UNIVERSITY OF DELAWARE

UD CYBERSECURITY

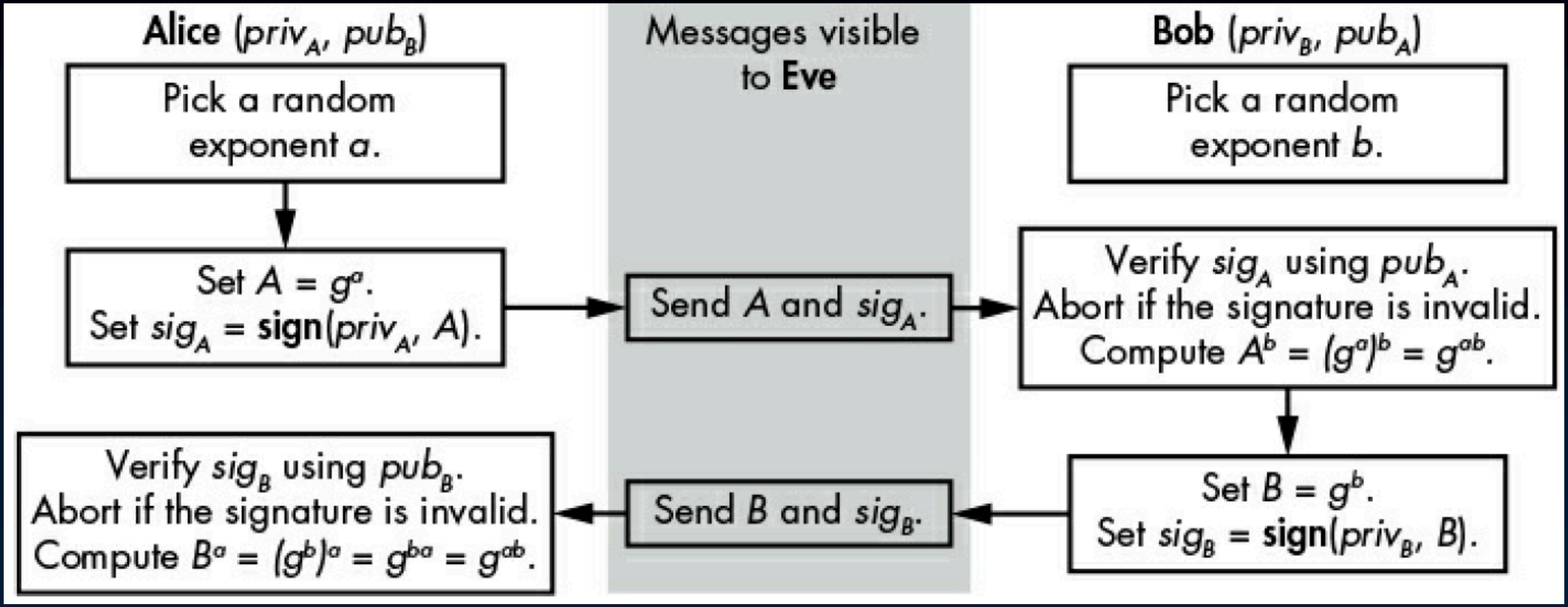
Applied Cryptography
CPEG 472/672
Lecture 11A

Instructor: Nektarios Tsoutsos

Authenticated D-H

- Mitigates MitM attack in anonymous D-H
  - Each party needs a private and public key
  - These are RSA keys for RSA-PSS signatures
  - Each party signs their messages
    - Eve cannot forge a valid signature
- Alice signs A with her private key
- Bob signs B with his private key
- Both verify the received signatures

Authenticated D-H



Alice ($priv_A$, pub_B)

Pick a random exponent a.

Set $A = g^a$.
Set sig_A = **sign**($priv_A$, A).

Verify sig_B using pub_B.
Abort if the signature is invalid.
Compute $B^a = (g^b)^a = g^{ba} = g^{ab}$.

Messages visible to **Eve**

Send A and sig_A.

Send B and sig_B.

Bob ($priv_B$, pub_A)

Pick a random exponent b.

Verify sig_A using pub_A.
Abort if the signature is invalid.
Compute $A^b = (g^a)^b = g^{ab}$.

Set $B = g^b$.
Set sig_B = **sign**($priv_B$, B).

- Eve learns nothing about g^{ab}

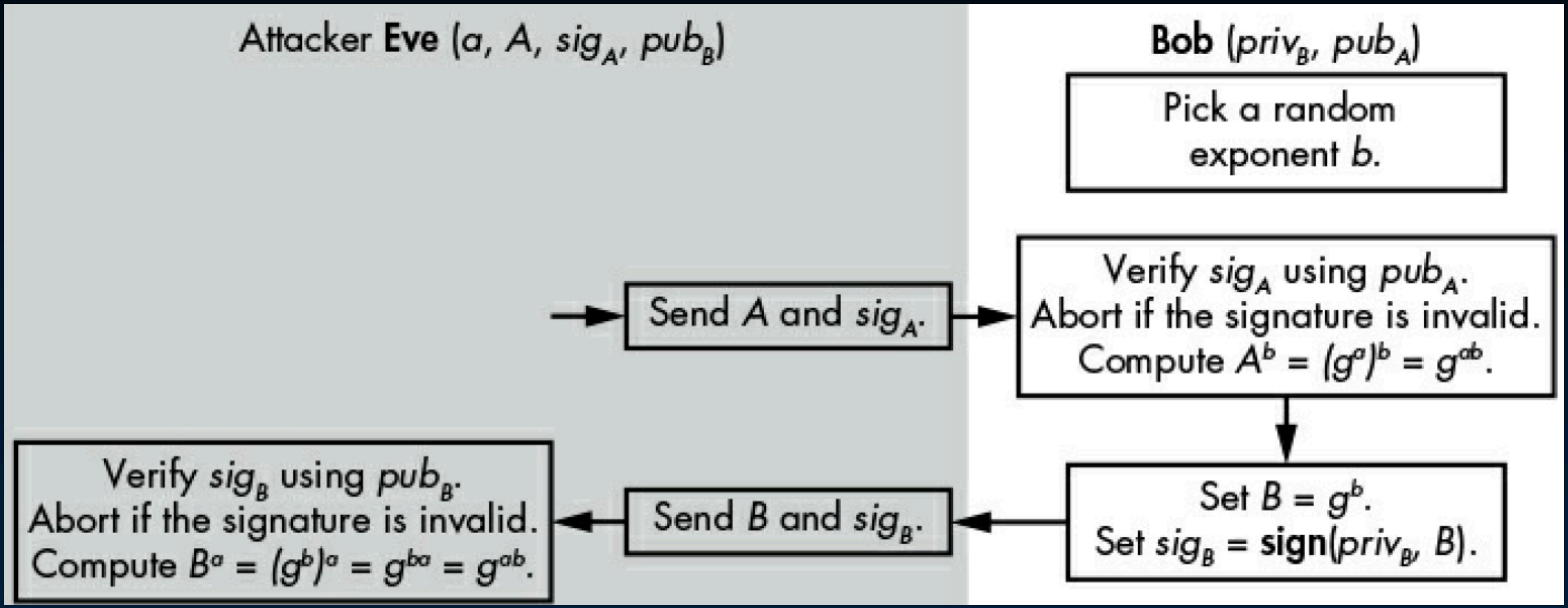
Authenticated D-H

- Offers Forward Secrecy
  - A breach may leak private keys but not any previous shared secrets g^{ab}
  - The temporary secrets can't be leaked
- Prevents key control
  - No party can control the shared secret
  - Alice may select a=0 so A=1 (it's detected)
- Vulnerable to replay attacks
  - Eve records and replays A, sig(A)
    - Key confirmation: $\mathcal{H}(p_A||p_B, g^{ab}),\ \mathcal{H}(p_B||p_A, g^{ab})$

Data leaks in Authenticated D-H

- Attacker learns temp secrets a and b
  - Can impersonate one of the parties
- Example
  - Eve learns a, A, sig(A)
  - Eve can initiate a new execution pretending to be Alice (impersonation)
  - Eve replays A, sig(A) to Bob
  - Bob verifies sig(A) and sends B, sig(B)
  - Both compute g^{ab}

Data leaks in Authenticated D-H



Attacker **Eve** (a, A, sig_A, pub_B)

Bob ($priv_B$, pub_A)

Pick a random exponent b.

Send A and sig_A.

Verify sig_A using pub_A. Abort if the signature is invalid. Compute $A^b = (g^a)^b = g^{ab}$.

Set $B = g^b$. Set sig_B = **sign**($priv_B$, B).

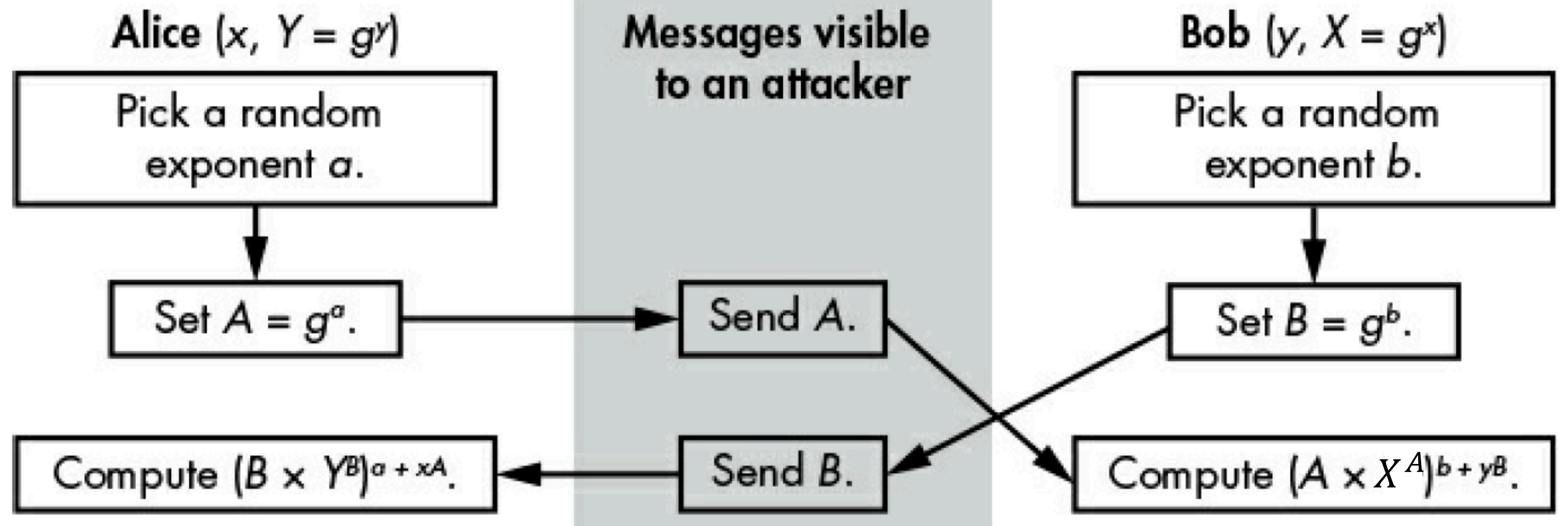
Send B and sig_B.

Verify sig_B using pub_B. Abort if the signature is invalid. Compute $B^a = (g^b)^a = g^{ba} = g^{ab}$.

Menezes-Qu-Vanstone (MQV)

- More secure than authenticated D-H
- Approved by NSA for critical assets
  - Dropped later
- Each party sends one value
  - Alice sends A, Bob sends B
- Priv and Pub keys are D-H keys not RSA
  - Private exponent x, public value g^x
- Both compute $g^{(b+yB)(a+xA)}$
  - Shared secret between Alice and Bob

Menezes-Qu-Vanstone (MQV)



Alice (x, $Y = g^y$)

Messages visible to an attacker

Bob (y, $X = g^x$)

Pick a random exponent a.

Set $A = g^a$.

Send A.

Pick a random exponent b.

Set $B = g^b$.

Send B.

Compute $(B \times Y^B)^{a + xA}$.

Compute $(A \times X^A)^{b + yB}$.

- Leaking a, b does not break MQV
  - Shared secret also depends on private keys
  - Breach: if x, y leaked, old shared keys safe

Menezes-Qu-Vanstone (MQV)

- No perfect forward secrecy
  - Eve can perform MitM and replace A with E
  - $E = g^e$ is computed by Eve using her e
  - Bob sends B to Alice and Eve records it
- This attack requires Eve to also steal Alice's private key x later
  - Eve can recover the shared secret from an old session
  - Attack not very useful, as Alice can detect she doesn't share the same key with Bob
  - The protocol is aborted immediately

Failures of D-H protocols

- Using the shared secret without hashing
  - The shared secret is not uniformly random
  - Cannot be used directly as a key
  - Need a KDF (e.g., HMAC-based KDF, scrypt)
- Some TLS versions allow anonymous D-H
- Not using safe primes in D-H
  - OpenSSL allowed unsafe primes
  - Allows small subgroups, easier to brute force
  - CVE-2-16-0701 exploit

Hands-on exercises

- Authenticated D-H key exchange
- Menezes-Qu-Vanstone (MQV)
- Bias in shared secret

Reading for next lecture

- Aumasson: Chapter 12 until The ECDLP Problem (inclusive)
  - We will have a short quiz on the material