ECE 646 – Lecture 4B

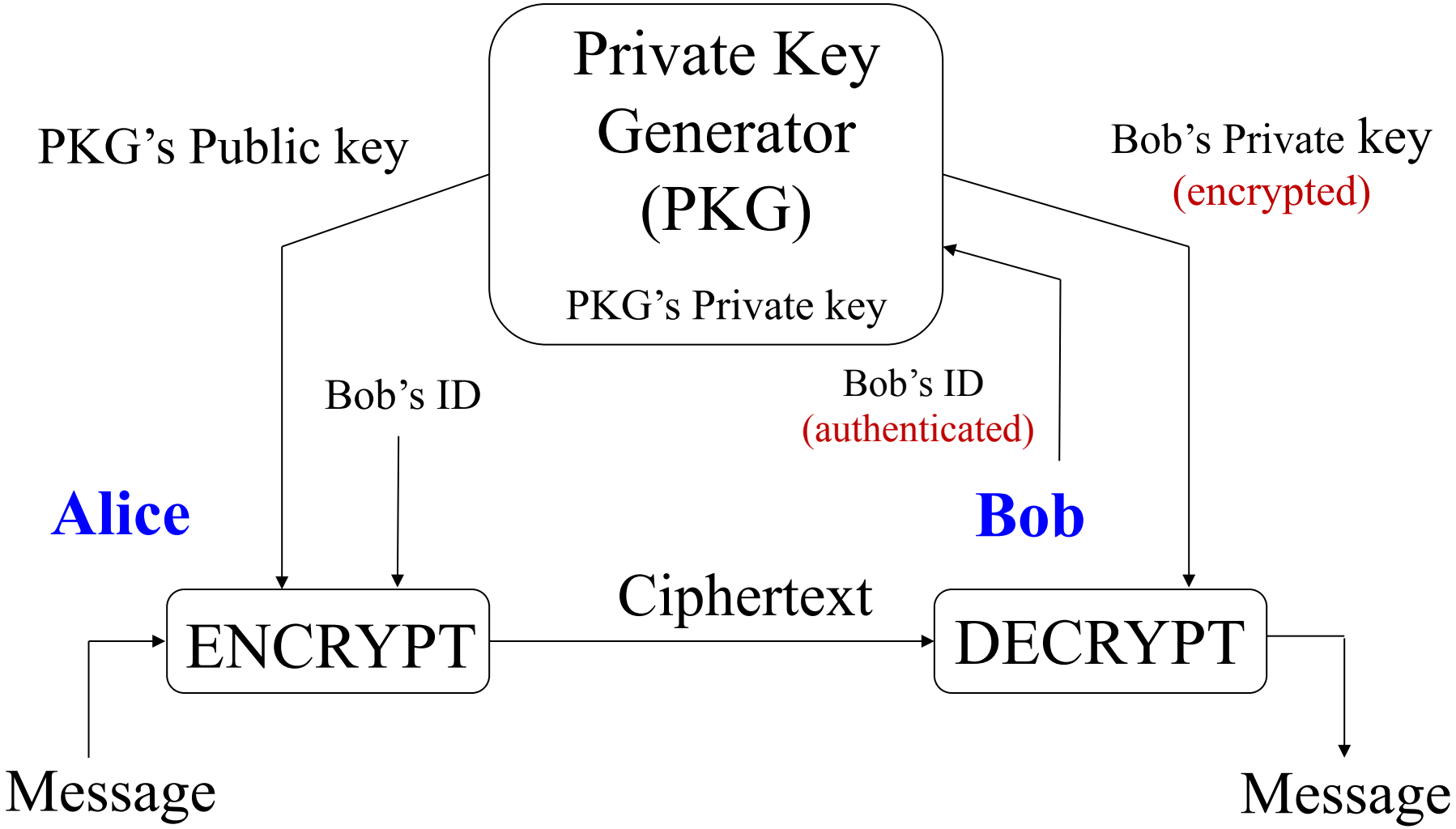
Identity-based Encryption

Certificate-based & Certificateless Cryptography

Identity-based Encryption

- The idea behind Identity-based Encryption (IBE) was originally proposed by Adi Shamir in 1984
- IBE remained one of the major unsolved problems in cryptography till early 2000
- In 2001, Dan Boneh and Matt Franklin, invented a practical scheme to implement IBE
- User's identity attributes, such as email addresses or phone numbers can be used to derive public keys

Identity-based Encryption Scheme



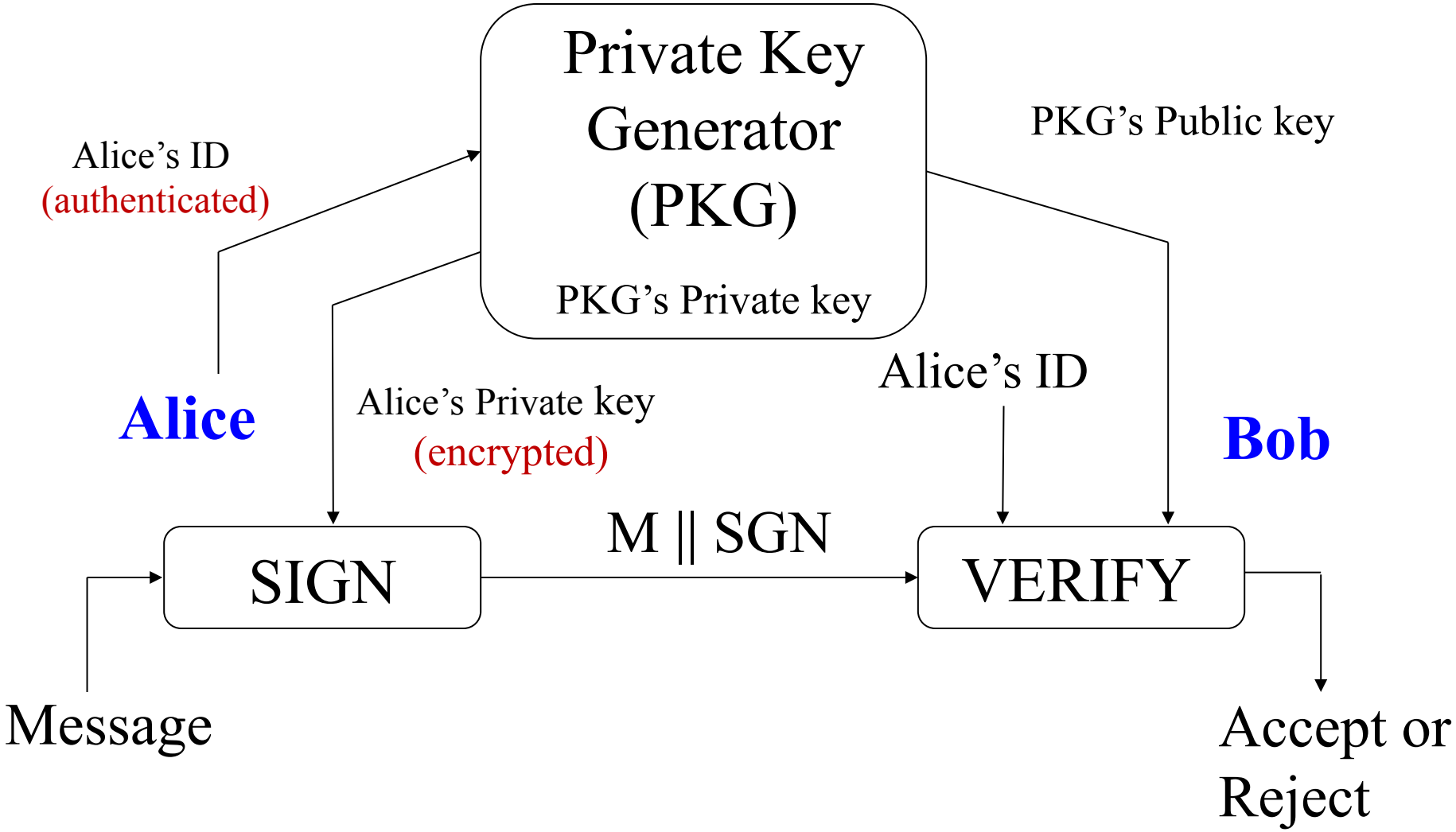
Identity-based Encryption Scheme

- Before operation can begin, the PKG must generate a public/ private key pair
- Alice uses Bob's identity and the PKG's public key to encrypt the Message, obtaining the corresponding Ciphertext
- Bob receives the ciphertext from Alice
- Bob authenticates with the PKG and sends authenticated Bob's ID that belongs to him
- PKG sends the encrypted Bob's private key to him over a secure channel
- Bob decrypts the Ciphertext using his private key to recover the Message

Identity-based Encryption Scheme

- Bob’s ID and PKG’s public key were both already known to Alice before beginning the encryption process.
- Alice requires no prior coordination or preparation on Bob's part to encrypt a message for him.
- Bob authenticates with the PKG by essentially sending it sufficient proof that the ID belongs to him

Identity-based Signature Scheme



Identity-based Signature Scheme

- Alice receives her private key from the PKG
- Alice generates a signature for the Message using her private key and transmits it to Bob
- After receiving the Message and Signature from Alice, Bob checks whether the Signature is genuine using Alice's identity and the PKG's public key.
- If it is, he returns “Accept”. Otherwise, he returns “Reject”.

Revocation in Identity-based Cryptography

- In identity-based cryptosystems (IBC's), a user's identity attributes, such as email addresses or phone numbers can be used to derive public keys

- Identity-based schemes also should have means to revoke users from the system

- Boneh and Franklin suggested that users can periodically obtain new private keys in IBC systems

- It can be done by attaching a time period to the identity, so the private key associated with that identity will be valid for the specified time

Identity-based Cryptography Pros

- No need to manage a public key infrastructure and certificates
- No preparation is required on the part of the recipient to receive an encrypted message
  - allows messages to be encrypted and sent to users who have not yet requested their private key from the private key generator
- Many organizations consider key escrow useful in order to be able to recover a user's encrypted data if the private key is lost
- To deliver decryption keys, any authentication resources that are already deployed (e.g., directories or web authentication) can be reused.

Identity-based Cryptography Cons

- Key escrow property is inherent in all IBC. The PKC knows the private keys and can easily decrypt and sign users' messages
- Requires a secure channel between a sender or recipient and the PKG to transmit the private key
- IBC technique cannot provide true non-repudiation since the PKG can forge the signature of any user

Identity-based Cryptography Cons

- The re-issuance of keys on a time basis raises a few problems
  - The PKG has to be online for a greater amount of time
  - A secure channel will be required more often for the transportation of keys

Certificate-based & Certificateless Cryptography

Suggested Reading

"**A Survey of Certificateless Encryption Schemes and Security Models**" by Alexander W. Dent,

available at https://eprint.iacr.org/2006/211.pdf

"**Certificateless Cryptography I**" and "**Certificateless Cryptography II**" by Kenny Paterson. Invited talks at Workshop on Pairing Based Cryptography, Australia, June 2007,

available at:

http://www.isg.rhul.ac.uk/~kp/certlessI.pdf

http://www.isg.rhul.ac.uk/~kp/certlessII.pdf

S.S. Al-Riyami and K.G. Paterson, "Certificateless public key cryptography," in C.S. Laih (ed.), ASIACRYPT 2003, Lecture Notes in Computer Science Vol. 2894, pp. 452-473, Springer, 2003,

available at

http://eprint.iacr.org/2003/126, and

https://www.iacr.org/archive/asiacrypt2003/12_Session11/28_118/28940457.pdf

- Certificate-based Cryptography
  - Traditional Public Key Cryptography based on Public Key Infrastructure PKI
- Identity-based Cryptography (IBC)
  - The public keys can be generated with the identity of the user
  - The private keys are managed by Private Key Generator (PKG)
- Certificateless Cryptography (CL-PKC)
  - PKG only computes a partial private key of user

Certificateless Cryptography

- Presented by Al-Riyami and Paterson in 2003 as a new model to support public key cryptography
- The motivation was to eliminate the key escrow without introducing certificates
- In contrast to identity-based cryptography, the Key Generating Center (KGC) does not have access to the entitie's private key

Certificateless Cryptography

- The KGC has public parameters and a master key
- The user has a secret value that is known only to the user.
- A partial private key is generated by the KGC with the user's identity and its own master key
- The KGC must ensure that the partial private keys are delivered to the user securely.
- The user then generates the full private key using the partial private key and its secret value
- User's public key is generated using KGC's public parameters and the user's secret value

Certificateless Cryptography

- The user's public key should be available to other users either by placing in a public directory or by sending with messages specially in signing applications
- Both the public key and the user's identity are used to encrypt messages or verify signatures
- CL-PKC is no longer identity-based since the public key is no longer computable from an identity alone

Certificateless Cryptography Pros

- CL-PKC is an intermediate model between traditional PKI and IBC
  - It does not require the use of certificates like PKI
  - It does not have the built-in key escrow feature of IBC
- The KGC does not have access to entitie's private keys
- The user does not need to have the private key before generating the public key although both of them need the same user's secret information to generate them
- The trust assumptions required for KGC are much reduced

Certificateless Cryptography Cons

- A secure channels are required to transport the partial private keys to the correct users
- It does not achieve the same security level as traditional PKI as the KGC can still be compromised.