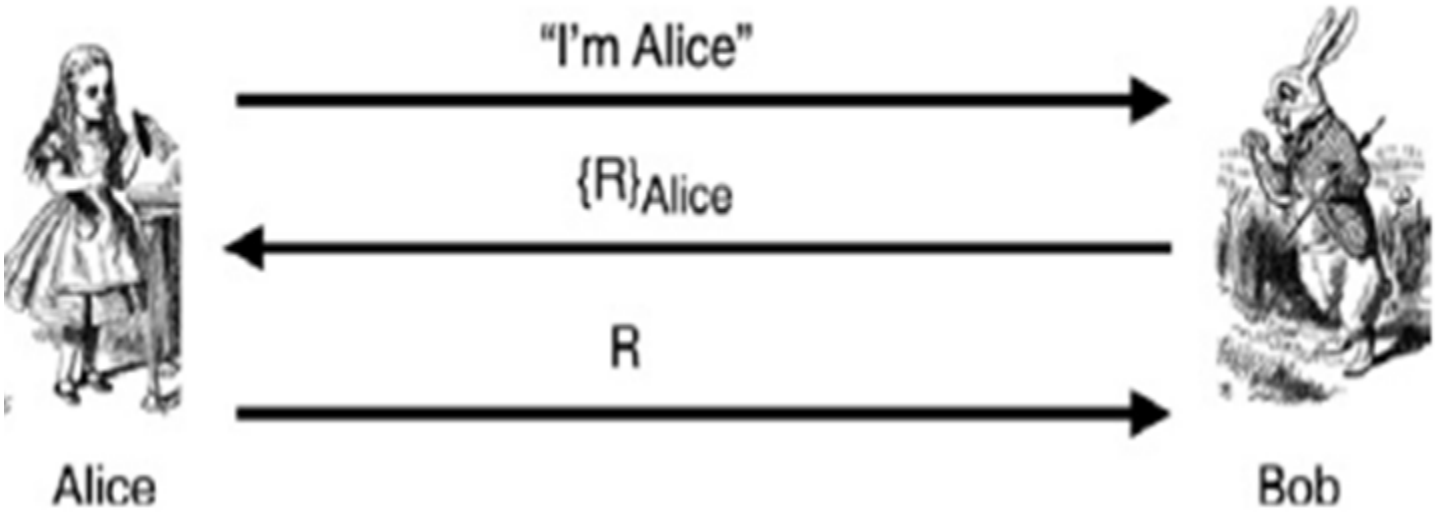
# Автентикација со користење симетричен клуч

- Подобра взаемна автентикација



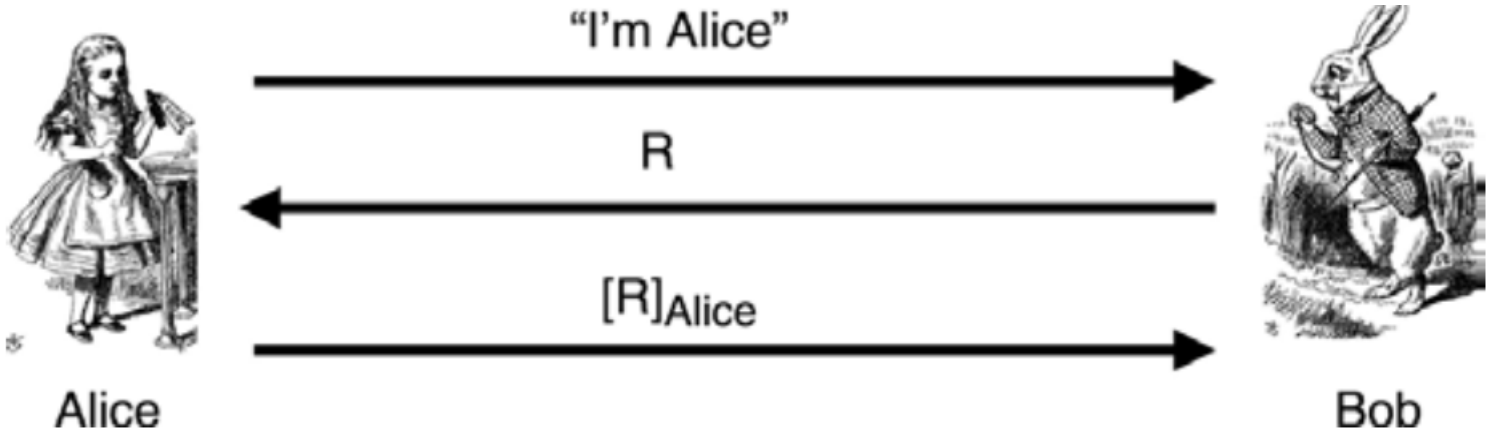
# Автентикација со користење јавни клучеви

- Bob ја автентицира Alice поради тоа што
  - само Alice може да ја пресмета операцијата на приватниот клуч што е потребна за да ја врати пораката **R**



# Автентикација со користење јавни клучеви

- Автентикација со дигитален потпис



# Автентикација со користење јавни клучеви

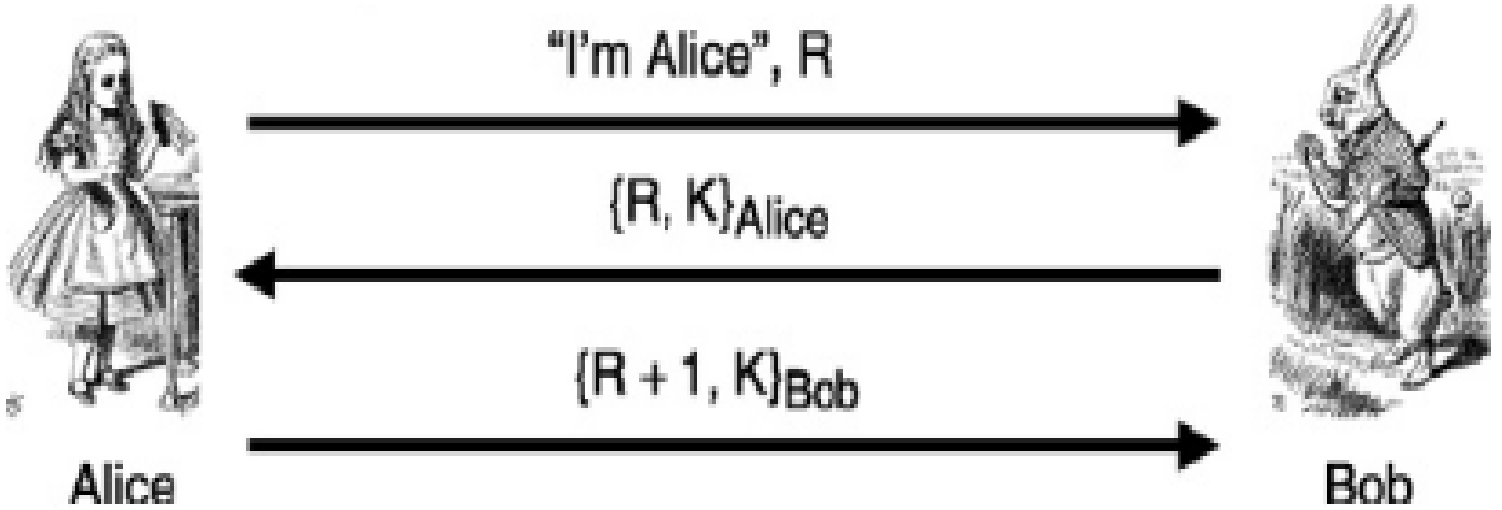
- Ако Alice го користи истиот пар клучеви за шифрирање и за автентикација, тогаш во протоколот може да се појави проблем
  - Да претпоставиме дека Trudy ја пресретнала пораката која е шифрирана со јавниот клуч на Alice, тогаш Trudy може да се преправа дека е Bob и да испрати порака до Alice и Alice ќе ја дешифрира и ќе ја испрати назад на Trudy
- Решение на овој проблем е секогаш да се користи различен пар клучеви за шифрирање и потпишување.

# Сесиски клучеви

- Често користени, дури и при користење на симетричен клуч за автентикација
- Се користат одделни клучеви за секоја сесија
- Сесиските клучеви се користат за целосна или делумна заштита

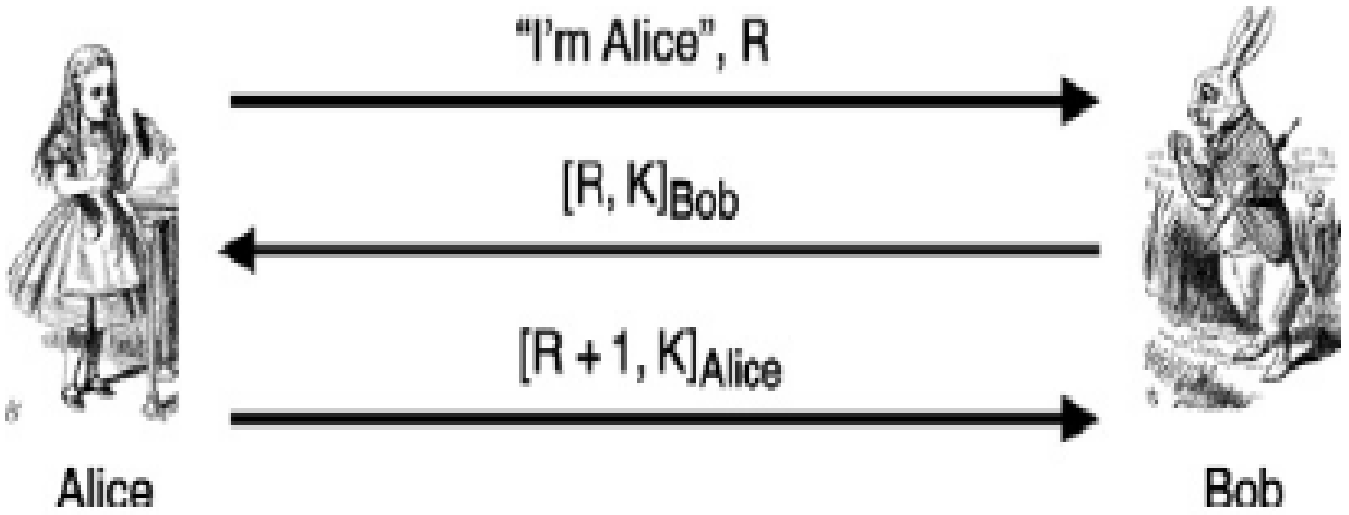
# Сесиски клучеви

- Автентикација и сесиски клуч
  - Нема взаемна автентикација



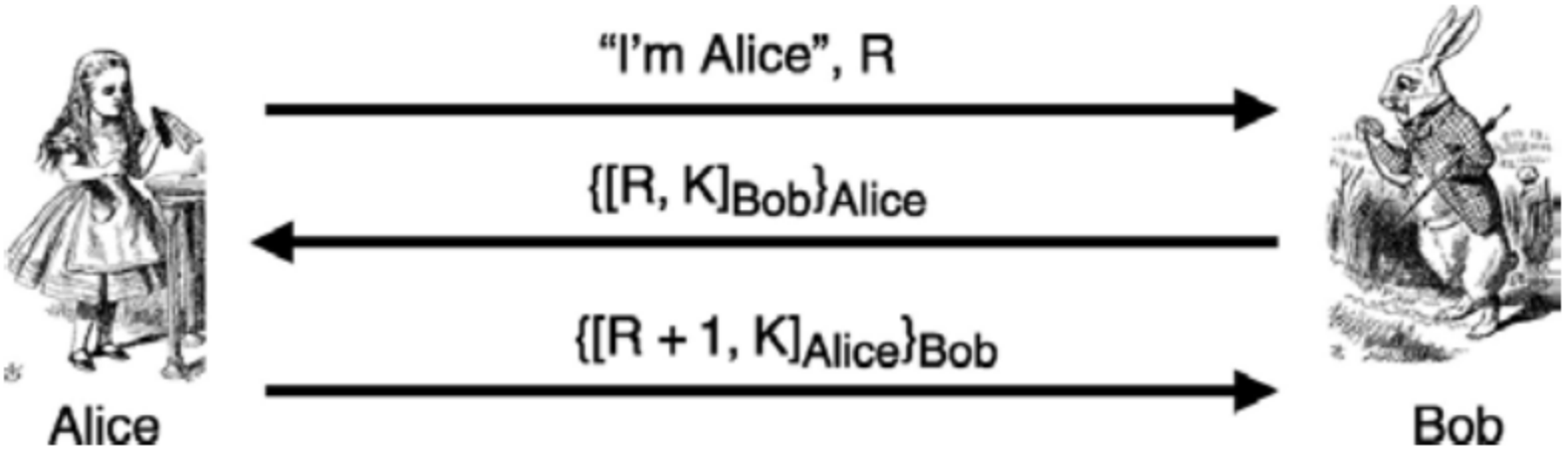
# Сесиски клучеви

- Потпис базирана автентикација и сесиски клуч
  - Недостаток:
    - Откако клучот е потпишан, секој може да го користи јавниот клуч на Bob (или на Alice ) и со тоа да го најде сесискиот клуч **K**
  - овозможува взаемна автентикација



# Сесиски клучеви

- Взаемна автентикација и сесиски клуч



# Сесиски клучеви

- Взаемна автентикација и сесиски клуч