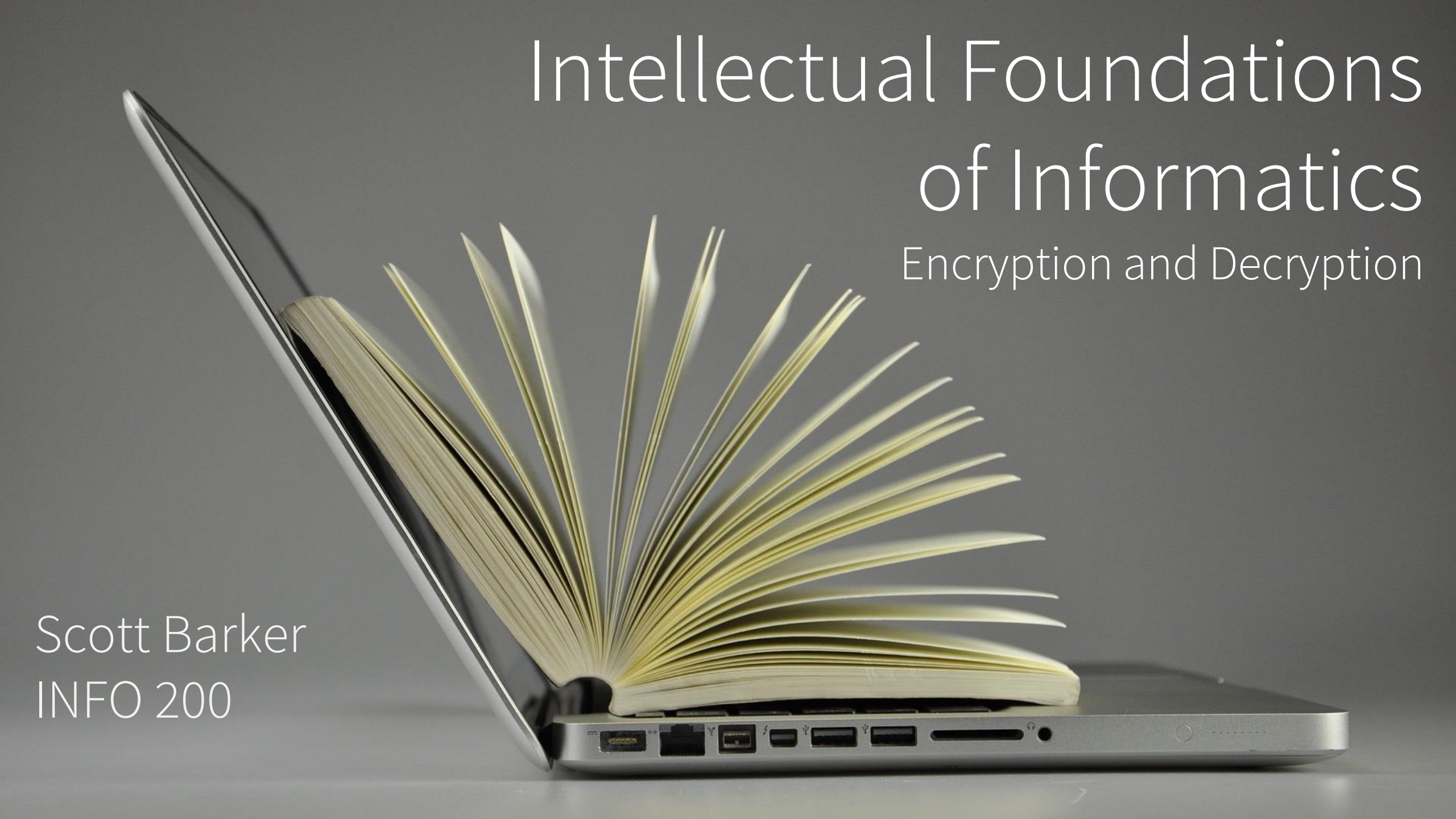
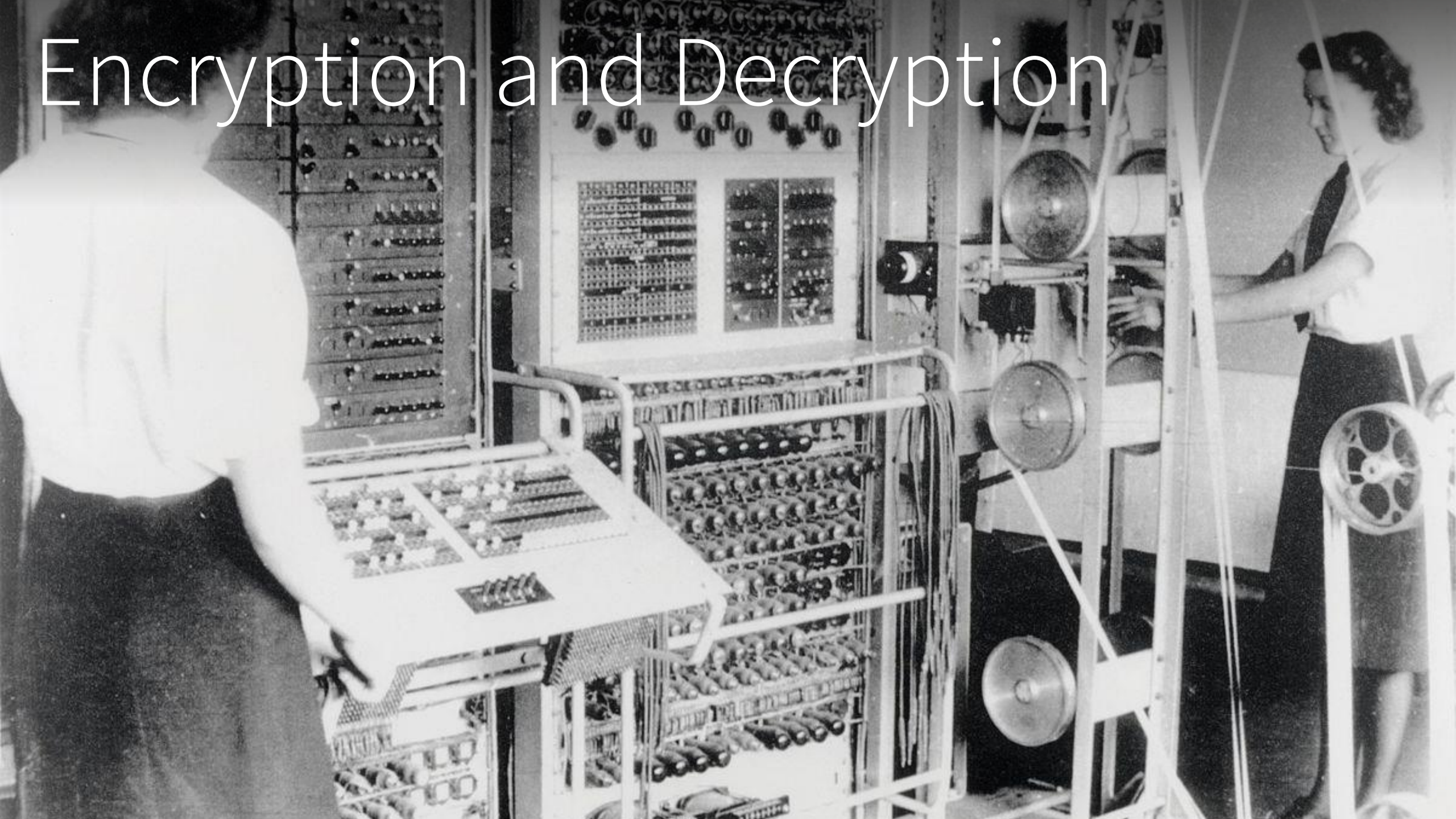
Intellectual Foundations of Informatics

Encryption and Decryption



Scott Barker
INFO 200

Encryption and Decryption



Our goal is to protect both data-at-rest and data-in-flight

Authentication and authorization can help for data-at-rest

Cryptography (encryption) can also be used to protect data at rest, as well as data in flight

Encryption

The process of encoding information or a message in such a way that only authorized parties can read it

- The original message is typically referred to as plaintext
- The encryption is performed by an algorithm or cipher
- The resulting message is known as ciphertext or a cryptogram

To decrypt the message (assuming use of a strong encryption algorithm) you need a key

Decryption might also be possible by guessing

Looking for common letters, words, frequency of letters lengths of words etc.

There are two types of encryption and decryption – symmetric and asymetric

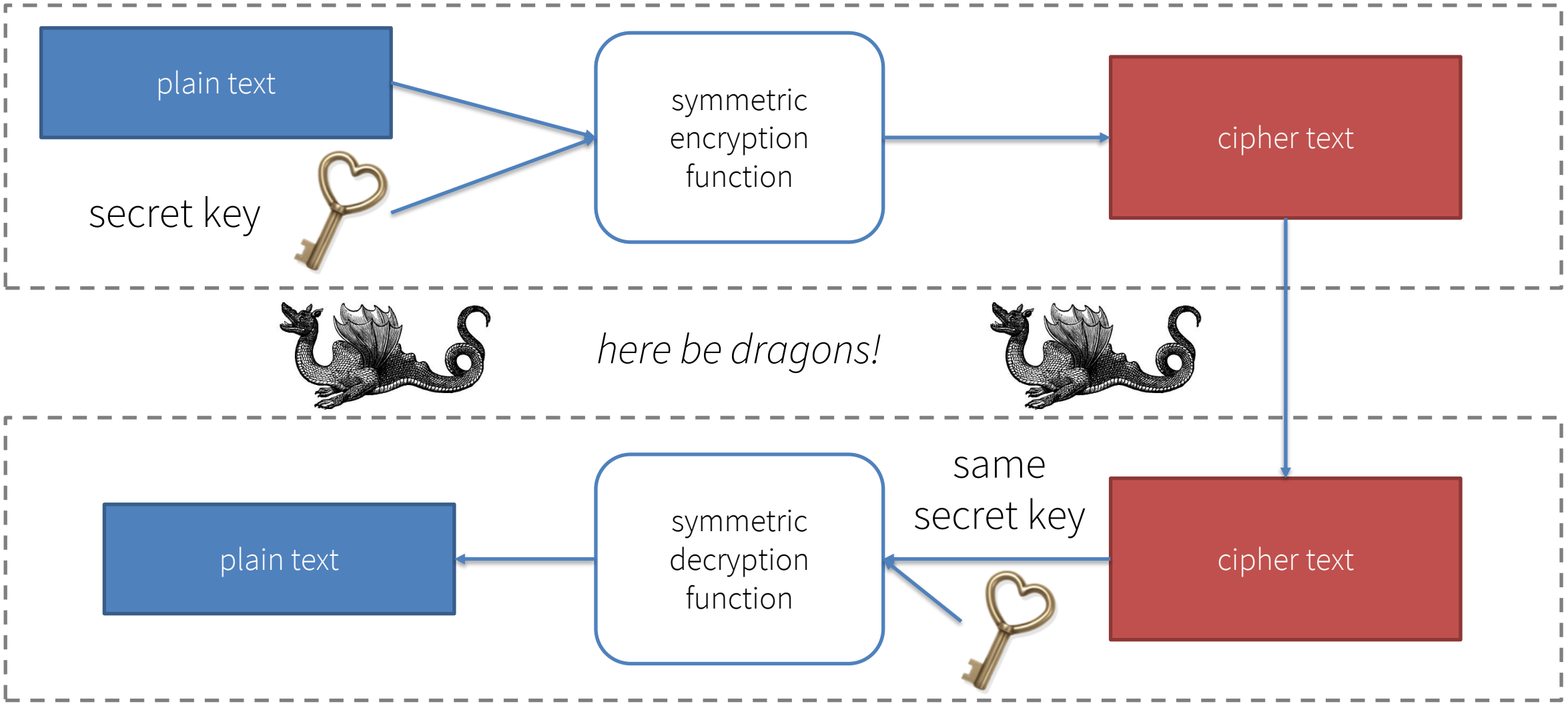
Cryptography Basics Video

Symmetric Encryption & Decryption

encrypt and decrypt
with same key

- Oldest and best known system, typically very fast
- Keys must be kept secret by both parties
- What if the key is discovered?
  Messages could be read by un-authorized parties
  New messages could be sent using that key by unauthorized parties
- Big problem - how does each party know the key if they are located at a distance or over the Internet?
  This is known as the key distribution problem

Symmetric Encryption



Full Disk Encryption

Uses symmetric encryption and especially useful on enterprise laptops or USB drives that store important corporate data. Provides extra security should that device be stolen

Bitlocker – Windows

FileVault – MacOS. Newer Macs with a “T2” chip encrypt automatically

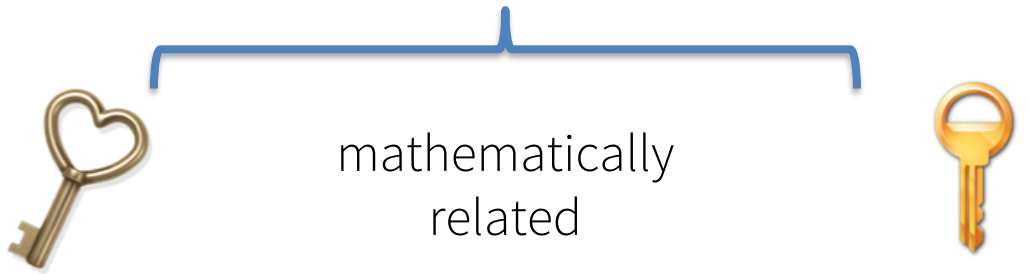
Many newer hard drives are “self-encrypting”, have a dedicated chip on it to do the encryption, doesn’t rely on software

Many Smart phones today do full disk encryption by default including iPhones, and they typically guard against brute force PIN guessing by locking the device

Law enforcement is generally not happy about full disk encryption

Asymmetric Encryption & Decryption

A **pair of keys** are required by each participant (the sender and receiver)
This pair of keys is generated at the same time, they are mathematically related

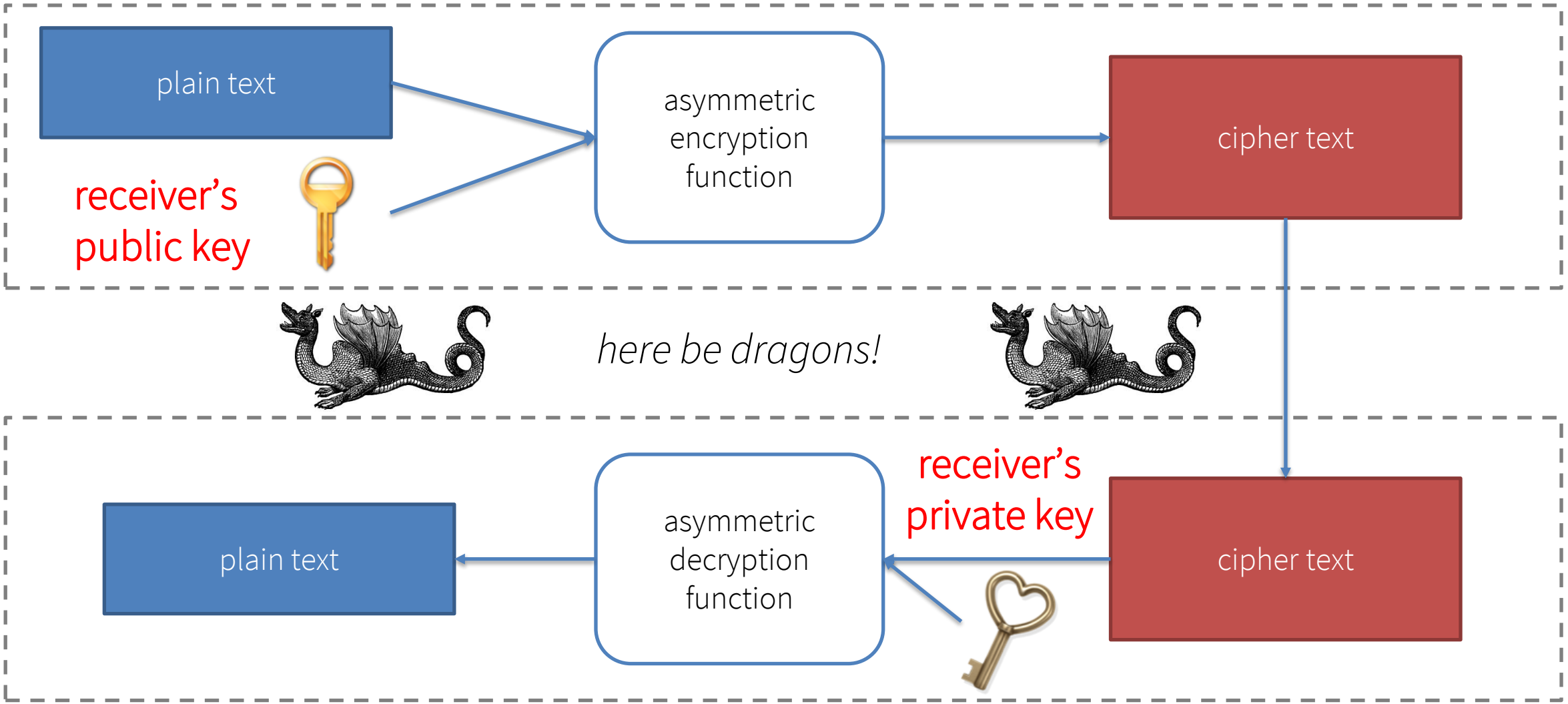


I have a private key that no one but me knows. I have a public key that I can share with the world. Same with the receiver.

Can encrypt with either key but decrypt only with the other

Typically the sender encrypts a message using the receivers public key and the receiver decrypts with their private key

Asymmetric Encryption



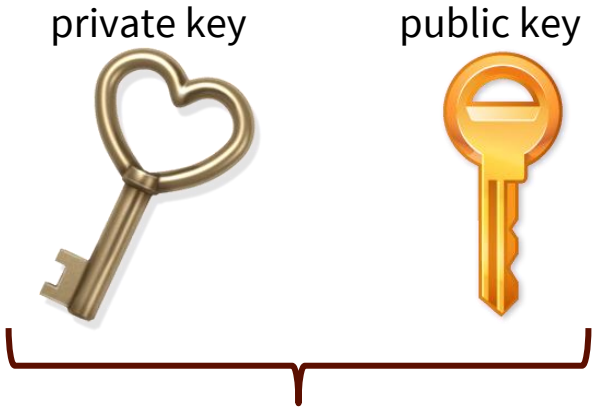
Symmetric

encrypt and decrypt using the **same key**

"keys" are very big binary values (currently 256 bits)

Fast; message can be unlimited in size

Asymmetric



key pair: encrypt with either key but must decrypt with the other key

slower

Public/Private Key Cryptography Explained

Putting it all together

How https works to protect information “in flight”

End Lecture