IPSec: IKE

- Readings
  - Chapter 18

IKE: Internet Key Exchange

- IKE has 2 phases
  - Phase 1 — IKE security association (SA)
  - Phase 2 — AH/ESP security association
- Phase 1 is comparable to SSL session
- Phase 2 is comparable to SSL connection
- Not an obvious need for two phases in IKE
- If multiple Phase 2's do not occur, then it is **more** expensive to have two phases!

IKE Phase 1

- Four different “key” options
  - Public key encryption (original version)
  - Public key encryption (improved version)
  - Public key signature
  - Pre-shared symmetric key
- For each of these, two different “modes”
  - Main mode (6 messages)
  - Aggressive mode (3 messages)
- **There are 8 versions of IKE Phase 1!**

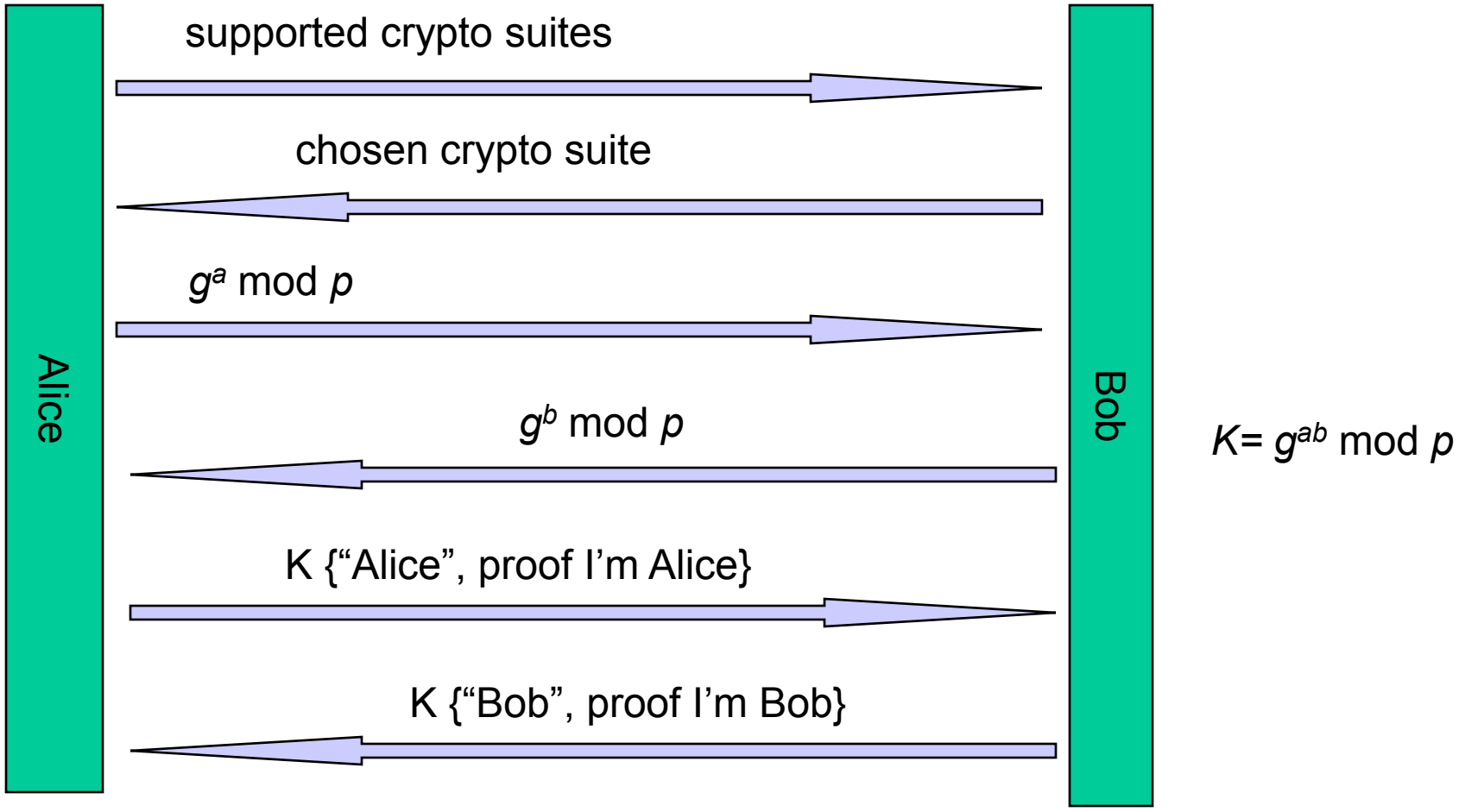
IKE Phase 1

- We'll discuss 6 of 8 phase 1 variants
  - Public key signatures (2 modes)
  - Symmetric key (2 modes)
  - Public key encryption (original version, 2 modes)
- Why public key encryption and public key signatures?
  - Always know your own private key
  - **May not** (initially) know other side's public key

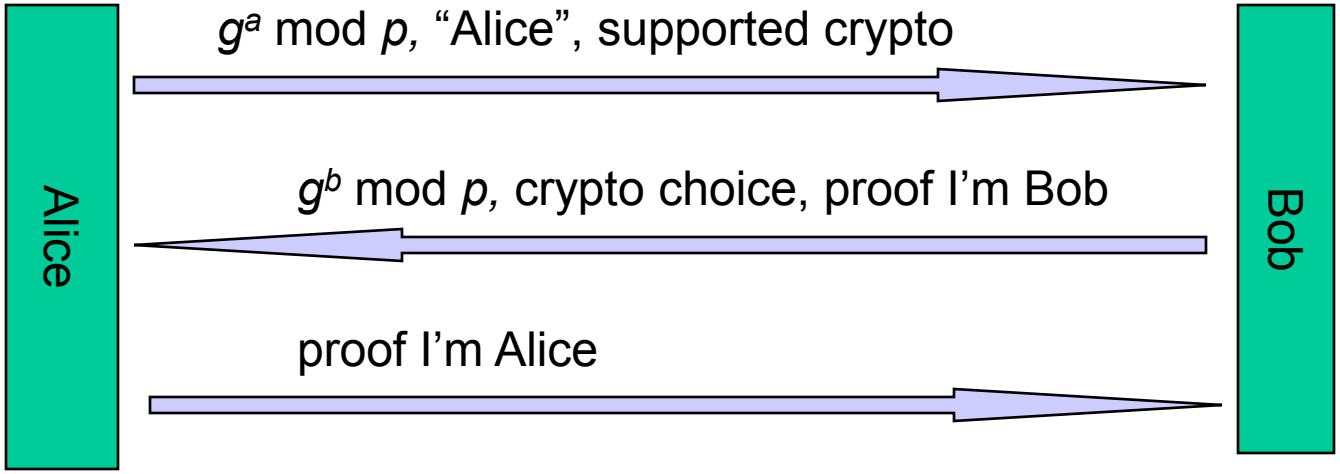
General Idea of IKE Phase 1

- Uses ephemeral Diffie-Hellman to establish session key
  - Achieves perfect forward secrecy (PFS)
- Let a be Alice's Diffie-Hellman exponent
- Let b be Bob's Diffie-Hellman exponent
- Let g be generator and p prime
- Recall p and g are public

General Idea of IKE Phase 1: Main Mode



General Idea of IKE Phase 1: Aggressive Mode



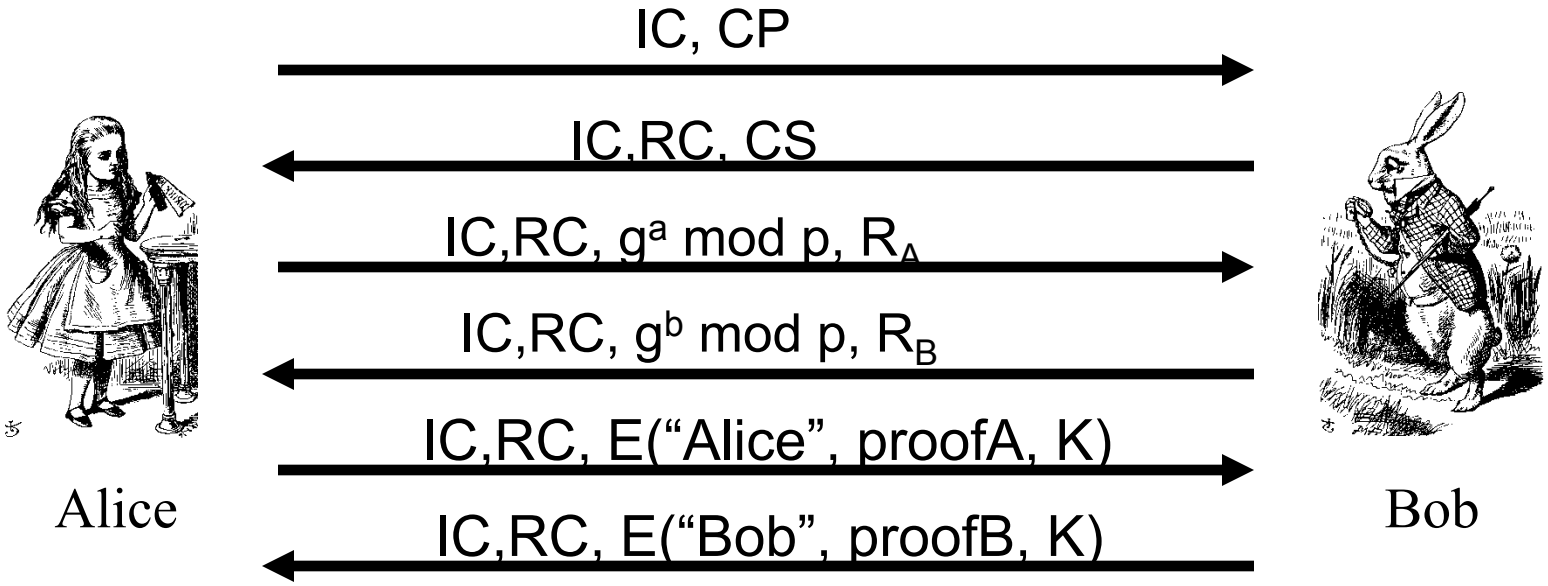
In aggressive mode, Alice chooses some DH context *(p, g)* and sends that in the first message exchange.
Bob may not support it, and reject the connection. If that happens, Alice should try and connect to Bob using main mode.

Aggressive mode provides mutual authentication, and a shared secret g^{ab} mod p, which can be used to derive keys for the symmetric crypto protocols.

Main vs Aggressive Modes

- Main mode **MUST** be implemented
  - Trying to protect identities
  - Crypto including DH parameters can be negotiated
- Aggressive mode **SHOULD** be implemented
  - In other words, if aggressive mode is not implemented, “you should feel guilty about it”
- Might create interoperability issues

IKE Phase 1: Digital Signature (Main Mode)



- IC = initiator "cookie", RC = responder "cookie"
- CP = crypto proposed, CS = crypto selected
- K = h(IC,RC,g^{ab} mod p,R_A,R_B)
- SKEYID = h(R_A, R_B, g^{ab} mod p)
- $proof_A$ = [h(SKEYID,g^a,g^b,IC,RC,CP,"Alice")]$_{Alice}$

IKE Phase 1: Public Key Signature (Aggressive Mode)

IC, “Alice”, g^a mod p, R_A, CP

IC,RC, “Bob”, R_B,
g^b mod p, CS, proofB

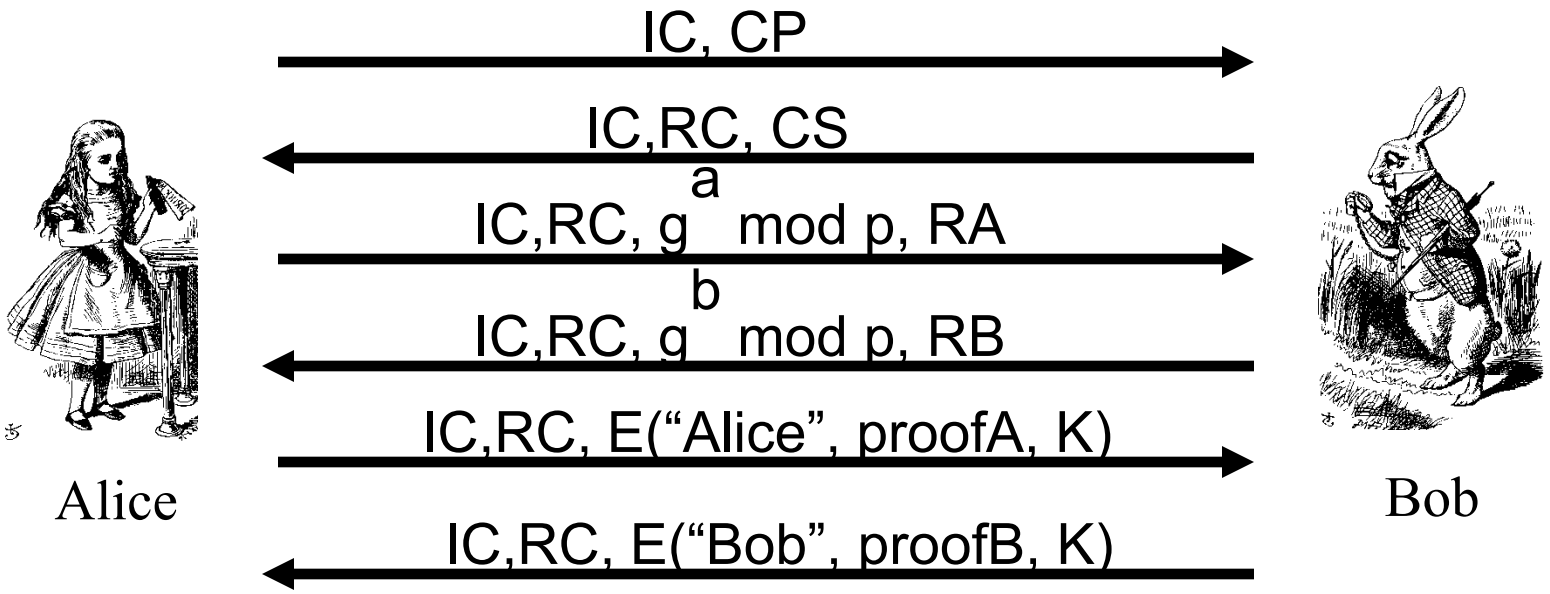
IC,RC, proofA

Alice

Bob

- Main difference from main mode
  - Not trying to protect identities
  - Cannot negotiate g or p

IKE Phase 1: Symmetric Key (Main Mode)

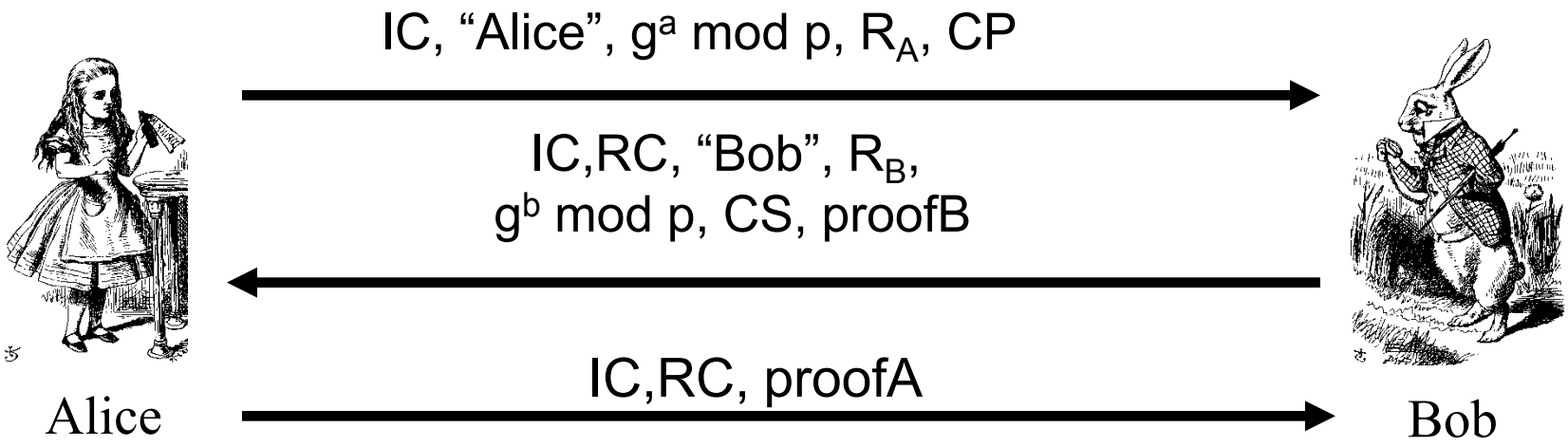


- Same as signature mode except
  - K_{AB} = symmetric key shared in advance
  - $K = h(IC,RC,g^{ab} \bmod p, R_A, R_B, K_{AB})$
  - $SKEYID = h(K, g^{ab} \bmod p)$
  - $proof_A = h(SKEYID, g^a, g^b, IC, RC, CP, \text{“Alice”})$

Problems with Symmetric Key (Main Mode)

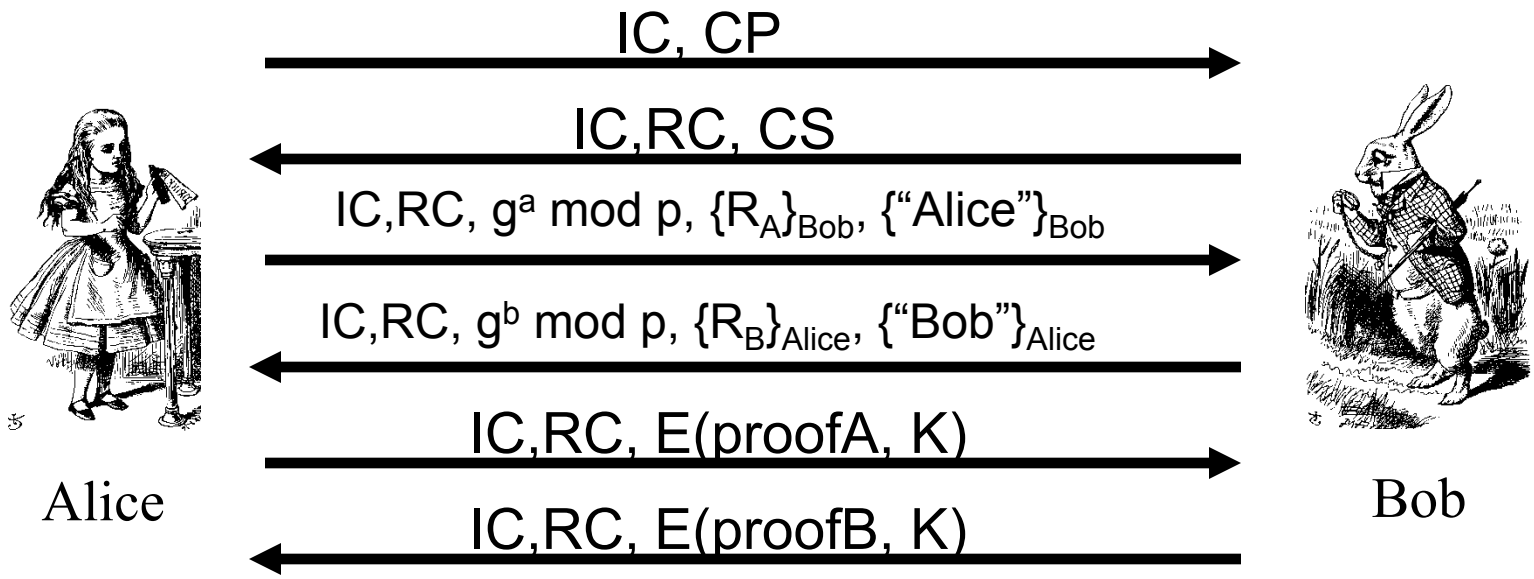
- Catch-22
  - Alice sends her ID in message 5
  - Alice's ID encrypted with K
  - To find K Bob must know K_{AB}
  - To get K_{AB} Bob must know he's talking to Alice!
- Result: **Alice's ID must be IP address!**
- Useless mode for the "road warrior"
- Why go to all of the trouble of trying to hide identities in 6 message protocol?

IKE Phase 1: Symmetric Key (Aggressive Mode)



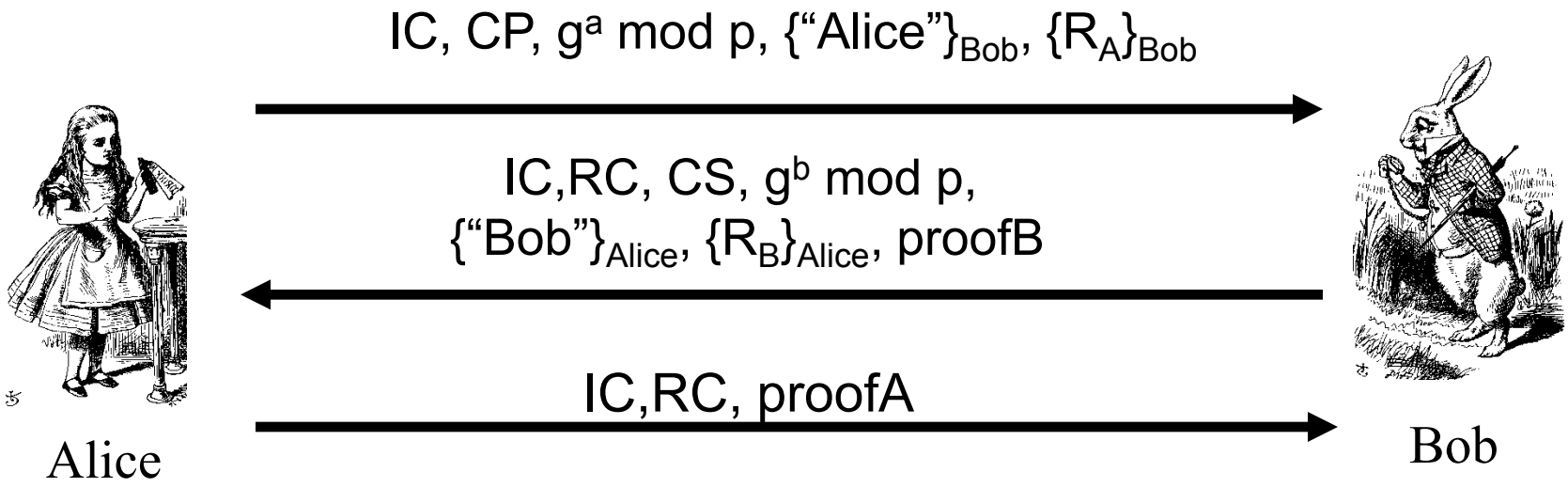
- Same format as digital signature aggressive mode
- Not trying to hide identities…
- As a result, does **not** have problems of main mode
- But does not (pretend to) hide identities

IKE Phase 1: Public Key Encryption (Main Mode)



- CP = crypto proposed, CS = crypto selected
- IC = initiator “cookie”, RC = responder “cookie”
- K = h(IC,RC,g^{ab} mod p,R_A,R_B)
- SKEYID = h(R_A, R_B, g^{ab} mod p)
- $proof_A$ = h(SKEYID,g^a,g^b,IC,RC,CP,“Alice”)

IKE Phase 1: Public Key Encryption (Aggressive Mode)



- K, $proof_A$, $proof_B$ computed as in main mode
- Note that identities are hidden
  - The only aggressive mode to hide identities
  - Then why have main mode?

Public Key Encryption Issue?

- Public key encryption, aggressive mode
- Suppose **Trudy** generates
  - Exponents **a** and **b**
  - Nonces $\mathbf{R_A}$ and $\mathbf{R_B}$
- Trudy can compute "valid" keys and proofs: $\mathbf{g^{ab}\ mod\ p}$, **K**, **SKEYID**, $\mathbf{proof_A}$ and $\mathbf{proof_B}$
- Also true of main mode

Public Key Encryption Issue?

Trudy as Alice

IC, CP, g^a mod p, $\{\text{“Alice”}\}_{Bob}$, $\{R_A\}_{Bob}$

IC,RC, CS, g^b mod p,
$\{\text{“Bob”}\}_{Alice}$, $\{R_B\}_{Alice}$, proofB

IC,RC, proofA

Trudy as Bob

- Trudy can create exchange that appears to be between Alice and Bob
- Appears valid to any observer, **including Alice and Bob!**

Plausible Deniability

- Trudy can create “conversation” that appears to be between Alice and Bob
- Appears valid, even to Alice and Bob!
- A security failure?
- In this mode of IPSec, it is a feature
  - **Plausible deniability:** Alice and Bob can deny that any conversation took place!
- In some cases it might be a security failure
  - If Alice makes a purchase from Bob, she could later repudiate it (unless she had signed)

IKE Phase 1 Cookies

- Cookies (or “anti-clogging tokens”) supposed to make denial of service more difficult
- No relation to Web cookies
- To reduce DoS, Bob wants to remain stateless as long as possible
- But Bob must remember CP from message 1 (required for proof of identity in message 6)
- Bob must keep state from 1st message on!
- These cookies offer little DoS protection!

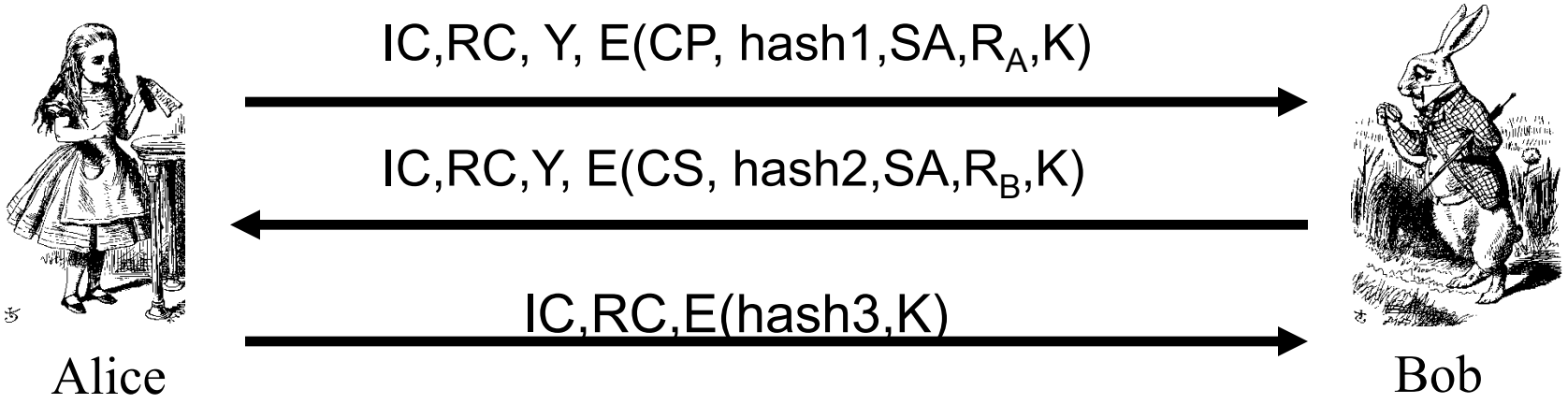
IKE Phase 1 Summary

- Result of IKE phase 1 is
  - Mutual authentication
  - Shared symmetric key
  - IKE **Security Association (SA)**
- But phase 1 is expensive (in public key and/or main mode cases)
- Developers of IKE thought it would be used for lots of things — not just IPSec
- Partly explains over-engineering…

IKE Phase 2 (AKA Quick Mode)

- Phase 1 establishes IKE SA
- Phase 2 establishes IPSec SA
- Comparison to SSL
  - SSL session is comparable to IKE Phase 1
  - SSL connections are like IKE Phase 2
- IKE **could** be used for lots of things
- But in practice, it's **not!**

IKE Phase 2



- Key K, IC, RC and SA known from Phase 1
- Proposal CP includes ESP and/or AH
- Hashes 1,2,3 depend on SKEYID, SA, R_A and R_B
- Keys derived from KEYMAT = h(SKEYID,R_A,R_B,protocol,SPI)
- Recall SKEYID depends on phase 1 key method
- Optional PFS (ephemeral Diffie-Hellman exchange)

IPSec

- After IKE Phase 1, we have an IKE SA
- After IKE Phase 2, we have an IPSec SA
- Both sides have a shared symmetric key
- We can now proceed IP datagram using ESP/AH

Reading Assignments

- Paper 15 (on phishing attacks)