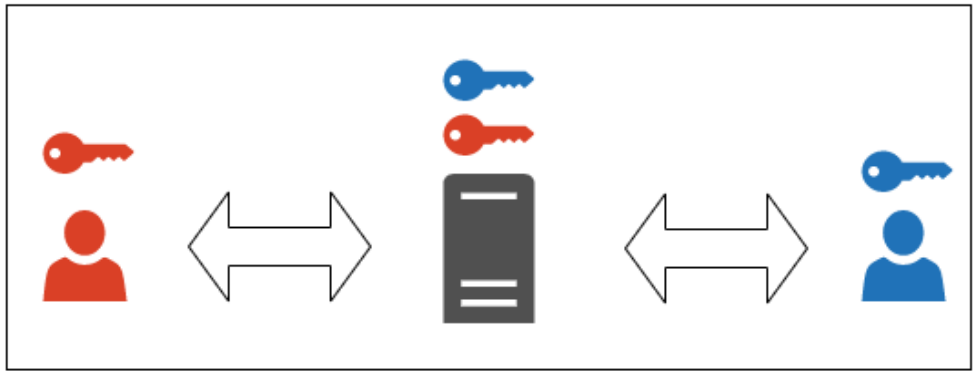
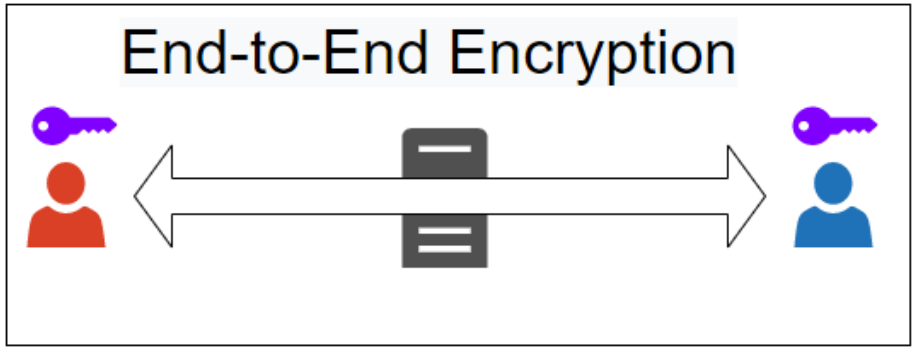
CS808 – Week 3

Dr Rosanne English

Encrypted Communication with Intermediary

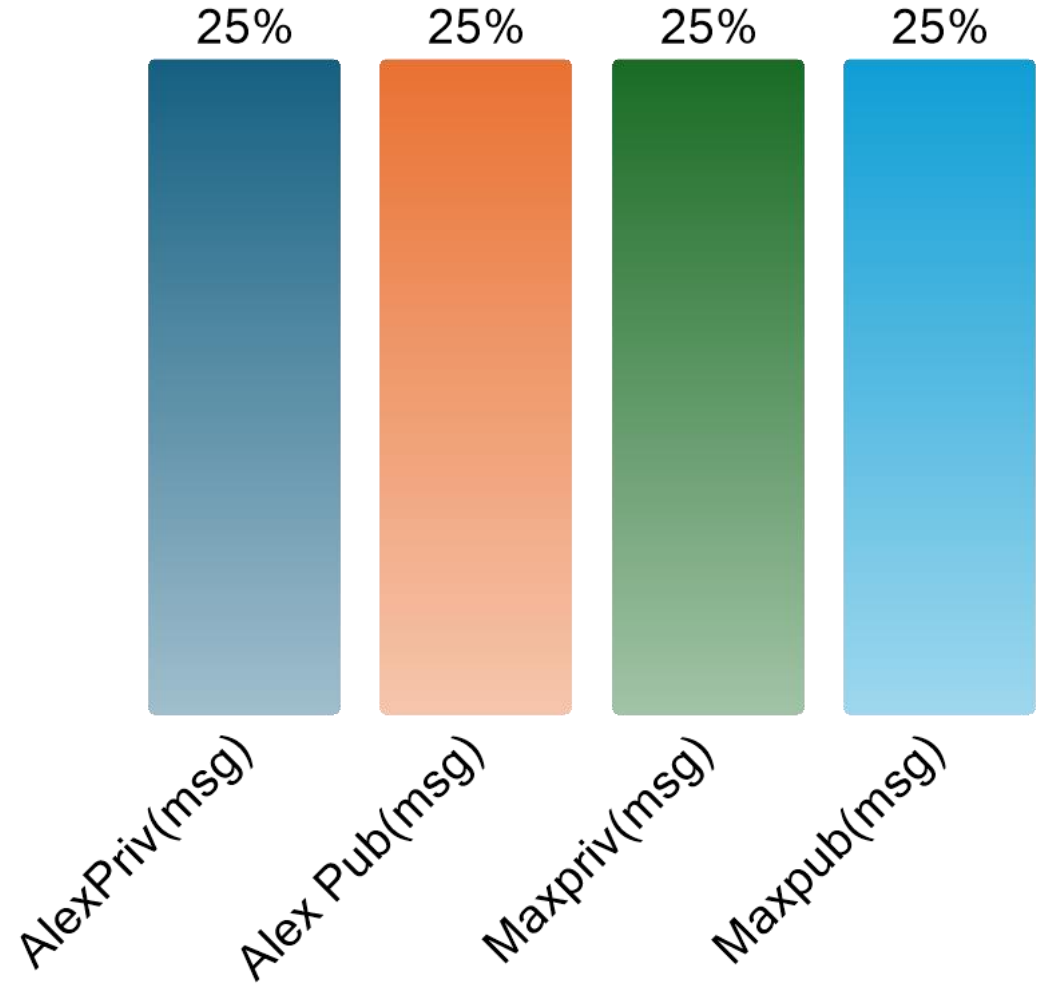


End to End Encryption



You want to send a message to Max which only Max can read. You have your own key pair, and Max's public key. How do you encrypt the message m to achieve this?

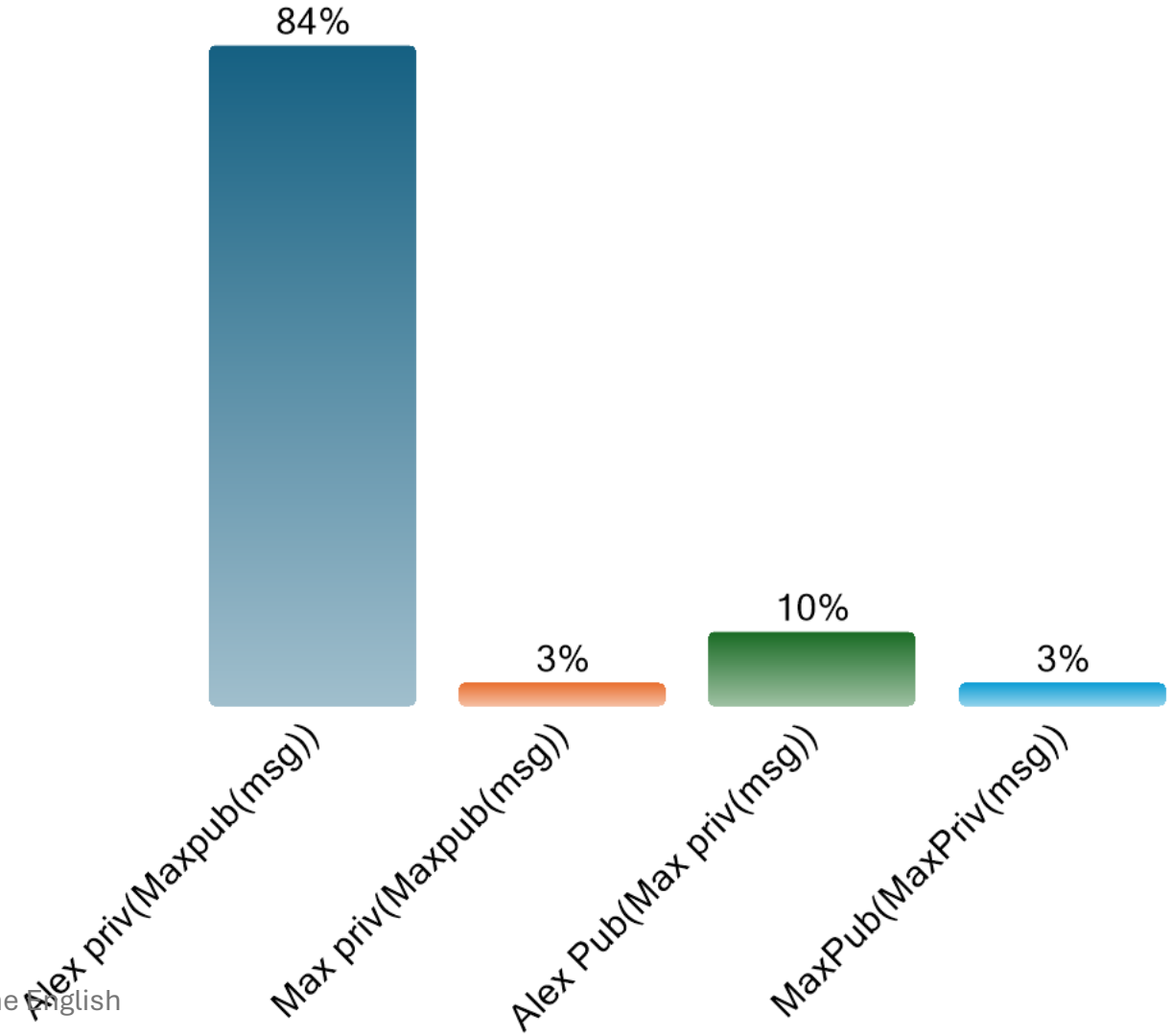
A. AlexPriv(msg)
B. Alex Pub(msg)
C. Maxpriv(msg)
✓ D. Maxpub(msg)



0

Alex wants to send a message such that only Max can read it, but also provide assurance that Alex sent the message. Max has your public key.

✔ A. Alex priv(Maxpub(msg))
B. Max priv(Maxpub(msg))
C. Alex Pub(Max priv(msg))
D. MaxPub(MaxPriv(msg))

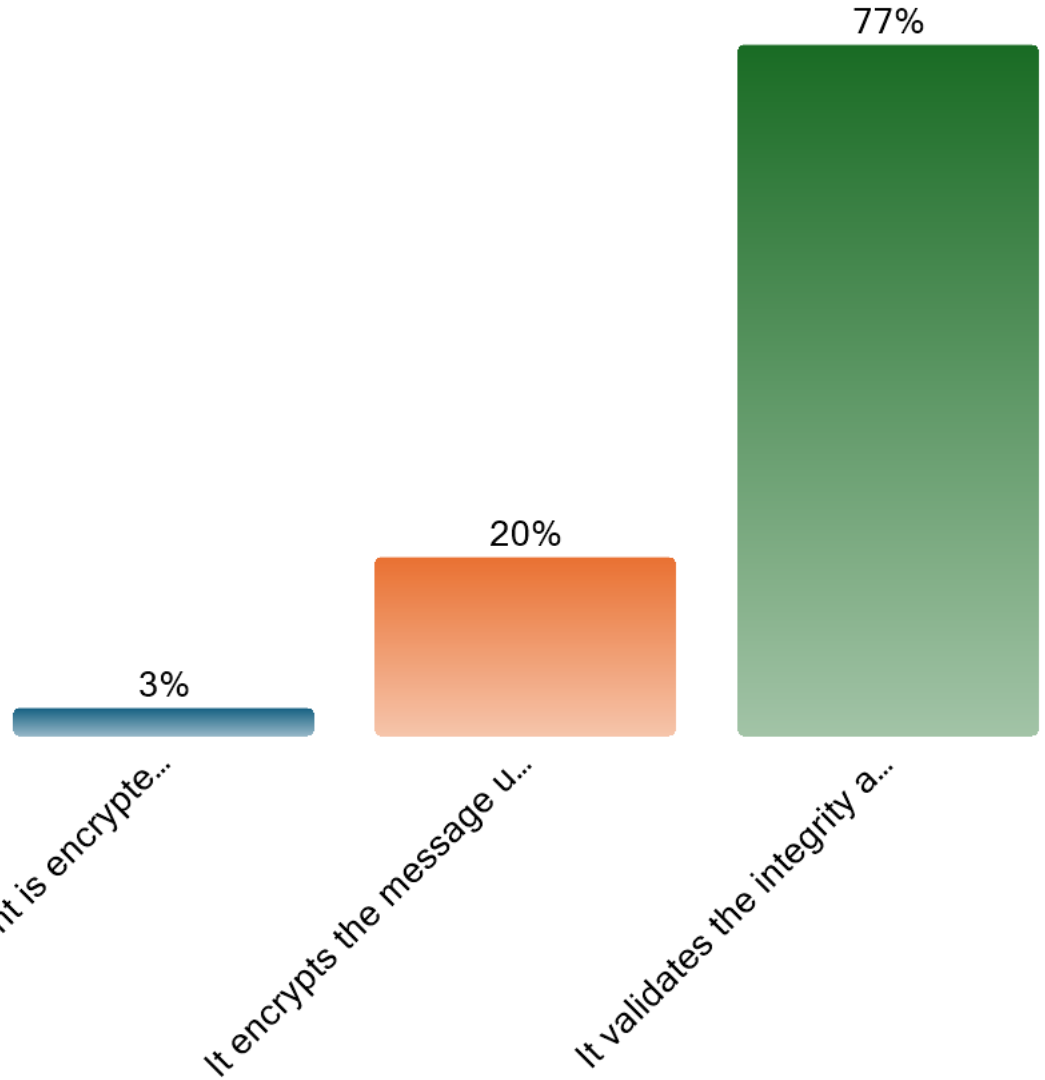


Which of the following best describes how a digital signature mitigates an attack where the attacker replaces the document?

A. The document is encrypted so the attacker can't change it

B. It encrypts the message using a hash function meaning the attacker can't replace it

C. It validates the integrity and authenticity through an encrypted hash ✓



0

Encryption for Different Purposes

- Encrypt with someone else's public key means confidentiality, only the person with the corresponding private key can read it
- Encrypt with your own private key provides confidence in the origin authenticity of the message, only you could encrypt it with the key which corresponds to your public key which will remove the encryption successfully
- Digital signatures – an encrypted hash sent alongside a message, encrypted using the sender's private key [when implementing using Public Key crypto]

SBQ 1

- Alain Thénardiers often uses his company's secure email server. He has lost his private key, but still has the corresponding public key.

a) Is he still able to send encrypted emails? What about receiving?

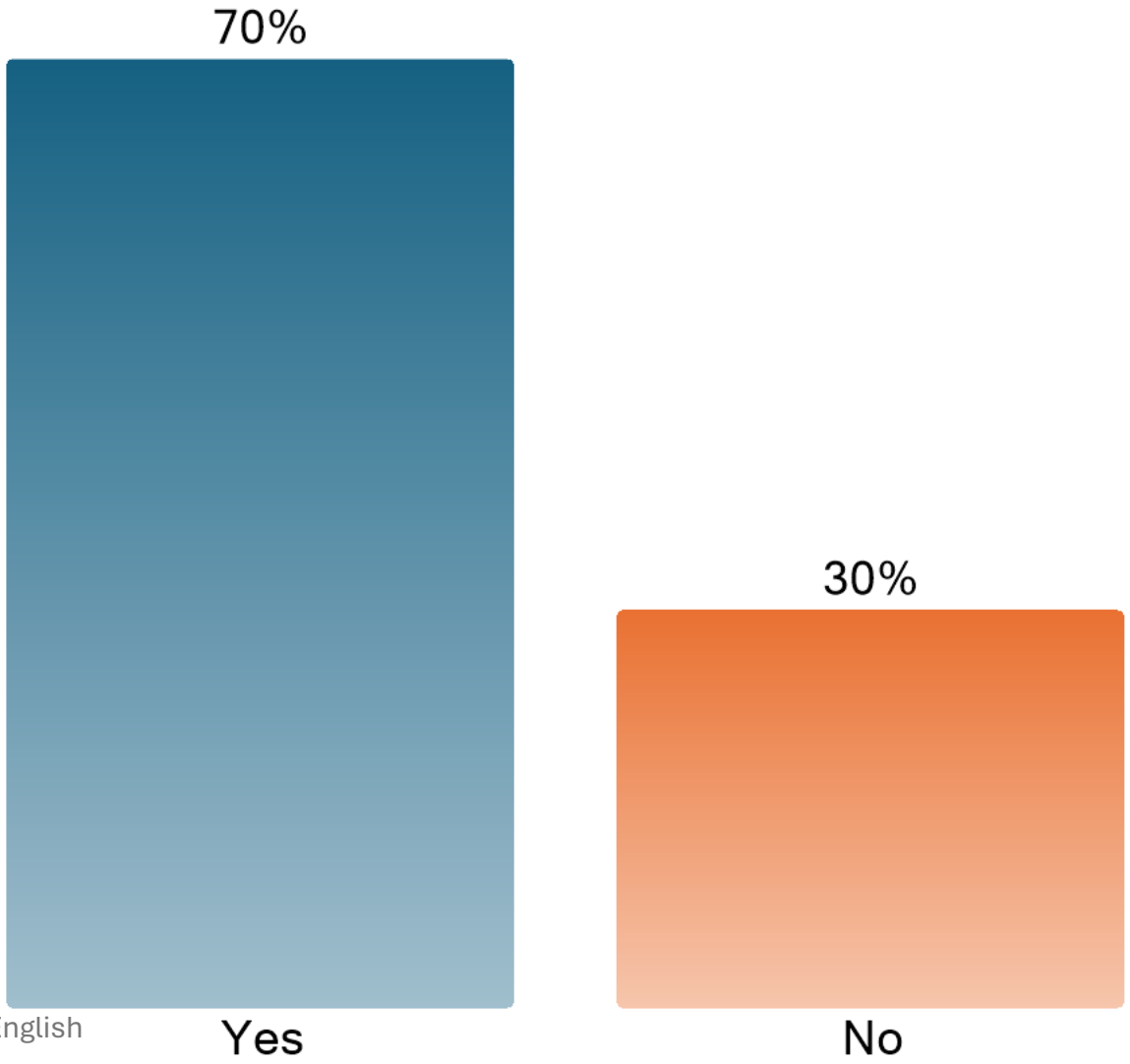
b) Is he still able to sign the email he sends? What about verifying the signatures of emails he received?

c) What must he do to be capable of carrying out all of the operations above?

Can Alain send encrypted emails?

✔A. Yes

B. No



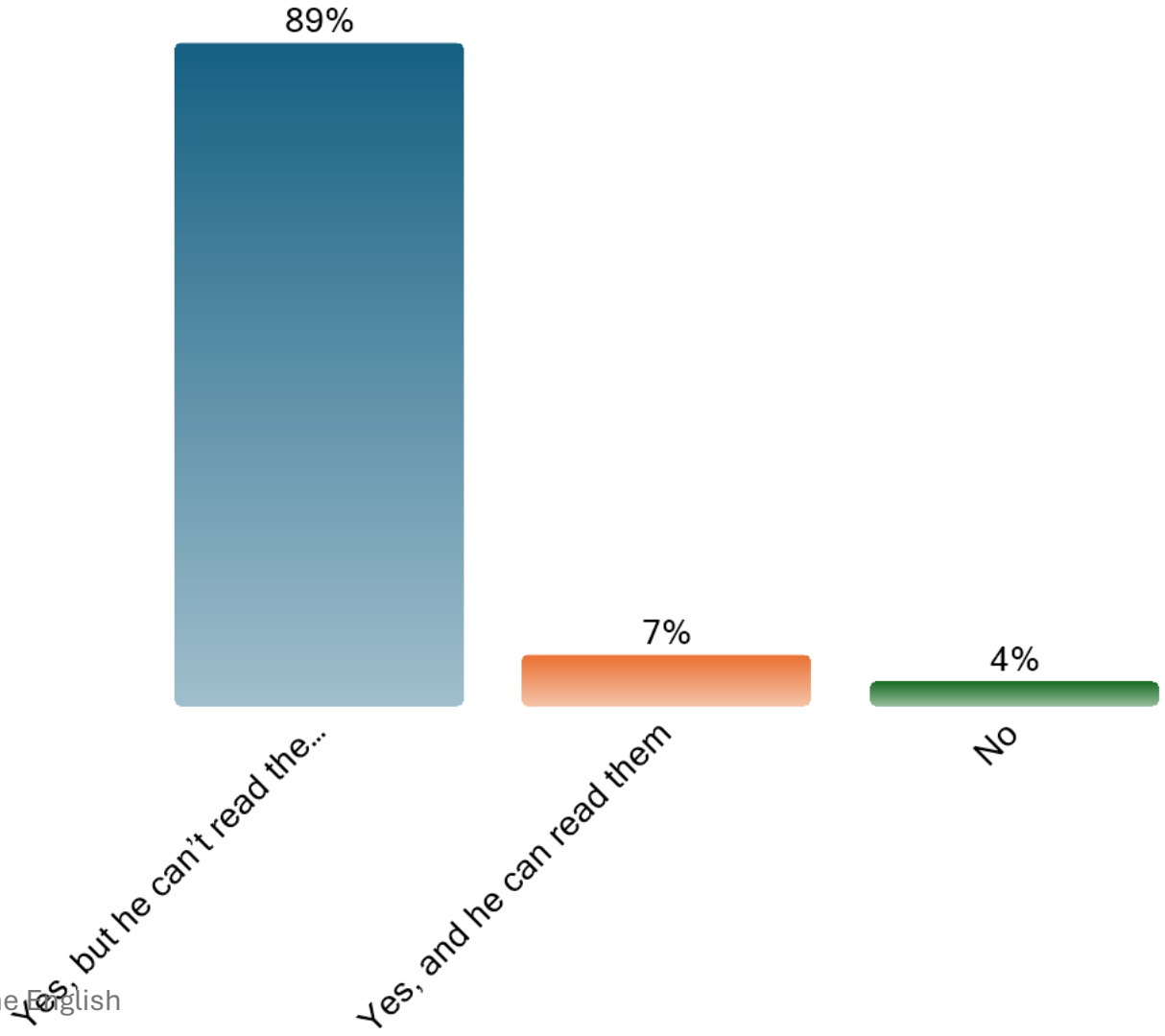
0

Can Alain receive encrypted emails?

✓ A. Yes, but he can't read them

B. Yes, and he can read them

C. No

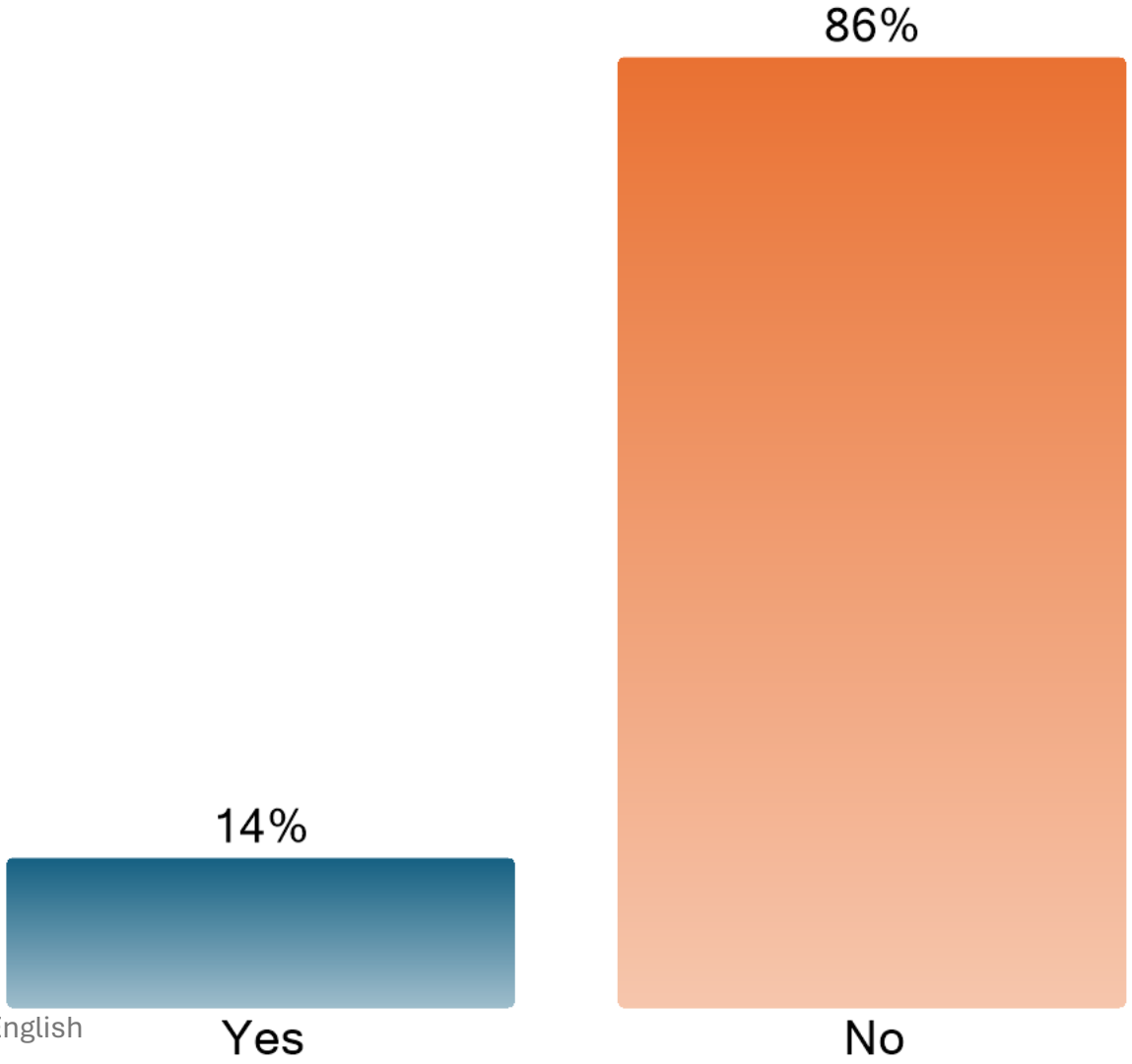


0

Can Alain sign emails he sends?

A. Yes

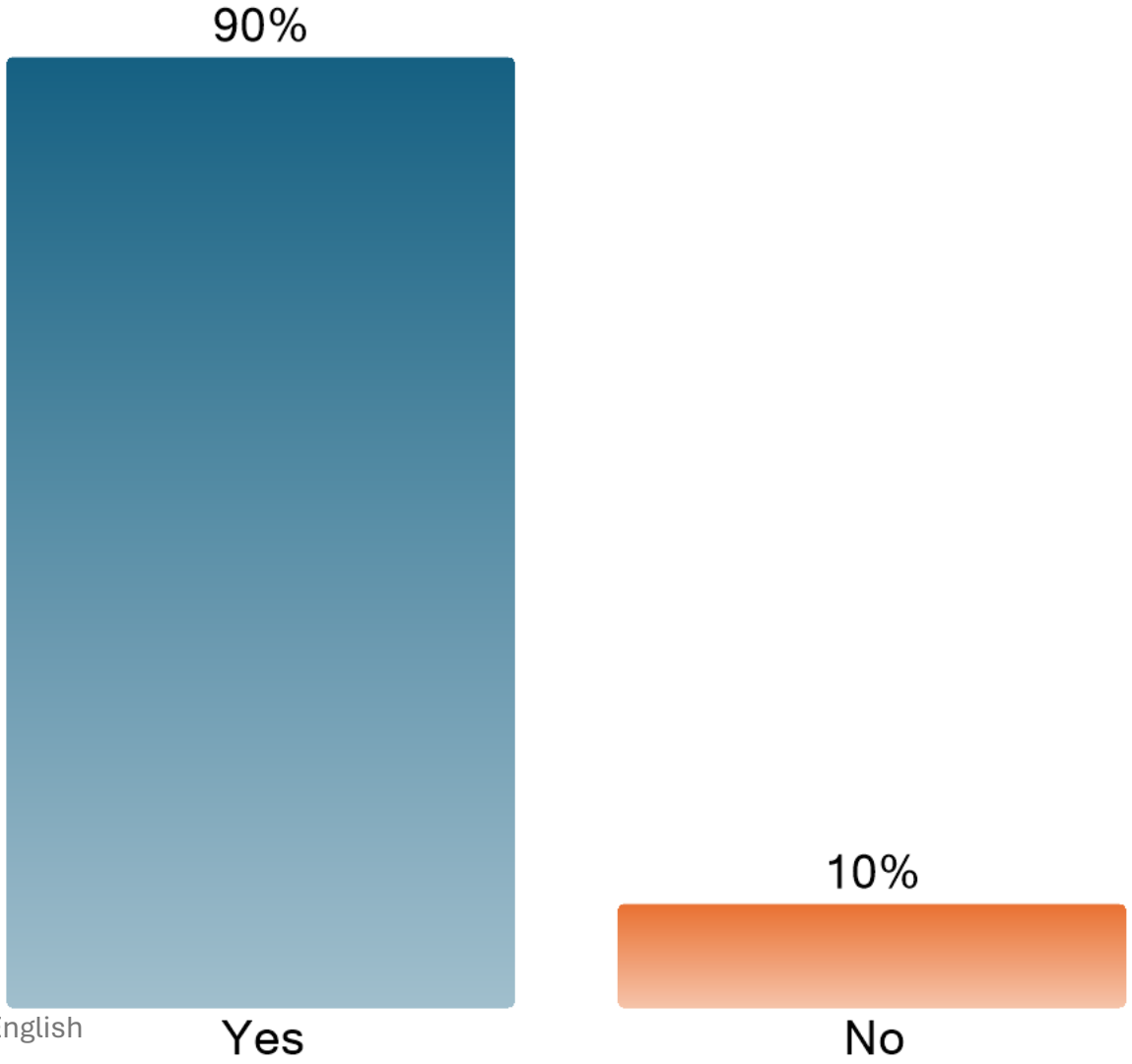
✓ B. No



Can Alain verify signatures he receives?

✔A. Yes

B. No



0

SBQ2

a) Bob would like to send Alice encrypted and signed information. They are both members of the group. What keys must Bob use to achieve this?

b) Name a well-known asymmetric encryption system, explain how it works The group has decided to use a hybrid system – using a combination of asymmetric and symmetric encryption.

c) Why might the group have decided to do this?

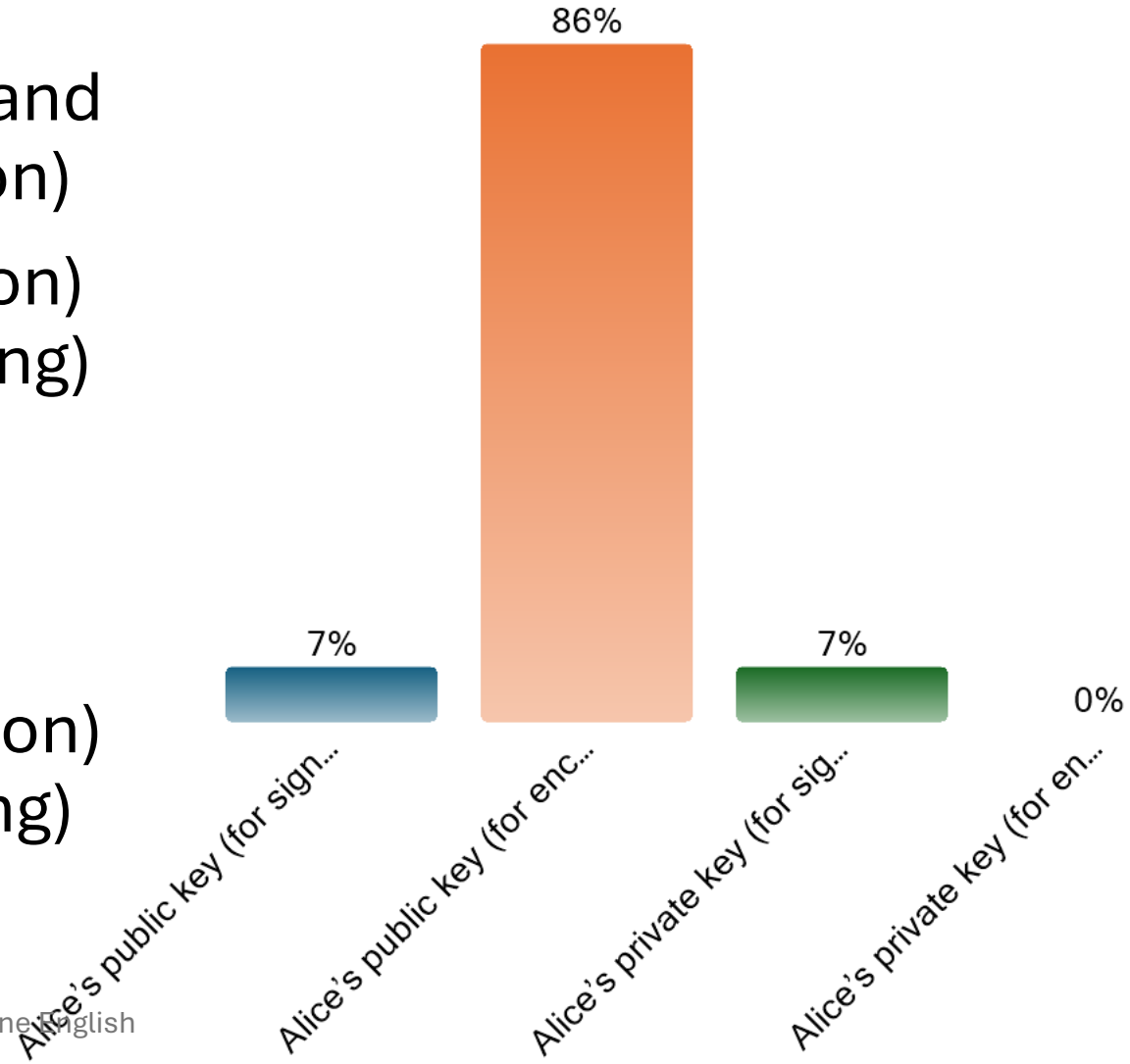
Bob would like to send Alice encrypted and signed information. They are both members of the group. What keys must Bob use to achieve this?

A. Alice's public key (for signing) and Bob's private key (for encryption)

✓ B. Alice's public key (for encryption) and Bob's private key (for signing)

C. Alice's private key (for signing) and Bob's public key (for encryption)

D. Alice's private key (for encryption) and Bob's public key (for signing)



SBQ3

- Not required to complete in an assessment context
- Full worked example will be provided in the solutions guide

SBQ4

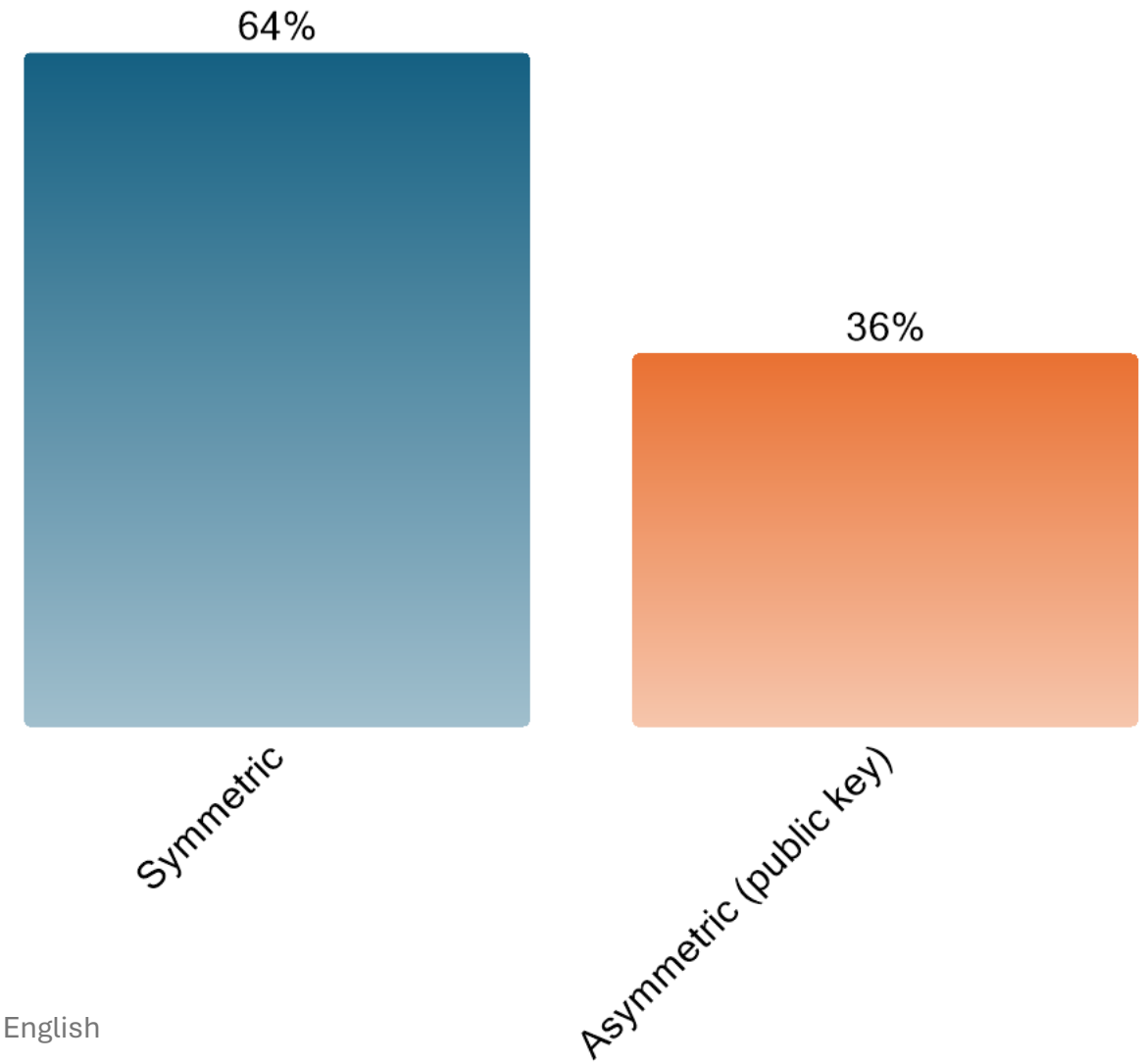
Your friend Miriam (who lives next door) has decided she'd like to share a file with you, but only with you. She's decided to encrypt the file before sending it to you.

a) What type of encryption (symmetric or asymmetric) should she use? Given your choice, propose a specific algorithm and explain to her on a high level how it works.

b) Miriam doesn't know how Diffie-Hellman relates to public key encryption, explain how they are related.

What type of encryption system should Miriam use?

A. Symmetric
B. Asymmetric (public key)



0

How does Diffie Hellman relate to Public key crypto?

key sharing problem

encryption