IPsec: IKE (Internet Key Exchange)

Key Management

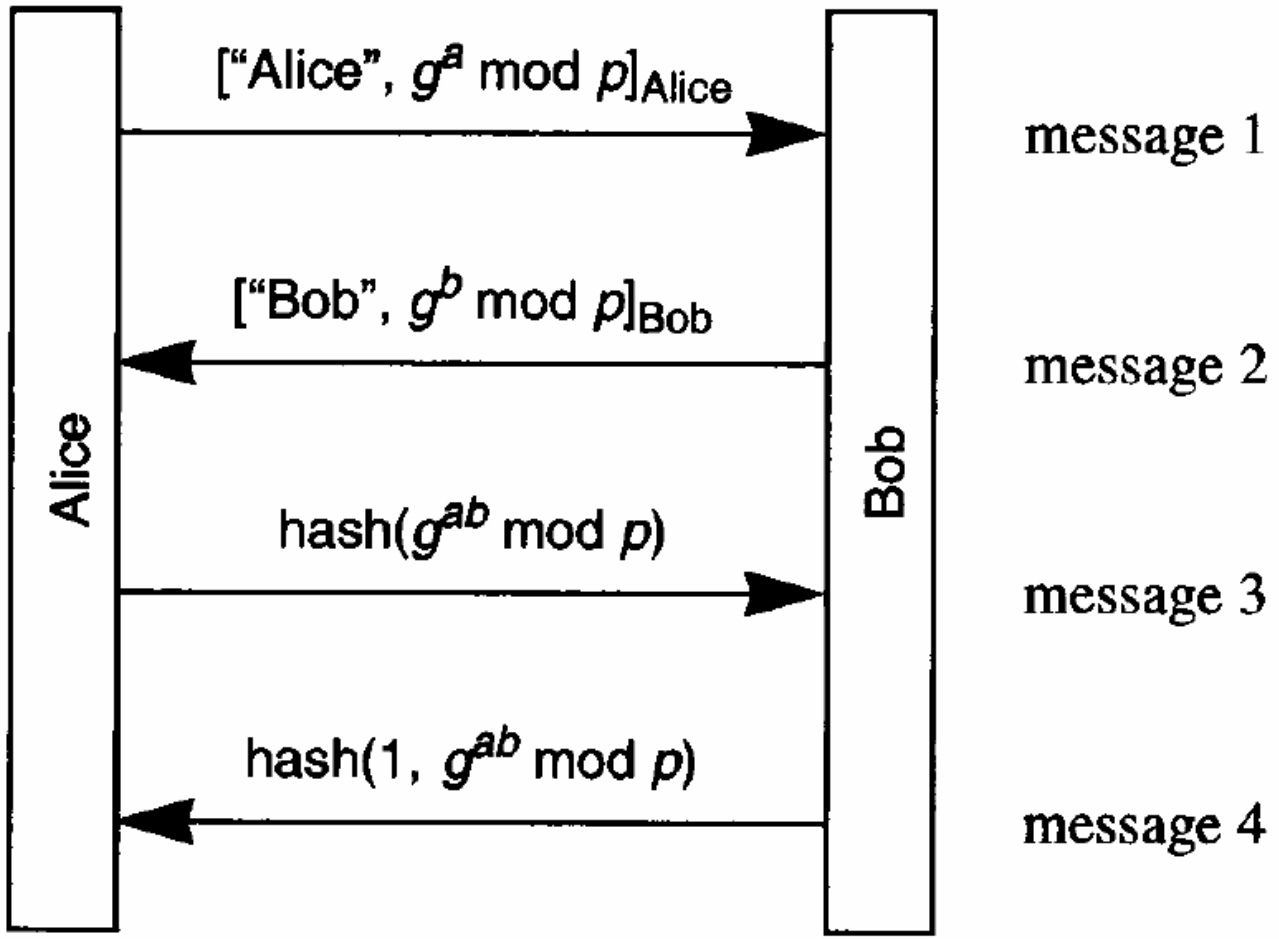
- Why do we need Internet Key Management
  - AH and ESP require encryption and authentication keys
- Process to negotiate and IPsec SA’s between two entities

Security Principles

- Basic security principles for session keys
  - Compromise of a session key
    - Does not permit reuse of the compromised session key
    - Does not compromise future session keys and long-term keys
- Perfect Forward Secrecy (PFS)
  - Compromise of current keys (session key or long-term key) does not compromise past session keys
  - Concern for encryption keys but not for authentication keys

Please refer to p. 407 of the textbook

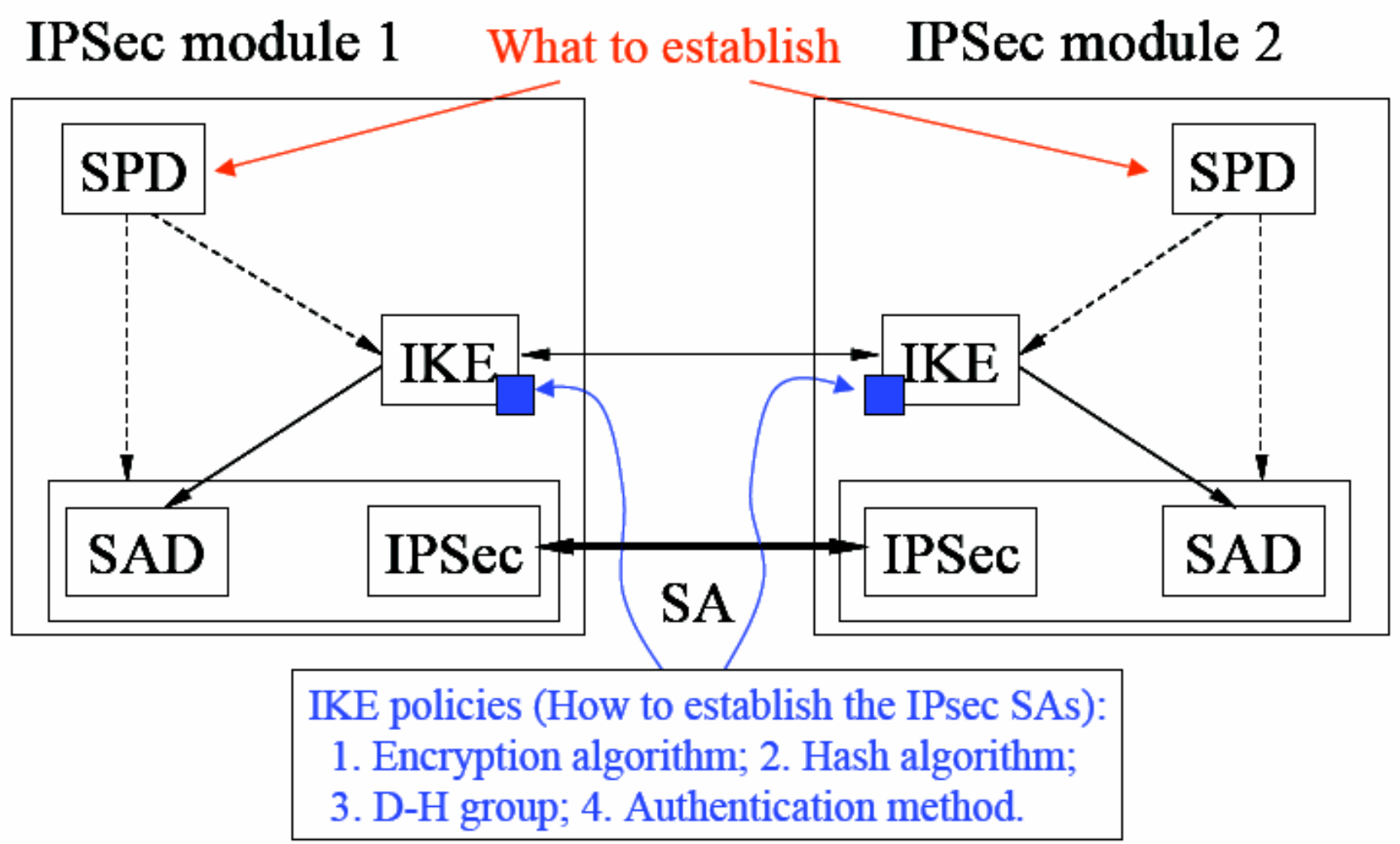
Diffie-Hellman for PFS using Signature Keys



Internet Key Management

- Manual Key Management
  - Mandatory
  - Useful when IPsec developers are debugging
  - Keys exchanged offline (phone, email, etc.)
  - Set up SPI and negotiate parameters

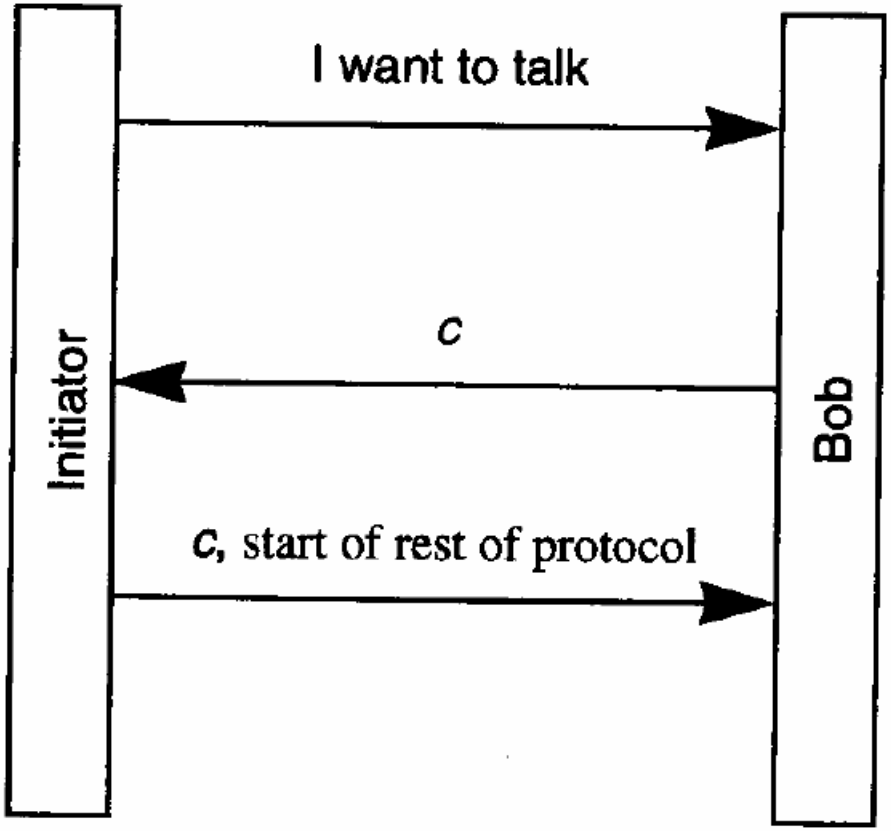
IPsec Architecture revisited



Internet Key Management

- Automatic key management
  - Simple Key-Management for Internet Protocols (SKIP)
  - ISAKMP/OAKLEY
    - Photuris
      - Ephemeral D-H + authentication + Cookie
      - The first to use cookie to thwart DoS attacks
    - SKEME (extension to Photuris)
    - Oakley (RFC 2412)
    - ISAKMP (RFC 2408)
    - ISAKMP/OAKLEY -> IKE (RFC 2409)

Stateless Cookie Protocol



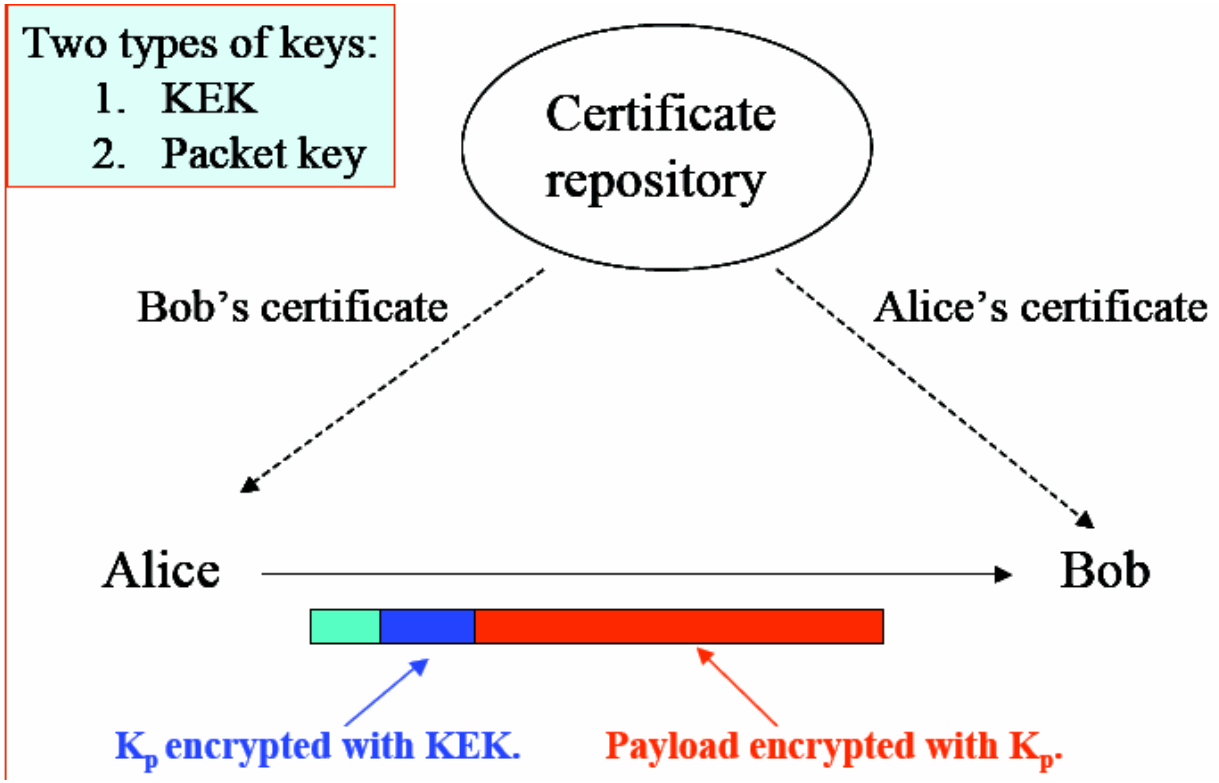
c = hash(IP address, secret)

Does c = hash(IP address, secret)?
If so, continue with protocol.

Please refer to p. 410-411 of the textbook

SKIP: Simple Key-Management for Internet Protocols

- Pre-Distribution and authenticated D-H public key
- Packet-specific encryption keys are included in the IP packet

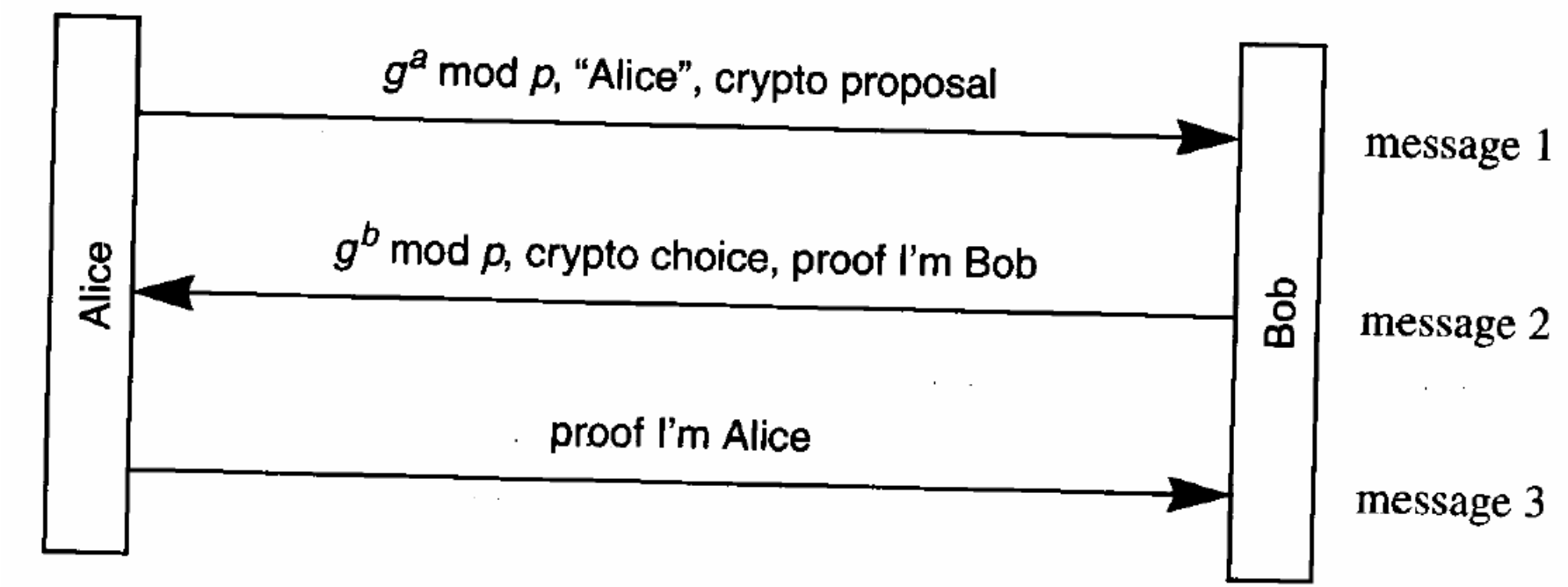


- No concept of SA: difficult to work with current IPsec architecture

IKE Phases

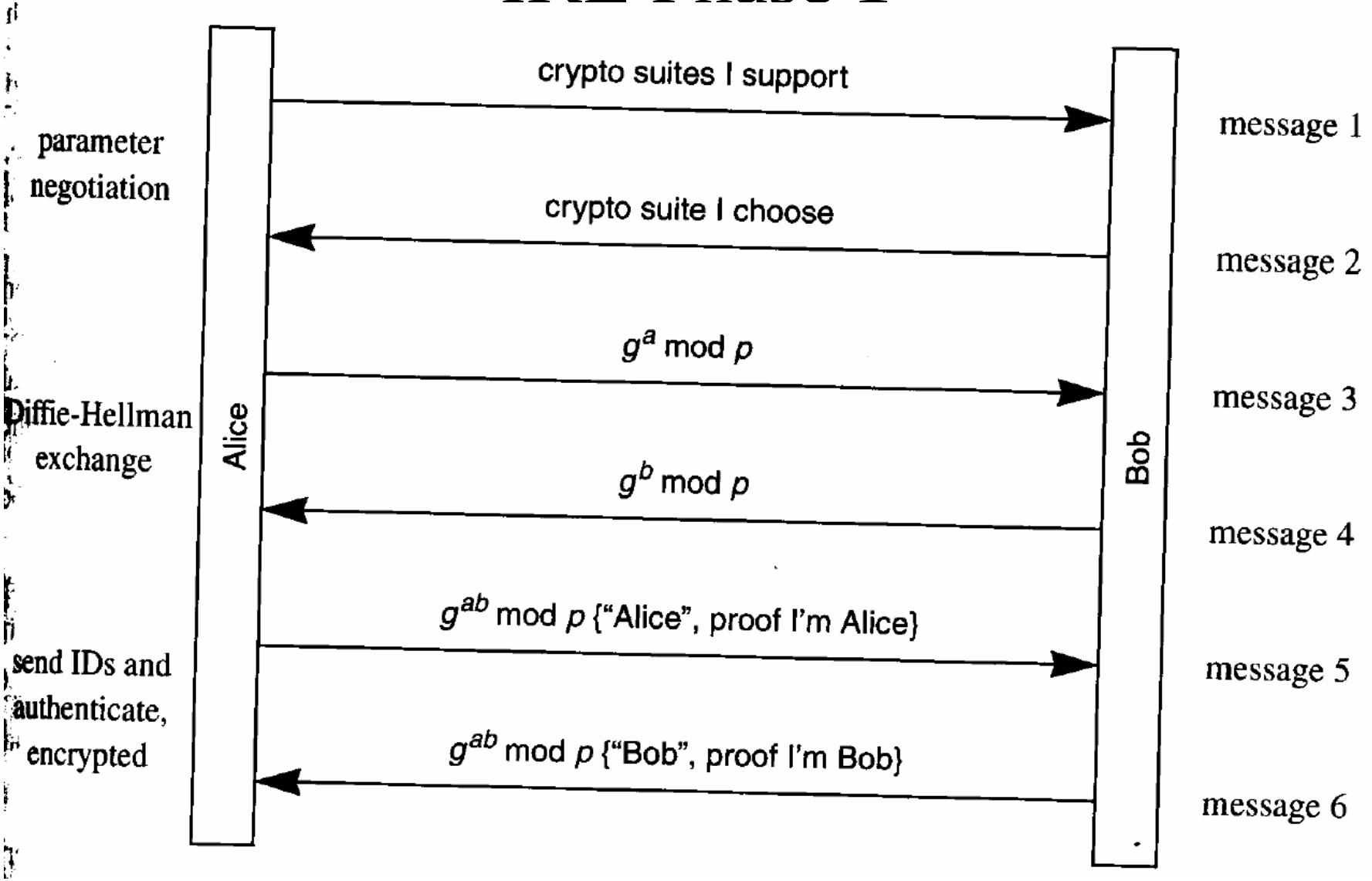
- Phase 1
  - Negotiate protection suite
  - Use Diffie-Hellman to establish shared secrets
  - Authenticate the shared secret, IKE SA
  - Based on three types of keys
    - Pre-shared secret key
    - Public encryption key
      - A public key pair whose usage is restricted to encryption/decryption
    - Public signature key
      - A public key pair whose usage is restricted to signing/signature verification

IKE Phase 1



General Idea for all IKE phase-1 protocol – Aggressive Mode

IKE Phase 1



General Idea for all IKE phase-1 protocol – Main Mode

IKE Phase 1

- Four Authentication Methods
  - Original public key encryption
  - Revised public key encryption
  - Public key signature
  - Pre-shared secret key encryption
- For each authentication method
  - Main mode protocol
  - Aggressive mode protocol

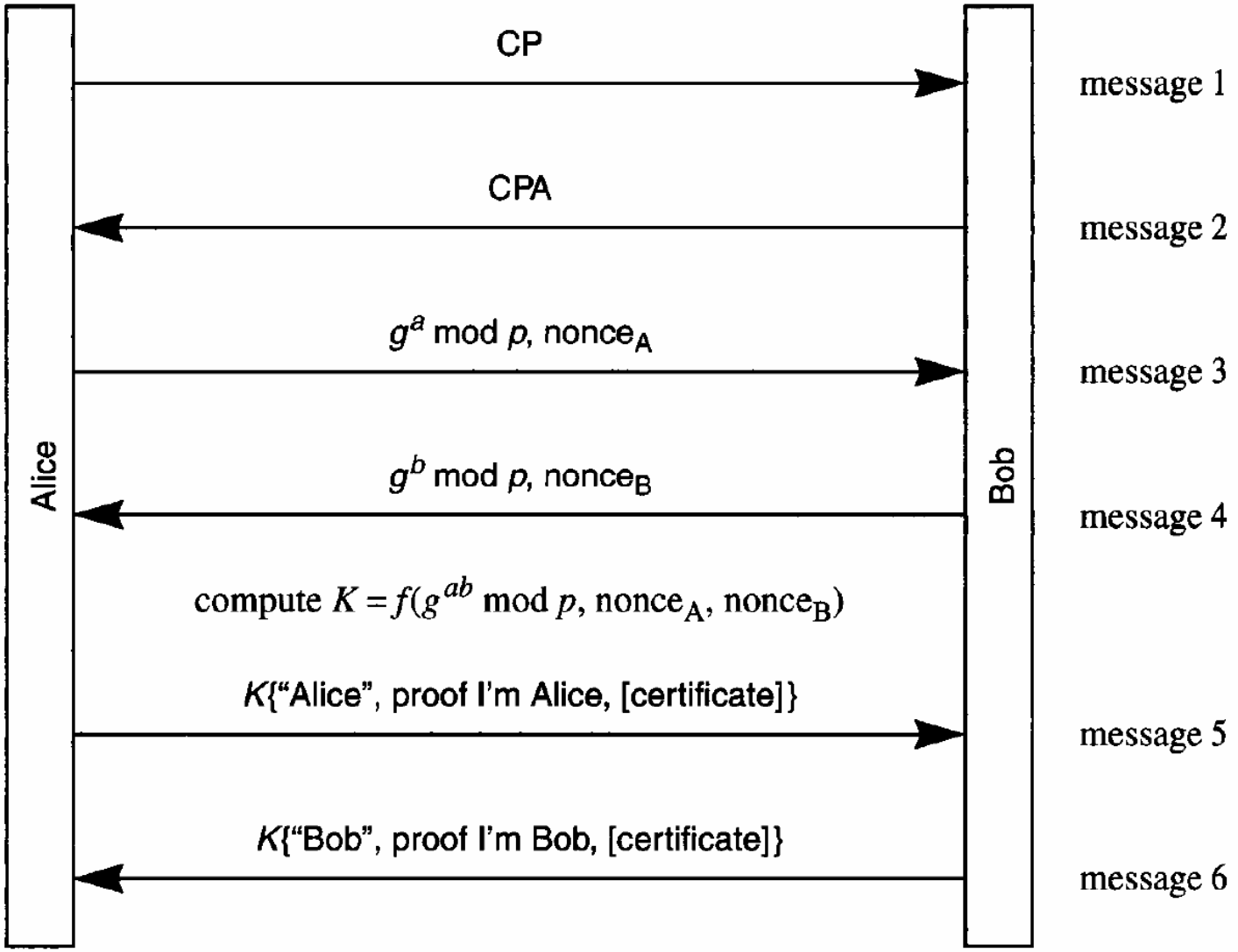
IKE Keys

- SKEYID:
  - Signature public key: prf(nonces, g^{xy})
  - Encryption public key: prf(hash(nonces), cookies)
  - Pre-shared key: prf(pre-shared secret key, nonces)

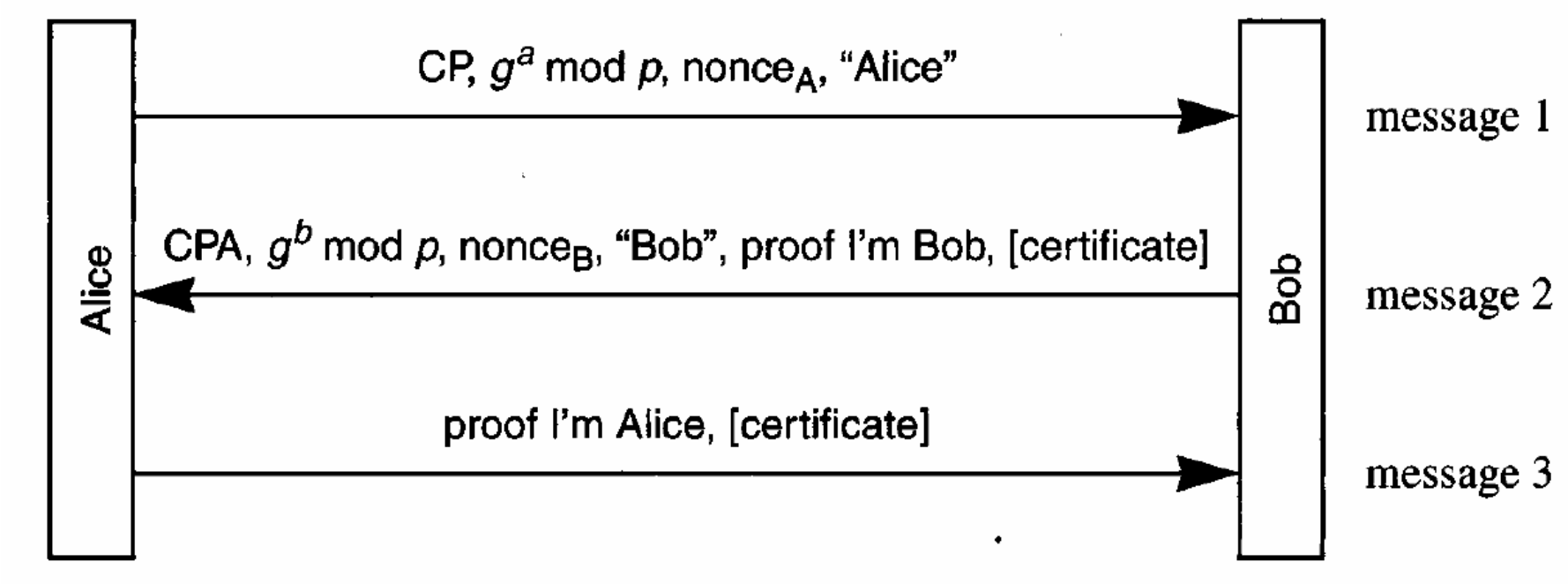
IKE Keys

- Three groups of keys
  - Derived key for non-ISAKMP negotiations
    - SKEYID_d = prf(SKEYID, (g^{xy}, cookies, 0))
  - Authentication Key (Integrity Protection Key)
    - SKEYID_a = prf(SKEYID, (SKEYID_d, (g^{xy}, cookies, 1))
  - Encryption Key
    - SKEYID_e = prf(SKEYID, (SKEYID_a, (g^{xy}, cookies, 2))
- To authenticate the established key
  - Initiator generates
    - Proof: prf(SKEYID, (g^{x}, g^{y}, cookies, A's initial crypto-parameters proposal, A's identity))
  - Responder generates
    - Proof: prf(SKEYID, (g^{y}, g^{x}, cookies, A's initial crypto-parameters proposal, B's identity))

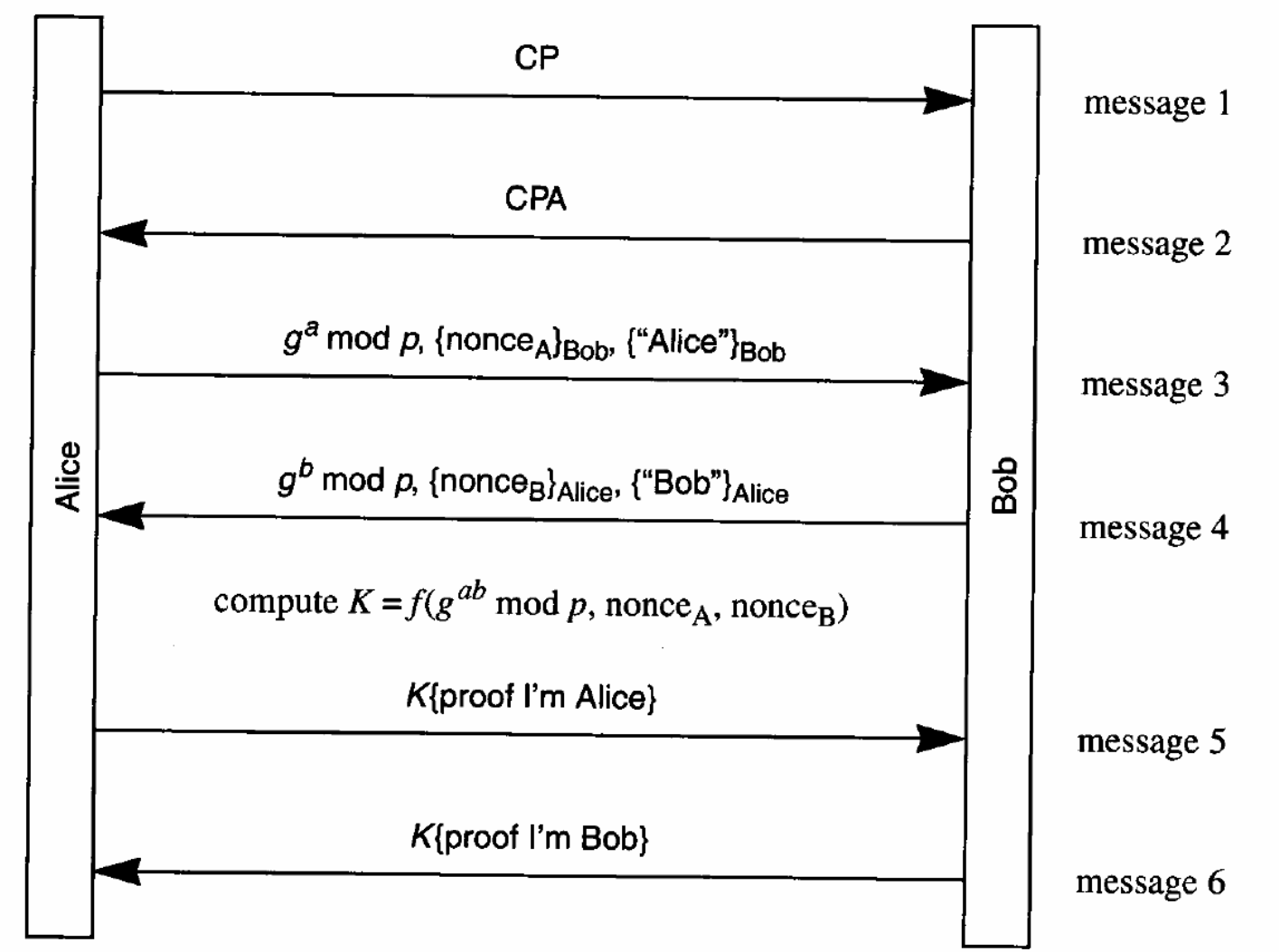
Public Signature Keys, main mode



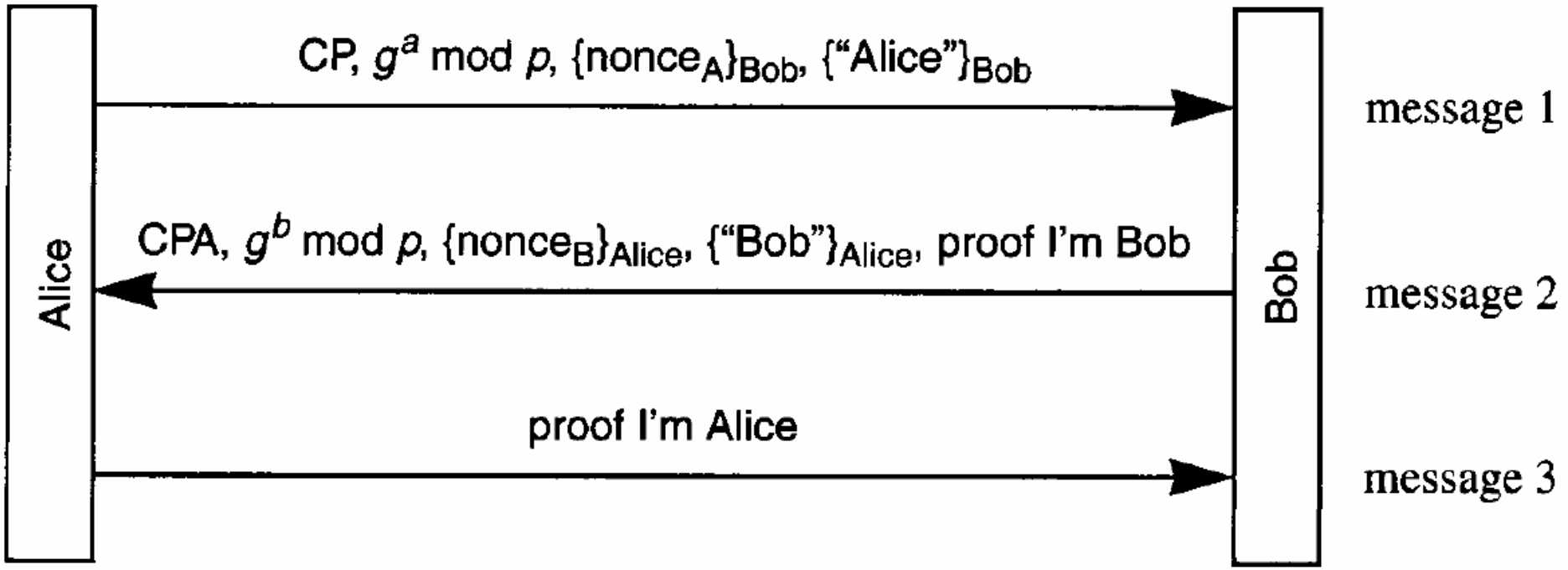
Public Signature Keys, Aggressive mode



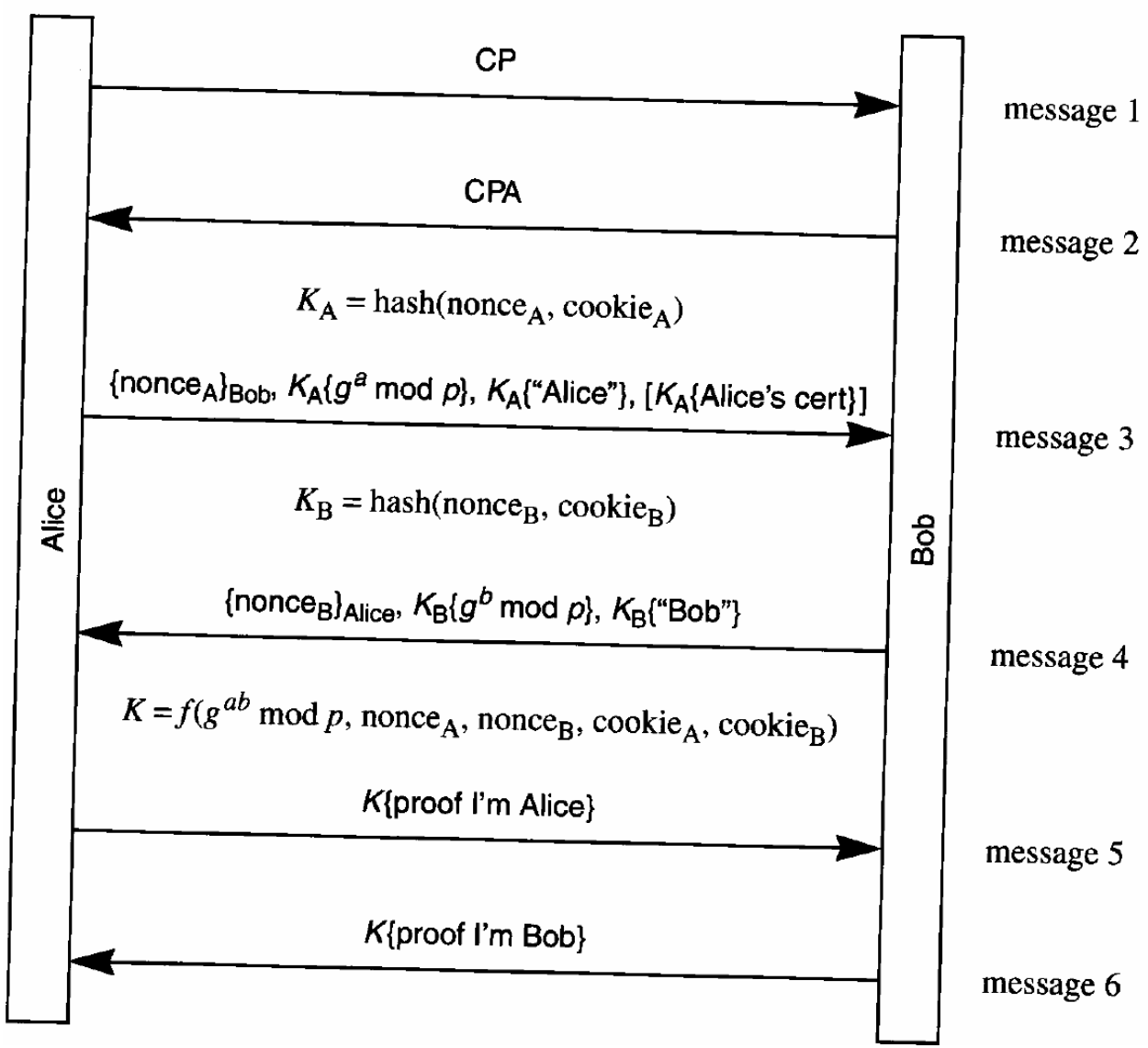
Public Encryption Keys, main mode, original protocol



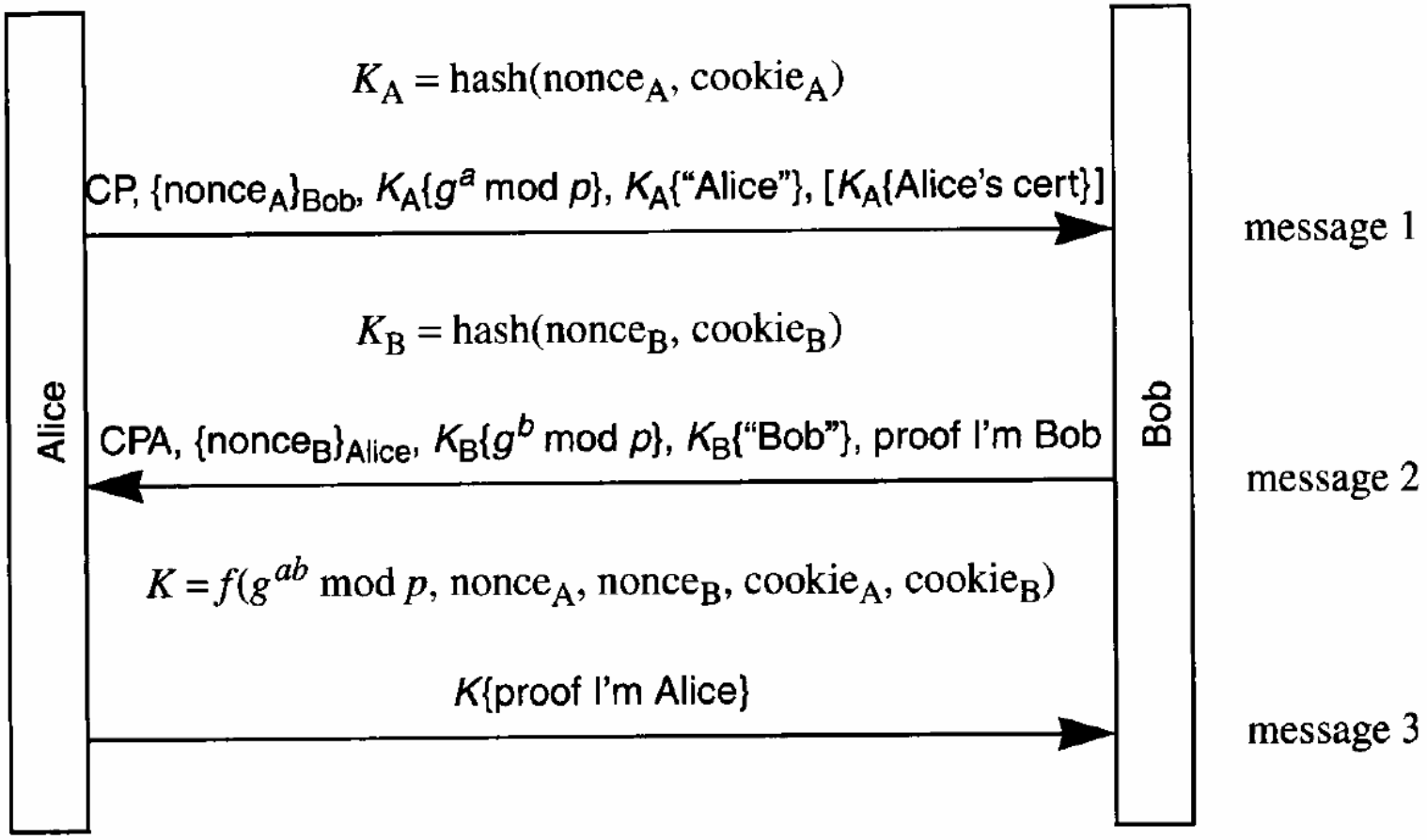
Public Encryption Keys, aggressive mode, original protocol



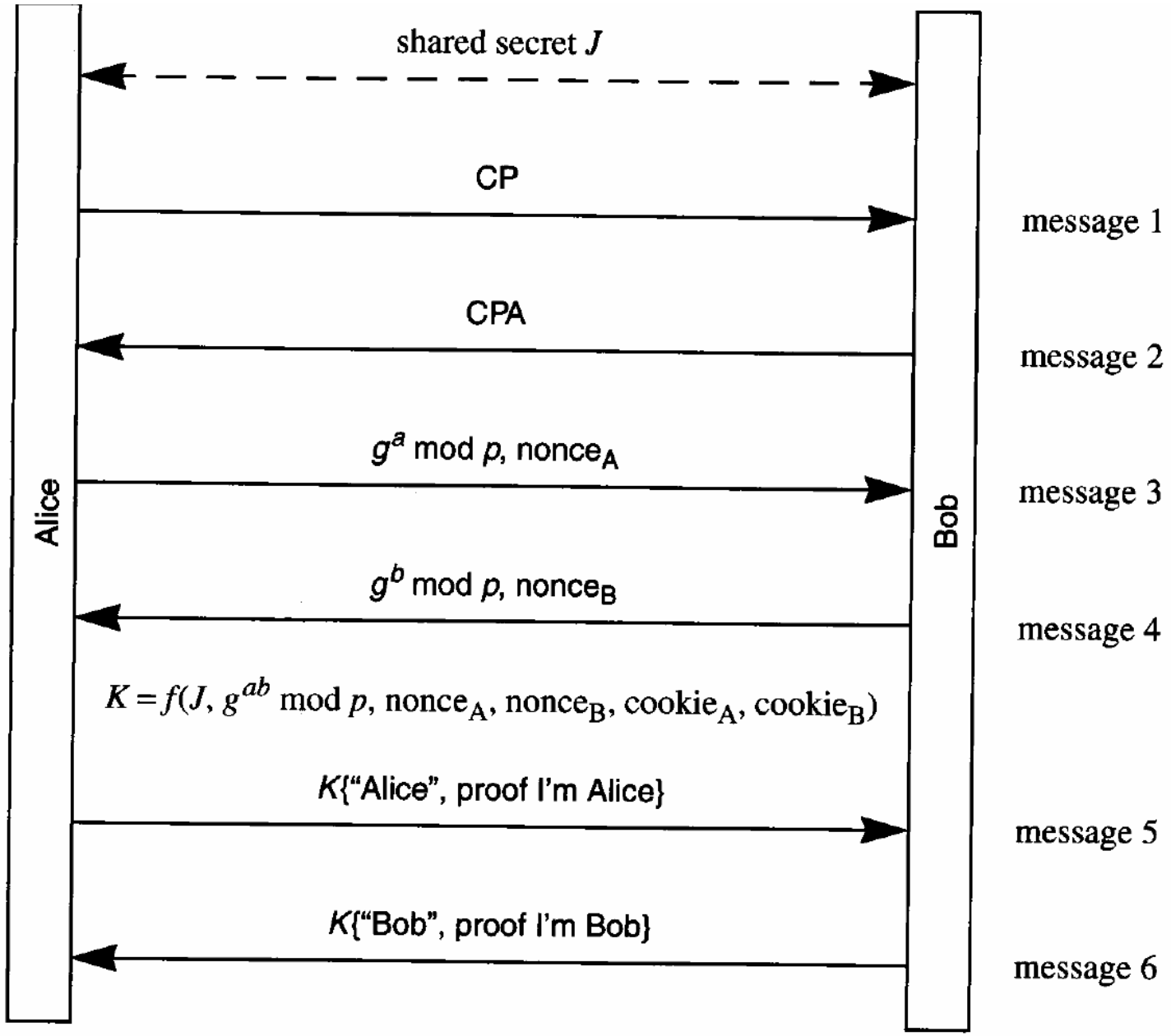
Public Encryption Keys, main mode, revised protocol



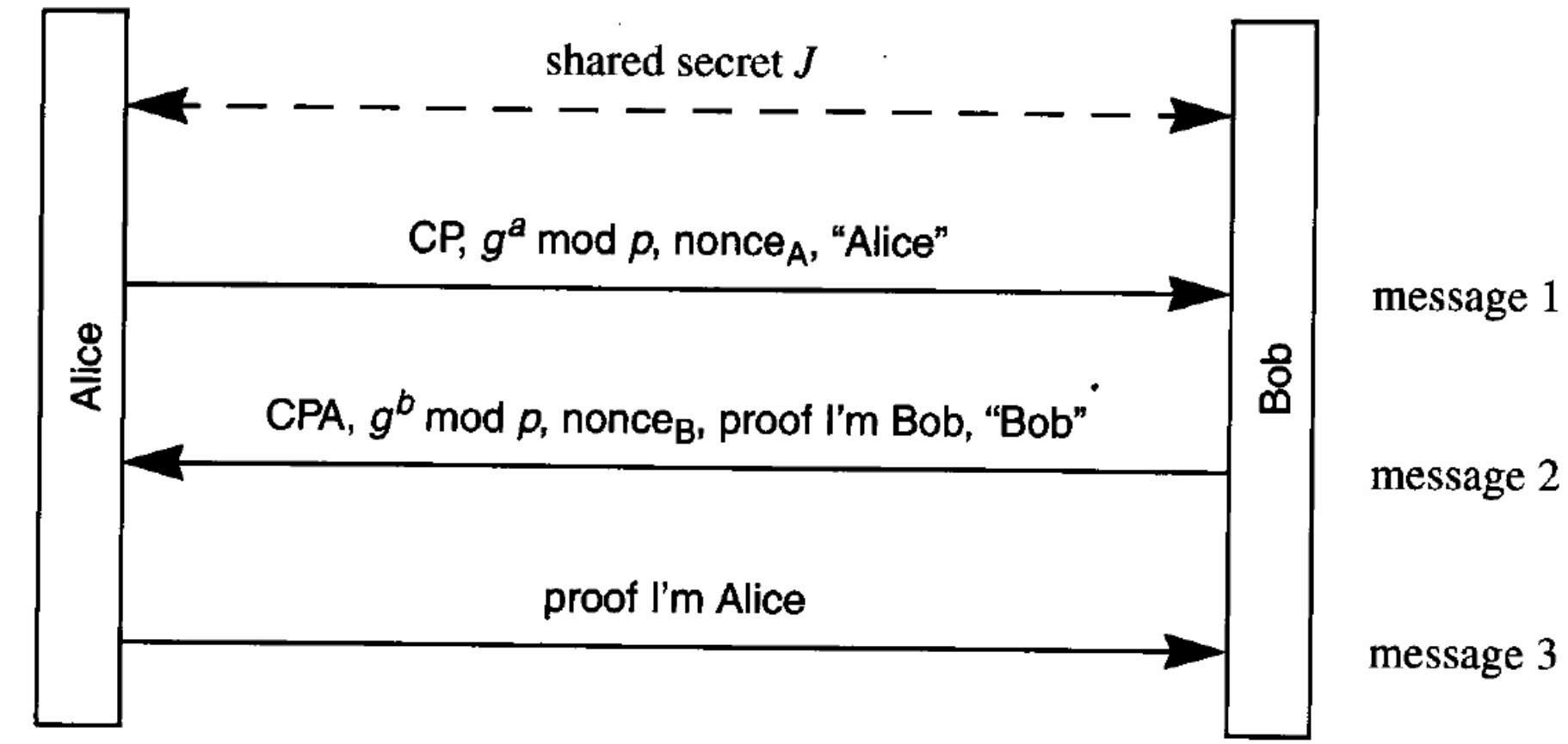
Public Encryption Keys, aggressive mode, revised protocol



Pre-shared secret, main mode



Pre-shared secret, aggressive mode



IKE Phase 2 – Quick Mode
Setting Up IPsec SAs

- Not a complete exchange itself
  - Must be bound to a phase 1 exchange
- Used t derive keying materials for IPsec SAs
- Information exchanged with quick mode must be protected by the ISAKMP SA
- Essentially a SA negotiation and an exchange of nonce
  - Generate fresh key material
  - Prevent replay attack

IKE Quick Mode