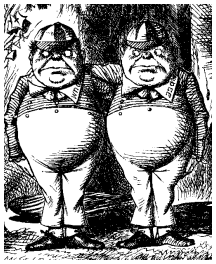
Nov 8
Simple Security Protocols continued

Part 3 ≥E Protocols

Mutual Authentication Attack



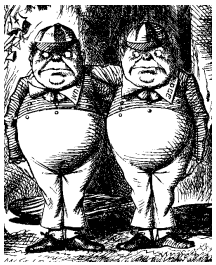
Trudy

1. "I'm Alice", R_A

2. R_B, $E(R_A,K_{AB})$

5. $E(R_B,K_{AB})$

Bob



Trudy

3. "I'm Alice", R_B

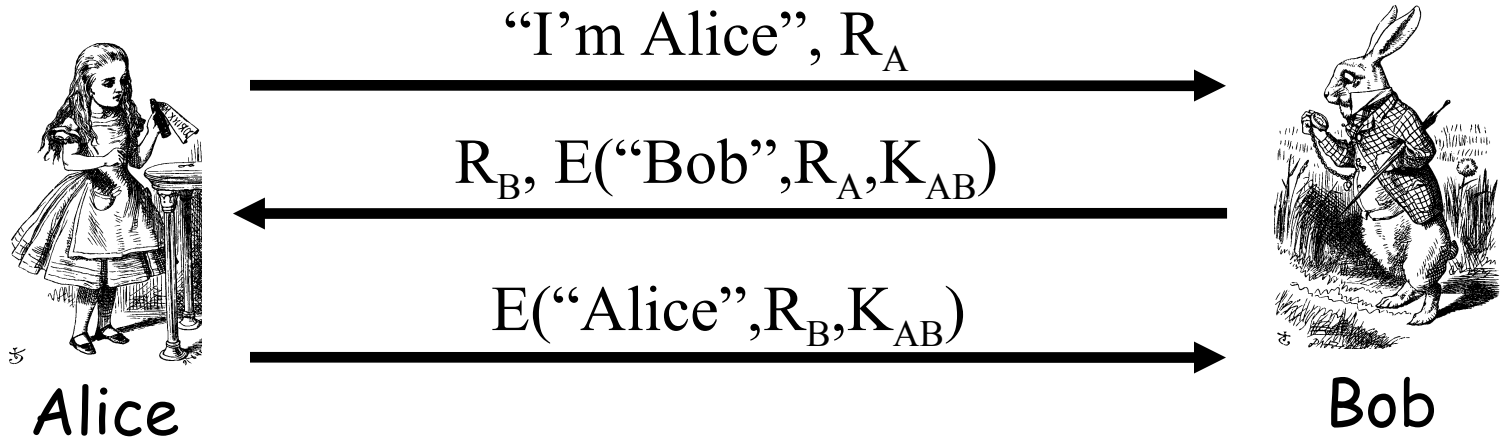
4. R_C, $E(R_B,K_{AB})$

Bob

Mutual Authentication

- Our one-way authentication protocol **not** secure for mutual authentication
- Protocols are subtle!
- The "obvious" thing may not be secure
- Also, if assumptions or environment changes, protocol may not work
  - This is a common source of security failure
  - For example, Internet protocols

Symmetric Key Mutual Authentication

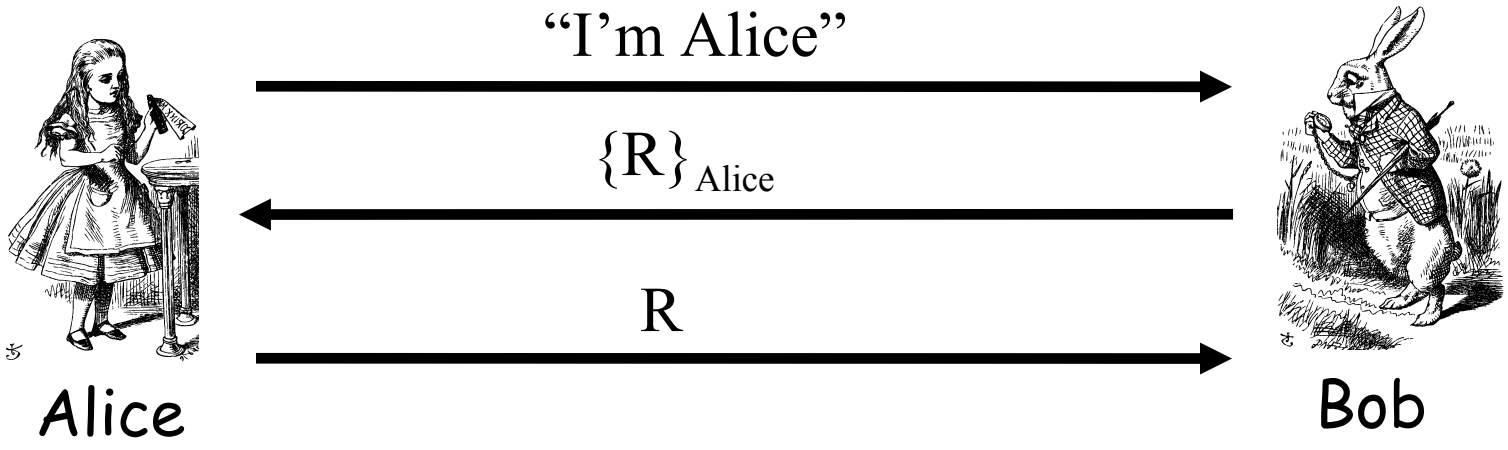


- Do these "insignificant" changes help?
- Yes!

Public Key Notation

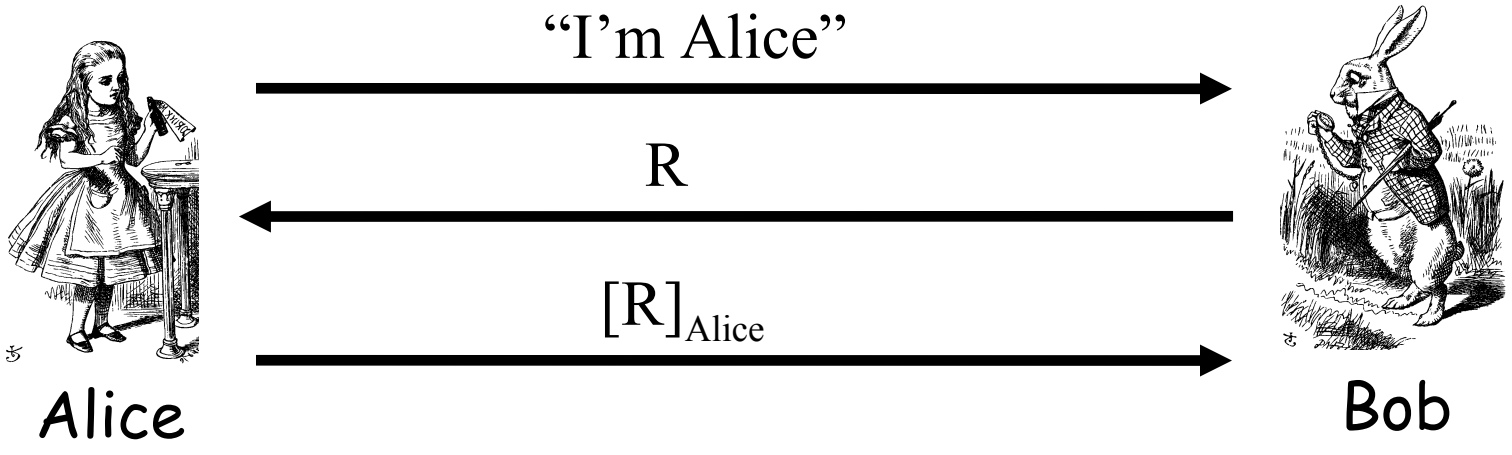
- Encrypt M with Alice's public key: $\{M\}_{Alice}$
- Sign M with Alice's private key: $[M]_{Alice}$
- Then
  - $[\{M\}_{Alice}]_{Alice} = M$
  - $\{[M]_{Alice}\}_{Alice} = M$
- **Anybody** can do **public key** operations
- Only **Alice** can use her **private key** (sign)

Public Key Authentication via Encryption



- Is Alice authenticated? Bob? Is this secure?
- Trudy can get Alice to decrypt anything! (how?)
  - Must have two key pairs (one for signature and one for encryption)

Public Key Authentication via Digital Signature



- Is this secure?
- Again ...Trudy can get Alice to sign (encrypt) anything!
  - Must have two key pairs

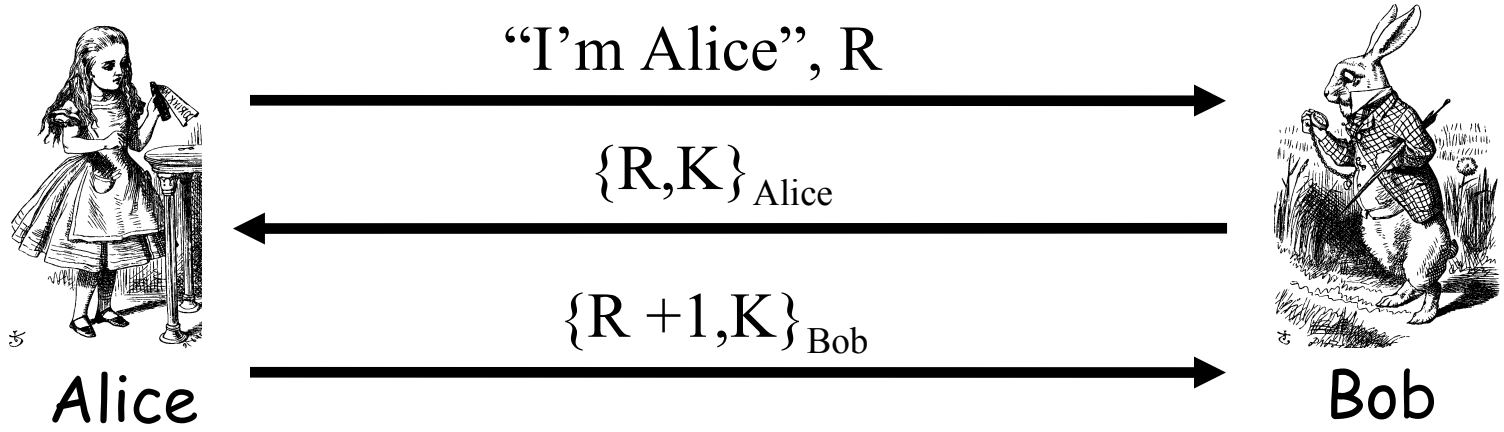
Public Keys

- Never use the same key pair for encryption and signing
- One key pair for encryption/decryption
- A different key pair for signing/verifying signatures

Session Key

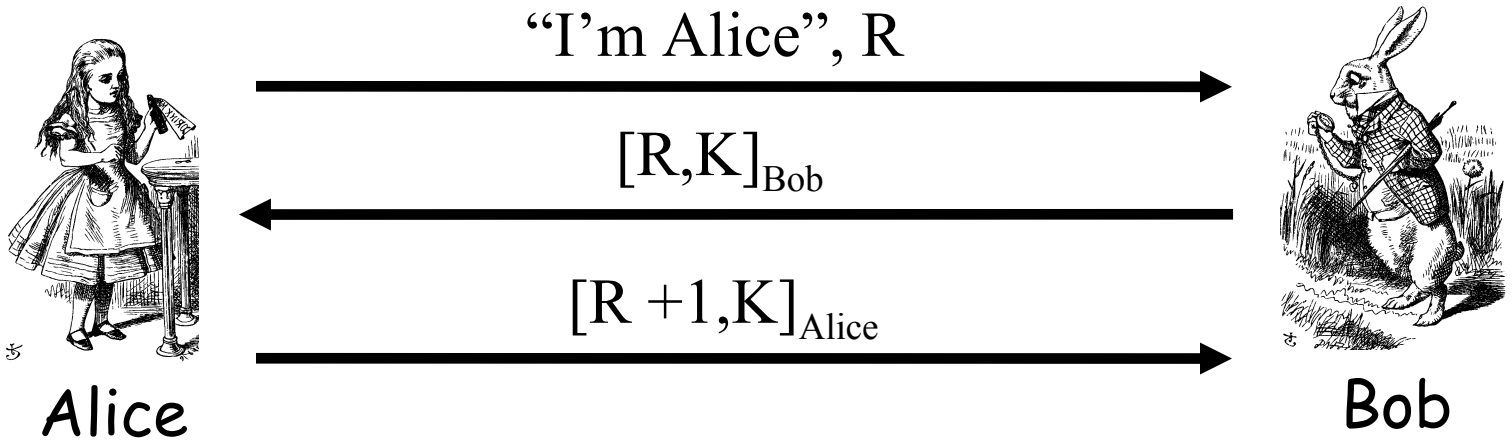
- Usually, a session key is required
  - Symmetric key for a particular session
- Can we authenticate and establish a shared symmetric key?
  - Key can be used for confidentiality
  - Key can be used for integrity
- In some cases, we may also require perfect forward secrecy (PFS)
  - Discussed later…

Authentication & Session Key



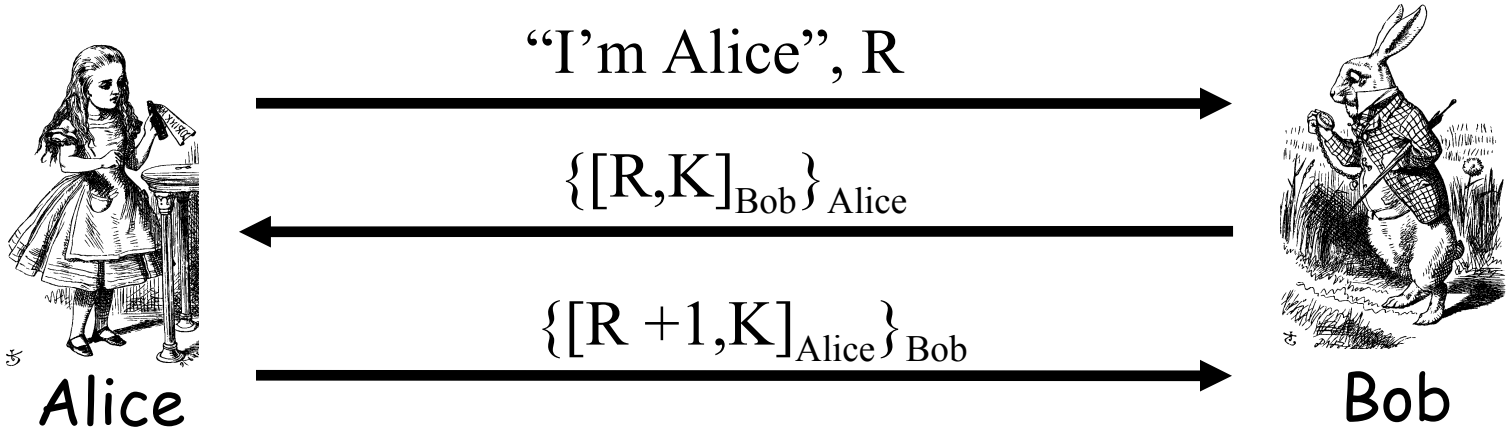
- Is this secure?
- OK for key, but no mutual authentication
- **Note** that K is acting as Bob's nonce

Public Key Authentication and Session Key



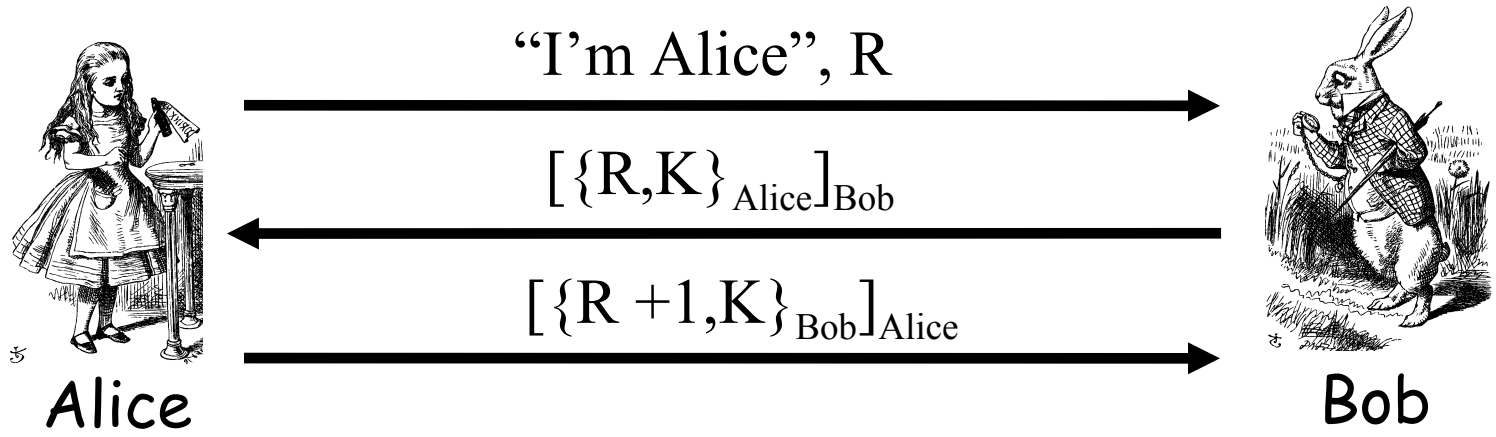
- Is this secure?
- Mutual authentication but key is not secret!

Public Key Authentication and Session Key



- Is this secure?
- Seems to be OK
- Mutual authentication and session key!

Public Key Authentication and Session Key



- Is this secure?
- Seems to be OK
  - Anyone can see $\{R,K\}_{Alice}$ and $\{R+1,K\}_{Bob}$

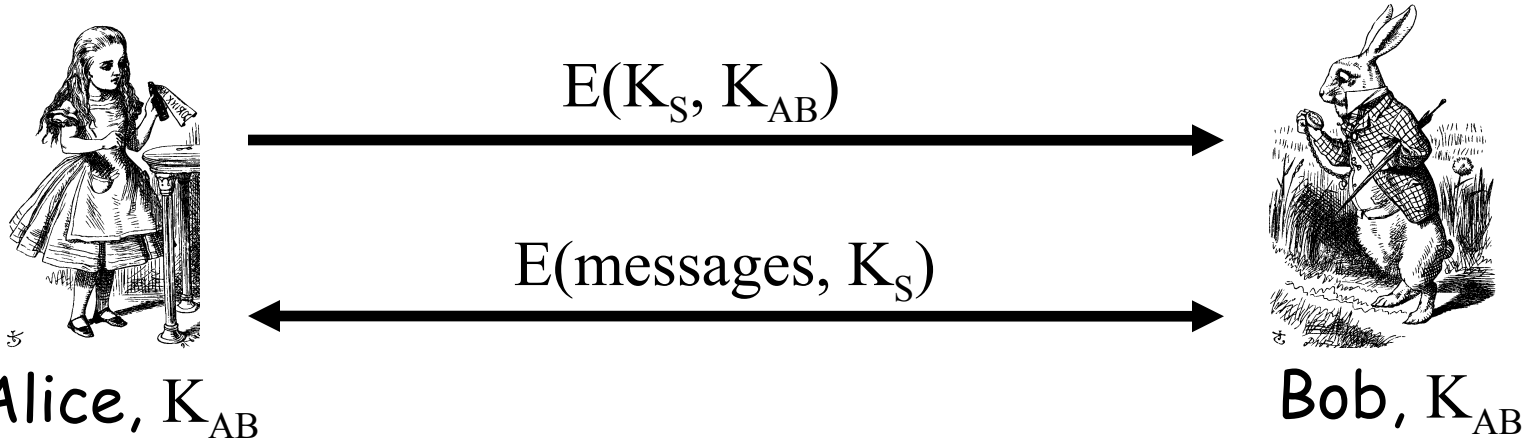
Perfect Forward Secrecy

- The concern…
  - Alice encrypts message with shared key K_{AB} and sends ciphertext to Bob
  - Trudy records ciphertext and later attacks Alice's (or Bob's) computer to find K_{AB}
  - Then Trudy decrypts recorded messages
- **Perfect forward secrecy (PFS):** Trudy cannot later decrypt recorded ciphertext
  - Even if Trudy gets key K_{AB} or other secret(s)
- Is PFS possible?

Perfect Forward Secrecy

- Suppose Alice and Bob share key K_{AB}
- For perfect forward secrecy, Alice and Bob cannot use K_{AB} to encrypt
- Instead they must use a **session key** K_S and forget it after it's used
- Problem: How can Alice and Bob agree on session key K_S and ensure PFS?

Naïve Session Key Protocol



- Trudy could also record $E(K_S, K_{AB})$
- If Trudy gets K_{AB}, she gets K_S