Applied Cryptography
CPEG 472/672
Lecture 10B

Instructor: Nektarios Tsoutsos

Diffie-Hellman (D-H) Key Exchange

- 1976: New Directions in Cryptography
  - First notion of public key protocol to establish a shared key between 2 parties
    - Establishing a shared key enables parties to create a secure communication channel
    - E.g., use the shared secret as AEAD or RSA key
  - All communication visible to attackers
    - Before D-H parties had to exchange envelopes
- Turing Award in 2015
- CryptoWars
  - https://stanfordmag.org/contents/keeping-secrets

Computing a shared key with D-H

- We have two parties: Alice and Bob
- We need two random integers $a, b \in \mathbb{Z}_p^*$
  - Each party selects their integer secretly
- Alice sends $A = g^a \bmod p$ to Bob
- Bob sends $B = g^b \bmod p$ to Alice
- Both compute $A^b = (g^a)^b = (g^b)^a = B^a \bmod p$
- The shared key is now $\mathrm{KDF}(g^{ab} \bmod p)$
  - The Key Derivation Function acts like a hash

Key Agreement Protocols

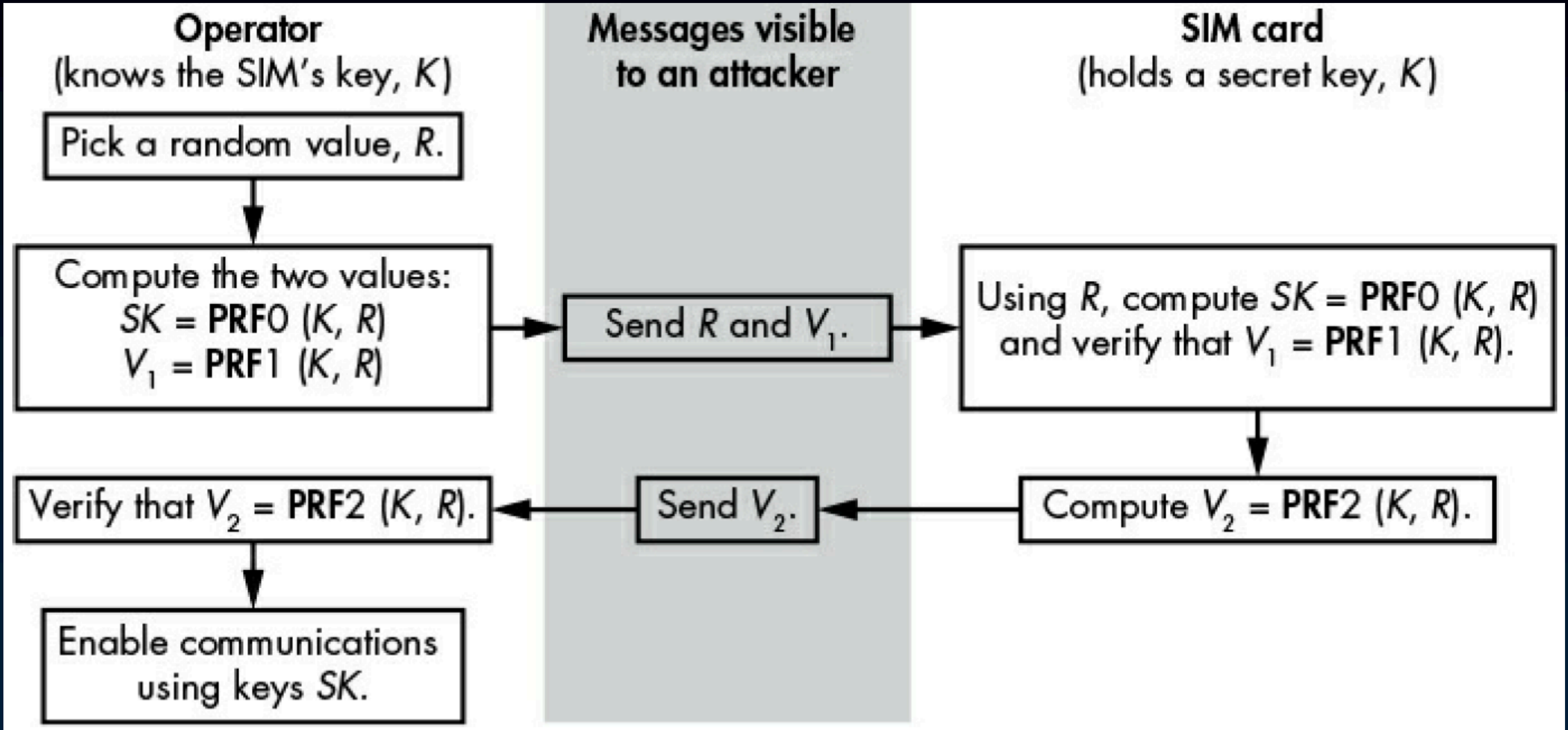
- Build secure communication between two or more parties over a network
  - Allows establishing a secret key
  - Shared secret is converted into session keys
- Attack models (what an attacker can do)
  - Eavesdropper: Observe exchanged msgs, and record, modify, drop, inject msgs
  - Data leak: Acquire session keys and temp secrets, but not any long-term secrets
  - Breach: Learn long-term secrets, can impersonate one or both parties
    - Cannot recover session secrets before breach

Key Agreement Protocols

- Security Goals (security guarantees)
  - Authentication: Mutual authentication
  - Key control: No party has full control on the share secret; all parties should contribute
  - Forward secrecy: Even if long-term secrets are exposed, the shared secrets of prior communications cannot be recovered
  - Resist impersonation: The attacker cannot impersonate a party even if the long-term key is compromised (KCI)
- Other goals: Performance, efficiency
  - Number of round trips (send + revc msgs)
  - Precomputations can save time

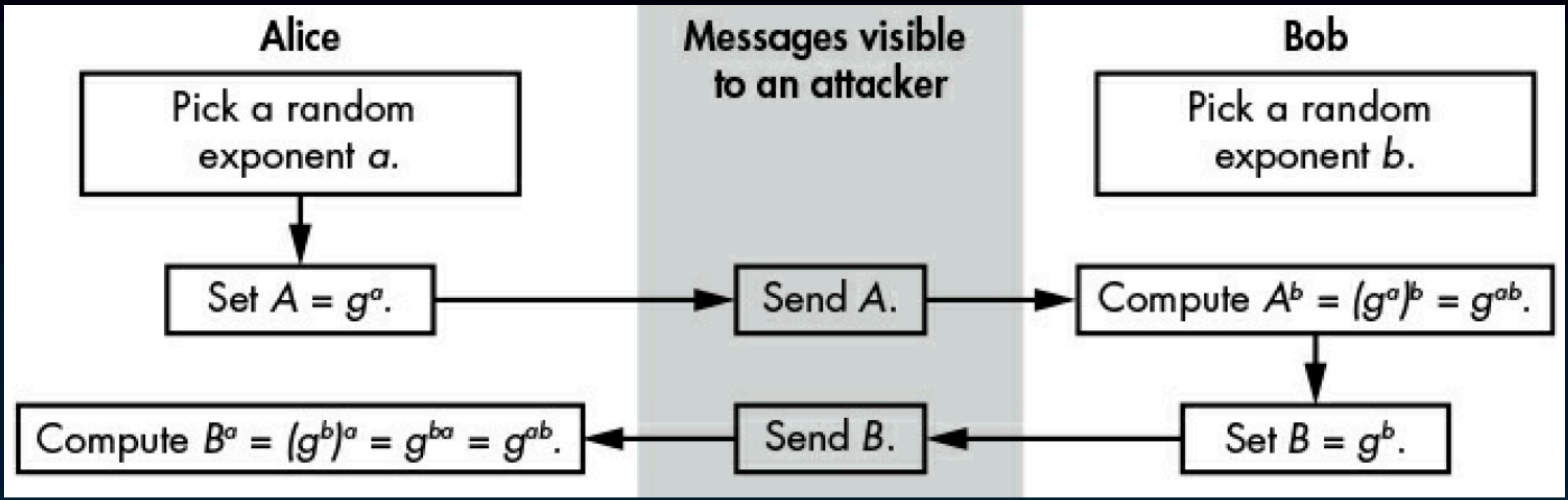
Example: Key Exchange without D-H

Authenticated key agreement for 3G/4G communications



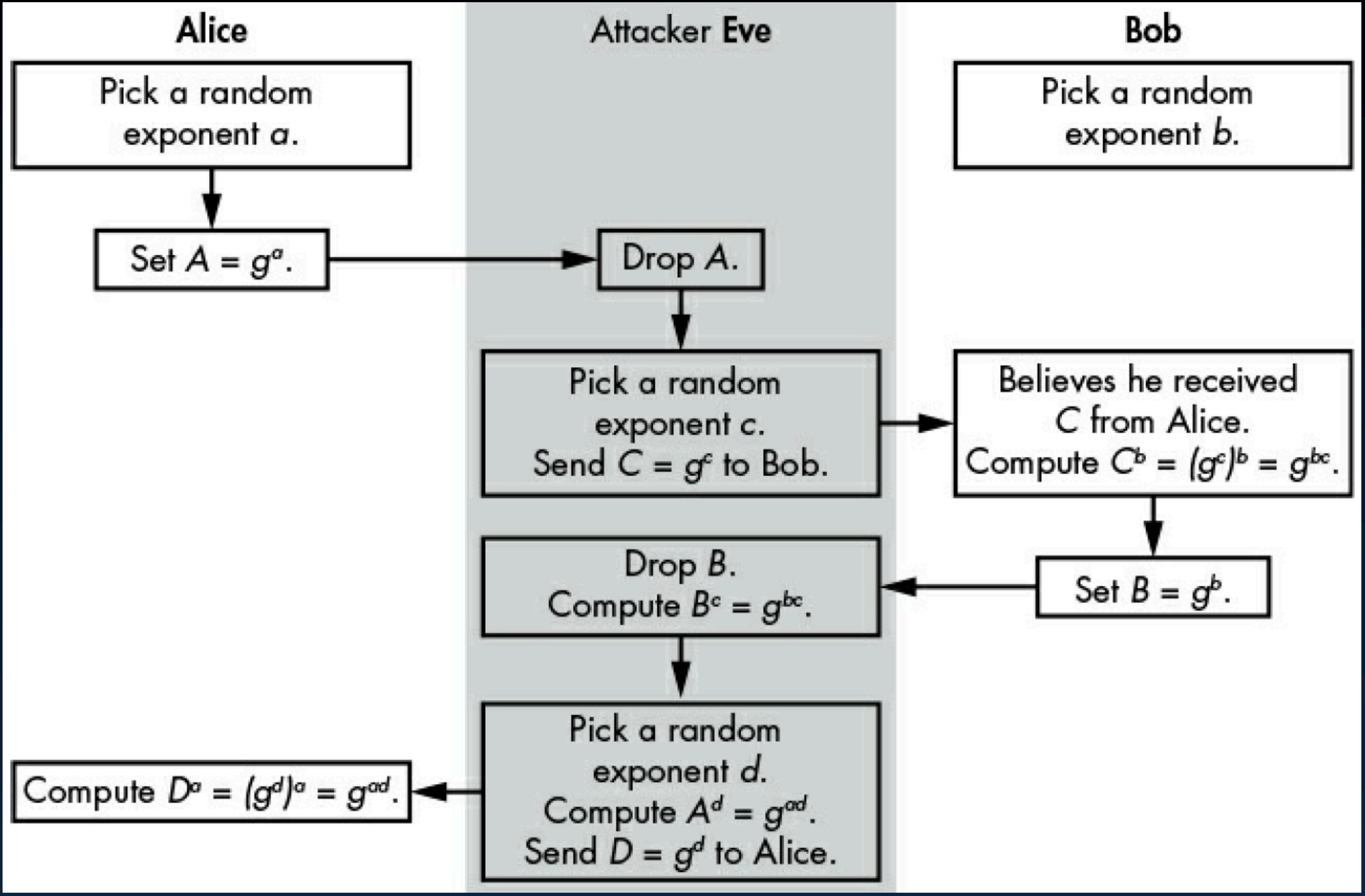
- Replay attacks? Ensure R is not reused
- If K leaked: MitM, decrypt msgs (needs R)
- No key control, no forward secrecy, KCI

Anonymous D-H



- Simple attack: MitM
  - To prevent MitM we need to authenticate the parties (each one will prove their ID)

MitM Attack on Anonymous D-H



D-H Problems

- Security lev. of D-H depends on size of p
  - Like RSA: 2048-bit p gives 90 bits of security
- Security of D-H based on DLP hardness
  - We break DLP if we find a given $b = g^a$ in $\mathbb{Z}_p^*$
  - We break D-H if we recover private value a
- Computational Diffie-Hellman (CDH)
  - Compute g^{ab} given only g^a and g^b
  - DLP is at least as hard as CDH
    - If we can solve DLP we can also solve CDH

D-H Problems (2)

- Decisional Diffie-Hellman (DDH)
  - Stronger than CDH hardness assumption
    - What if we get half bits of g^{ab} given only g^a, g^b?
    - This is bad, but does not qualify as solving CDH
  - The attacker should learn nothing about g^{ab}
    - g^{ab} must be indistinguishable from random
  - Given g^a, g^b and d, an attacker can't decide if $d = g^{ab}$ or $d = g^c$ for a random integer c
  - CDH is at least as hard as DDH
    - If you can solve CDH you can solve DDH

Math Background: D-H Function

- We work in group $\mathbb{Z}_p^*$ where p is a prime
  - The group $\mathbb{Z}_p^*$ is cyclic of order $\varphi(p) = p - 1$
    - The group has $p - 1$ integers
  - Exactly half of these $p - 1$ integers (we call them y_i) have a special property:

$$y_i = x^2 \bmod p \qquad \text{for some } x \in \mathbb{Z}_p^*$$

  - The number of y_i integers is $q = (p - 1)/2$ and form a subgroup of $\mathbb{Z}_p^*$ with q elements
    - If that subgroup had a prime order, then each element would be a generator of the subgroup
    - Can q be a prime number?

Math Background: D-H Function (2)

- So far: $q = (p-1)/2$, p is prime
  - If q is also prime, every y_i in the subgroup would be a generator of that subgroup
    - Why we want to have a prime-order subgroup?
    - Because the DLP is hard in these subgroups
      - The Pohlig-Hellman algorithm cannot break DLP
    - Finding a generator is easy (any element works)
- If both p, q are primes then $p = 2q + 1$
  - Such p is called a safe prime
  - More complex search vs finding RSA primes
    - Takes 1000x longer to find them

Math Background: Subgroups example

- Cyclic group $\mathbb{Z}_{23}^{*}$ where $23 = 2 \cdot 11 + 1$

g: #order(g): Generated integers $g^0, g^1, \ldots, g^{order}$

```
 1: # 1:  1,  1
 2: #11:  1,  2,  4,  8, 16,  9, 18, 13,  3,  6, 12,  1
 3: #11:  1,  3,  9,  4, 12, 13, 16,  2,  6, 18,  8,  1
 4: #11:  1,  4, 16, 18,  3, 12,  2,  8,  9, 13,  6,  1
 5: #22:  1,  5,  2, 10,  4, 20,  8, 17, 16, 11,  9, 22, 18, 21, 13, 19,  3, 15,  6,  7, 12, 14,  1
 6: #11:  1,  6, 13,  9,  8,  2, 12,  3, 18, 16,  4,  1
 7: #22:  1,  7,  3, 21,  9, 17,  4,  5, 12, 15, 13, 22, 16, 20,  2, 14,  6, 19, 18, 11,  8, 10,  1
 8: #11:  1,  8, 18,  6,  2, 16, 13, 12,  4,  9,  3,  1
 9: #11:  1,  9, 12, 16,  6,  8,  3,  4, 13,  2, 18,  1
10: #22:  1, 10,  8, 11, 18, 19,  6, 14,  2, 20, 16, 22, 13, 15, 12,  5,  4, 17,  9, 21,  3,  7,  1
11: #22:  1, 11,  6, 20, 13,  5,  9,  7,  8, 19,  2, 22, 12, 17,  3, 10, 18, 14, 16, 15,  4, 21,  1
12: #11:  1, 12,  6,  3, 13, 18,  9, 16,  8,  4,  2,  1
13: #11:  1, 13,  8, 12, 18,  4,  6,  9,  2,  3, 16,  1
14: #22:  1, 14, 12,  7,  6, 15,  3, 19, 13, 21, 18, 22,  9, 11, 16, 17,  8, 20,  4, 10,  2,  5,  1
15: #22:  1, 15, 18, 17,  2,  7, 13, 11,  4, 14,  3, 22,  8,  5,  6, 21, 16, 10, 12, 19,  9, 20,  1
16: #11:  1, 16,  3,  2,  9,  6,  4, 18, 12,  8, 13,  1
17: #22:  1, 17, 13, 14,  8, 21, 12, 20, 18,  7,  4, 22,  6, 10,  9, 15,  2, 11,  3,  5, 16, 19,  1
18: #11:  1, 18,  2, 13,  4,  3,  8,  6, 16, 12,  9,  1
19: #22:  1, 19, 16,  5,  3, 11,  2, 15,  9, 10,  6, 22,  4,  7, 18, 20, 12, 21,  8, 14, 13, 17,  1
20: #22:  1, 20,  9, 19, 12, 10, 16, 21,  6,  5,  8, 22,  3, 14,  4, 11, 13,  7,  2, 17, 18, 15,  1
21: #22:  1, 21,  4, 15, 16, 14, 18, 10,  3, 17, 12, 22,  2, 19,  8,  7,  9,  5, 13, 20,  6, 11,  1
22: # 2:  1, 22,  1
```

Math Background: D-H Function (3)

- Select one of the y_i values as g
  - With a safe prime p, each y_i is a generator
  - The order of each y_i element is q
  - g is public along with p
- If p is safe we can also choose $g = 2$
  - Why this is ok?
  - We know the order of any $x \in \mathbb{Z}_p^*$ must divide the order of the group, which is $p - 1 = 2q$
    - The divisors of $2q$ are $1, 2, q, 2q$
    - If $x \neq 1$ and $x \neq p - 1$, its order is either q or $2q$

Hands-on exercises

- Anonymous D-H key exchange
- MitM attack on anonymous D-H

Reading for next lecture

- Aumasson: Chapter 11 until the end
  - We will have a short quiz on the material