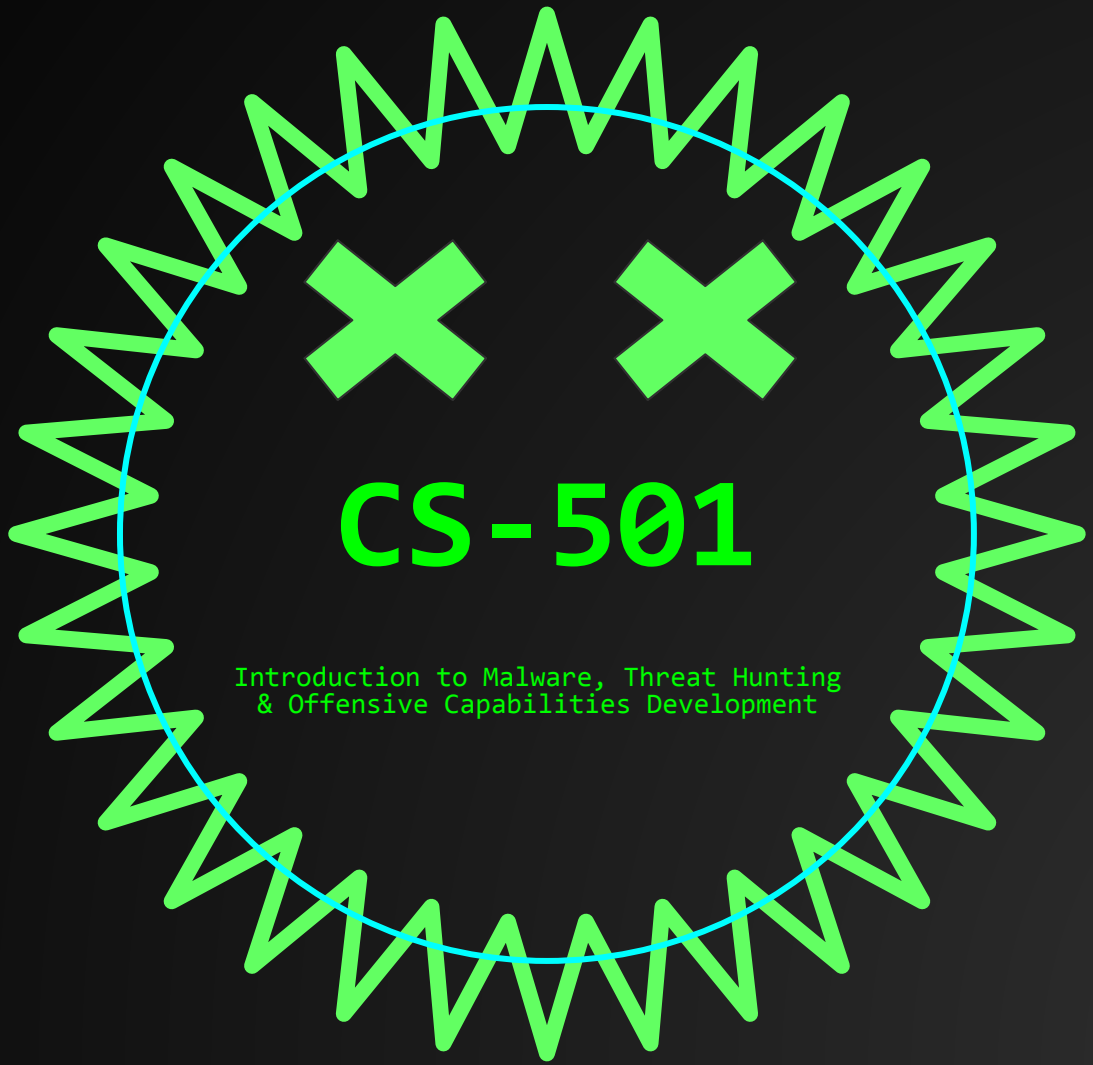


CS-501

Introduction to Malware, Threat Hunting
& Offensive Capabilities Development

Lecture 16
Asymmetric Crypto

Asymmetric Cryptography

AKA (Public Key Cryptography)

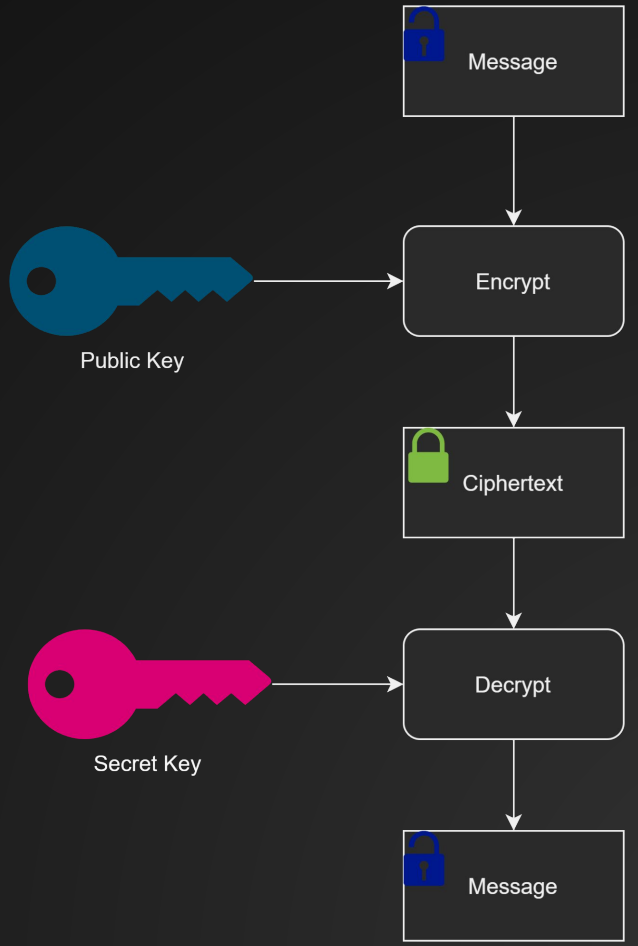
How do we securely communicate with someone we have never met before?

Classic example: how does your browser establish a secure connection with google.com?

Public Key Encryption

Anybody with the public key can encrypt messages

Only the owner of the private key can decrypt messages



Examples

RSA

El Gamal

Various using Elliptic Curves

Crowded Room Key sharing

Cryptography is magic

Imagine walking into a crowded room and shouting something at your friend.

Your friend hears you, shouts something back, and you miraculously walk away with a secret key.

In particular, it is secret from everyone else in the room!

What does this look like in practice? Glad you asked…

Diffie Hellman

- Based on the Discrete Logarithm problem, + some other assumptions
- How does it work…?