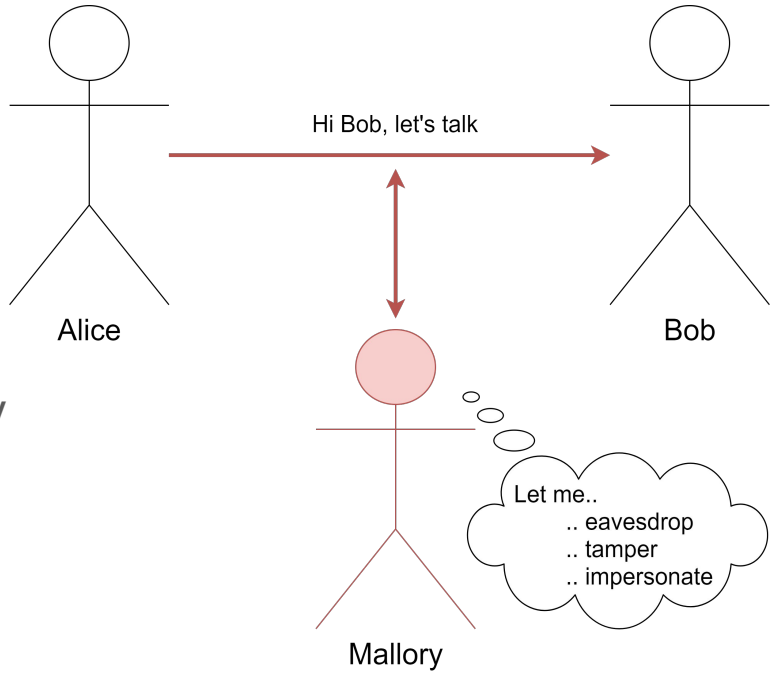
Asymmetric Cryptography

Scenario

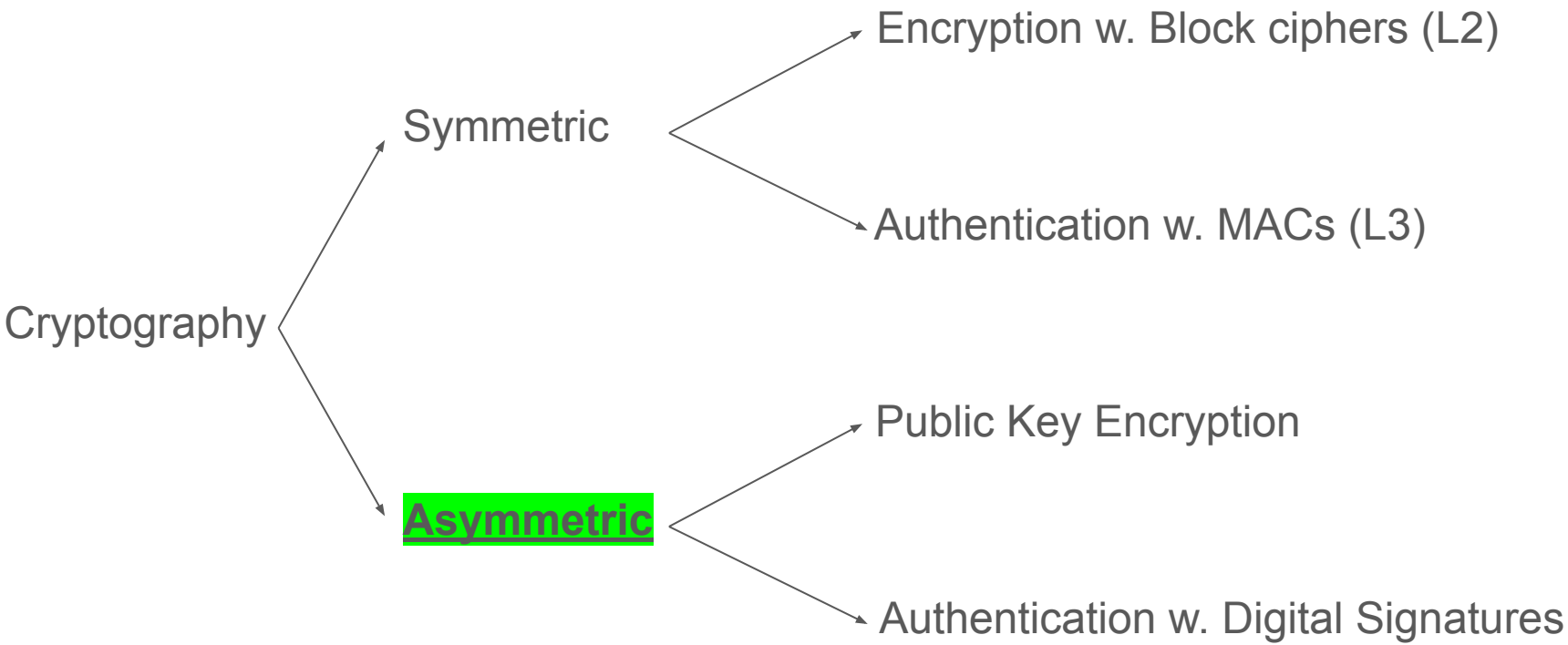
Alice and Bob want to communicate securely, i.e., encrypt/authenticate the traffic, over an unprotected communication channel, e.g., Internet

.. but they talk for the first time and they do not share a symmetric secret key, meaning that they cannot use symmetric cryptography (block ciphers, MACs, etc.)

Example: when you first visit a website



Encryption classification

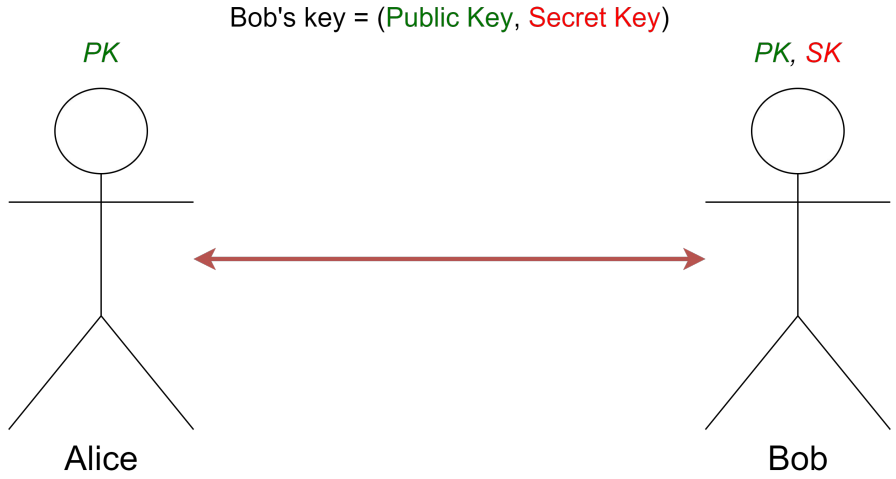


Asymmetric cryptography

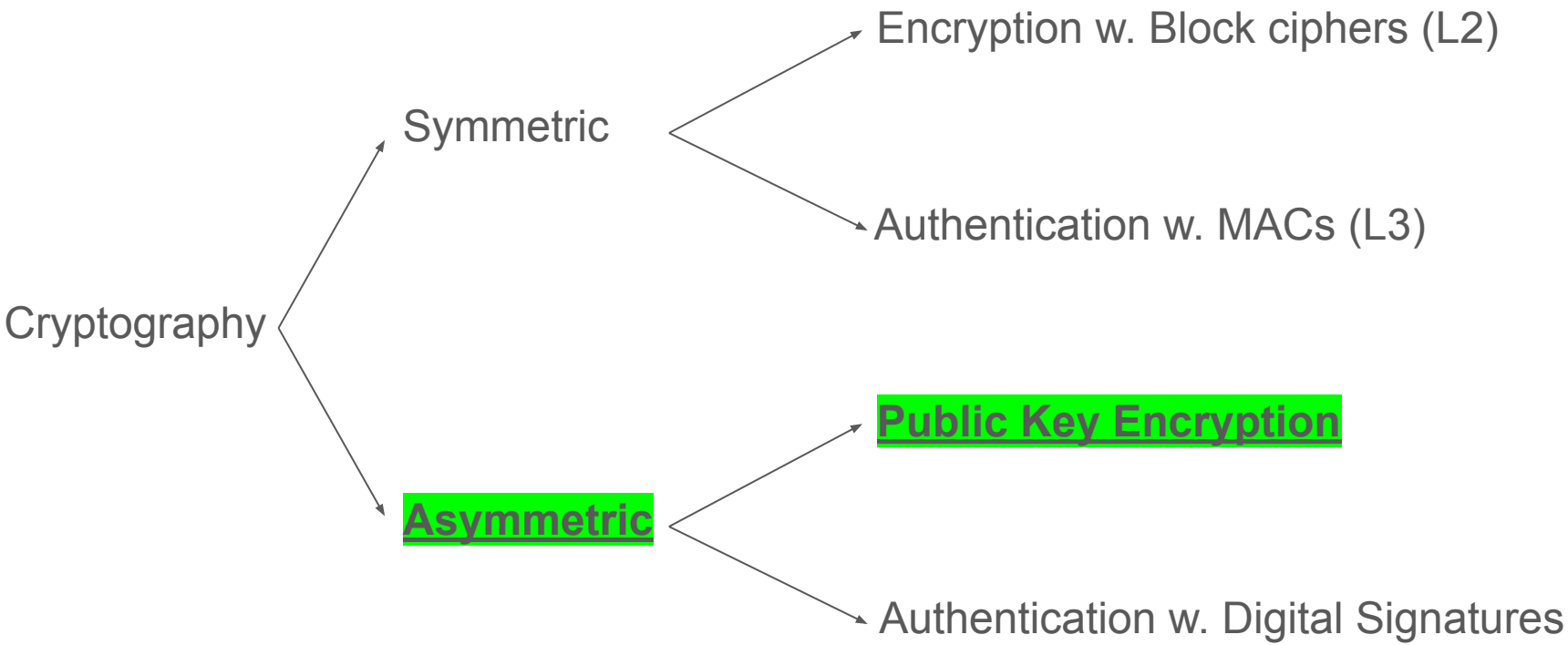
Main idea: use different keys for encryption/authentication

Asymmetric key

- Public part (known by everybody)
- Secret part (known only by the owner)



Encryption classification



Public key encryption schemes

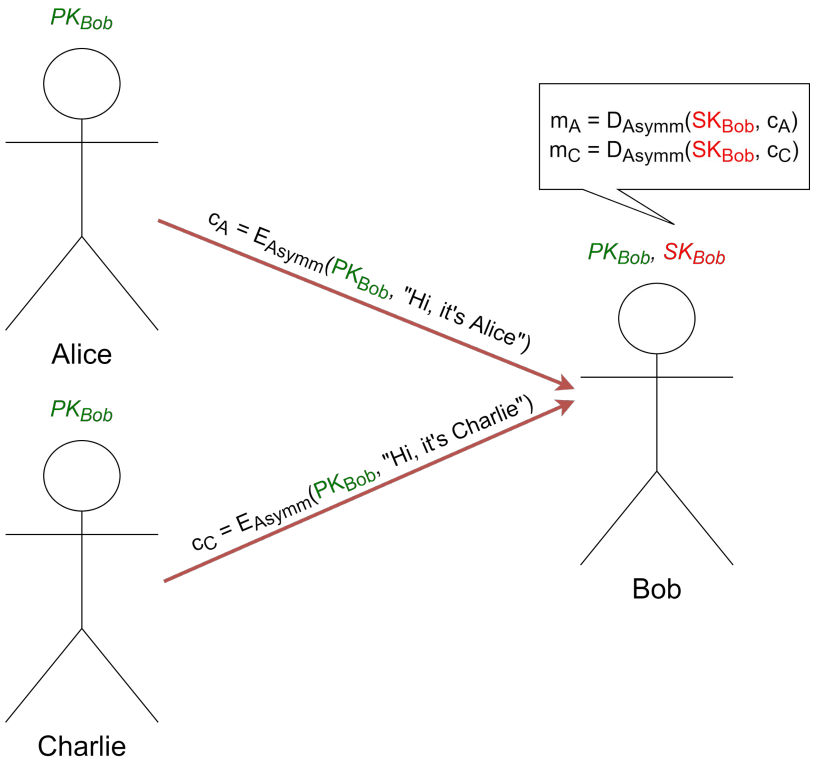
Main idea: Everybody can encrypt a message using the public key, but only the owner of the secret key can decrypt them

Encryption algorithm

- Takes as input the public key and the message
- Outputs the ciphertext

Decryption algorithm

- Takes as input the secret key and the ciphertext
- Outputs the original message



Public key encryption schemes (cont.)

Anyone else

- Can encrypt messages
- Can not decrypt any messages

Key owner

- Can decrypt all messages

Public key encryption in practice

Example of cryptosystem: RSA

Used in protocols such as SSL/TLS (discussed in other lab)

- usually to establish a symmetric key (**why?**)

Public key encryption in practice

Example of cryptosystem: RSA

Used in protocols such as SSL/TLS (discussed in other lab)

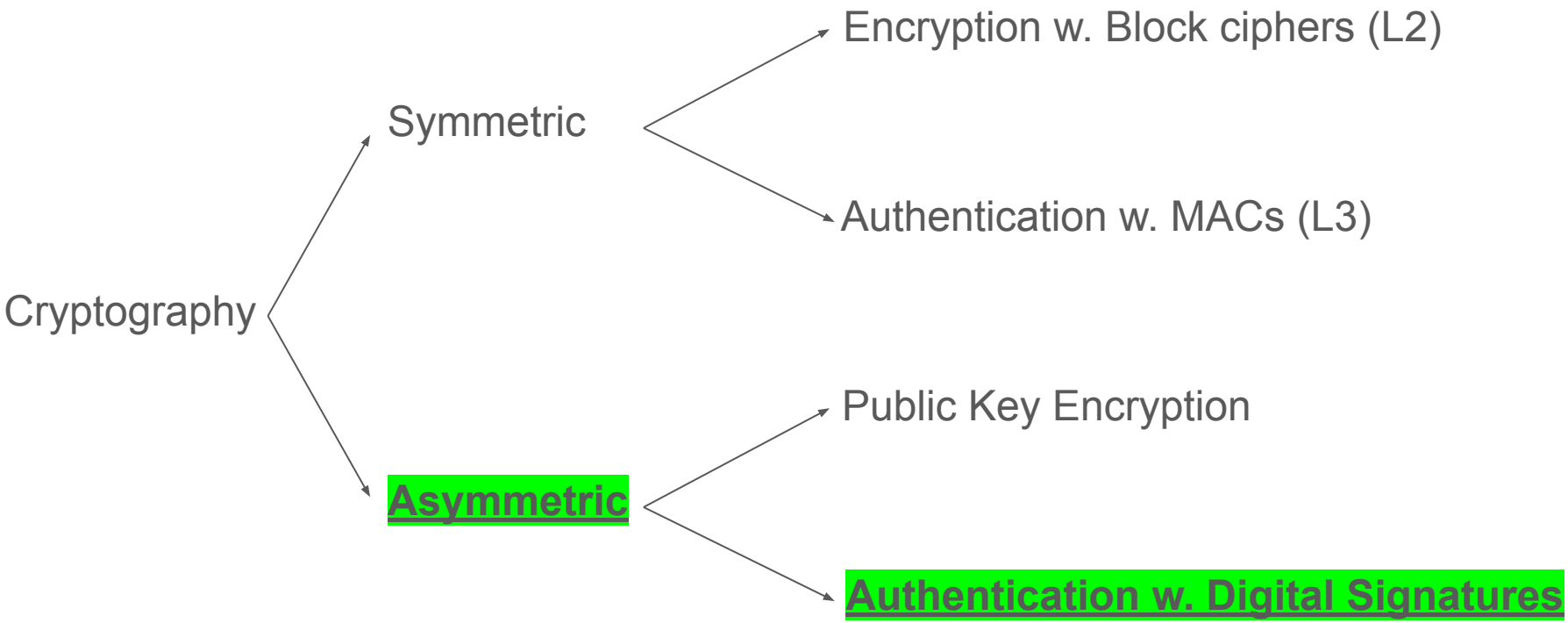
- usually to establish a symmetric key (**why?**)

Some advantages of symmetric encryption

- Much faster (usually accelerated with HW as well)
- Smaller footprint

Let’s test!

Encryption classification



Digital signatures

Main idea: a method of singing digital data

Q: Is it secure to sign a document by reproducing your real-world signature in a drawing program (e.g. Paint) ?

Digital signatures

Main idea: a method of singing digital data

Q: Is it secure to sign a document by reproducing your real-world signature in a drawing program (e.g. Paint) ?

No, anyone may copy your signature and paste it on other documents

Working principle

- To avoid forgeries, the digital signatures are computed using a secret key and the data to be signed, i.e., only the secret key owner can sign data
- Using the public key, anybody can verify the signatures

Digital signatures (cont.)

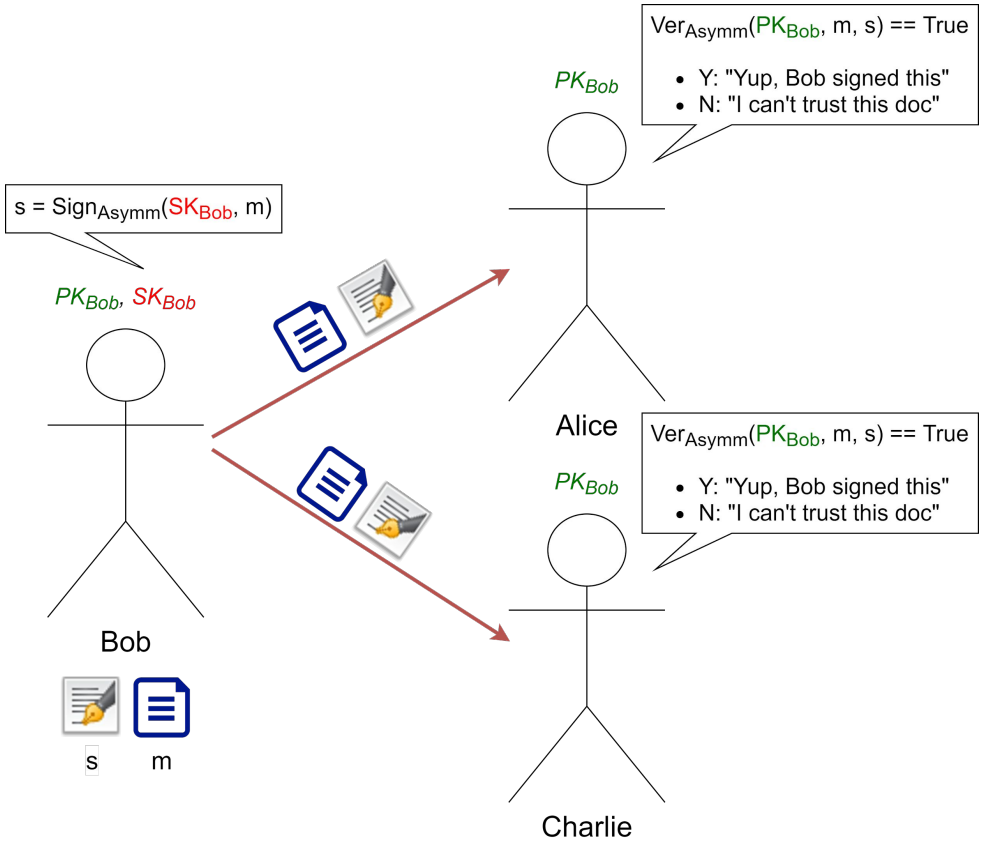
Signing algorithm

- Takes as input the message and the secret key
- Outputs a digital signature

Verification algorithm

- Takes as input the message, signature and public key
- Outputs true if verification succeeds, otherwise false

Example of algorithms: RSA, DSA



Digital signatures (cont.)

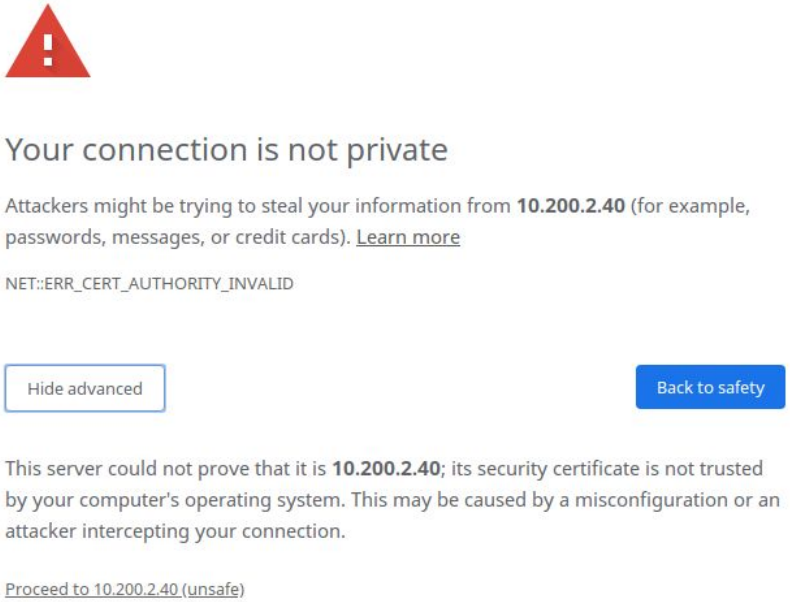
Anyone else

- Can verify signatures
- Can not sign data

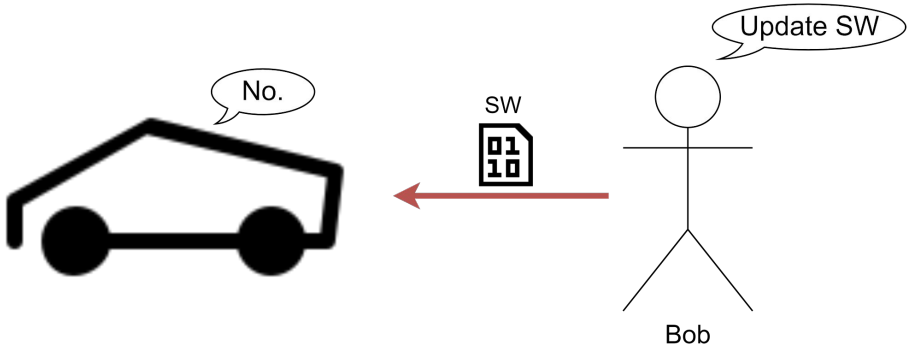
Key owner

- Can sign data

Authentication w. digital signatures in practice



Authentication w. digital signatures in practice (cont.)



Authentication w. digital signatures in practice (cont.)