Asymmetric Cryptography and Digital Signature

If I were again beginning my studies, I would follow the advice of Plato and start with mathematics.

-Galileo Galilei

Cybersecurity
Cryptography Day 2

Today’s Objectives

By the end of class, you will be able to:

- [ ] Compare and contrast block and stream ciphers.
- [ ] Describe how public-key cryptography uses a key pair for encryption and decryption.
- [ ] Use the command line program GPC to encrypt and sign documents with public and private keys.
- [ ] Determine how digital signatures use private and public keys to generate and verify signatures.
- [ ] Describe how digital certificates verify digital entities.

Activity: Cryptography Refresher

In this activity, you'll review the topics covered last class.

Activities/Stu_Review/README.md

Suggested Time:
7 Minutes

Block vs. Stream Cipher

Block vs. Stream Ciphers

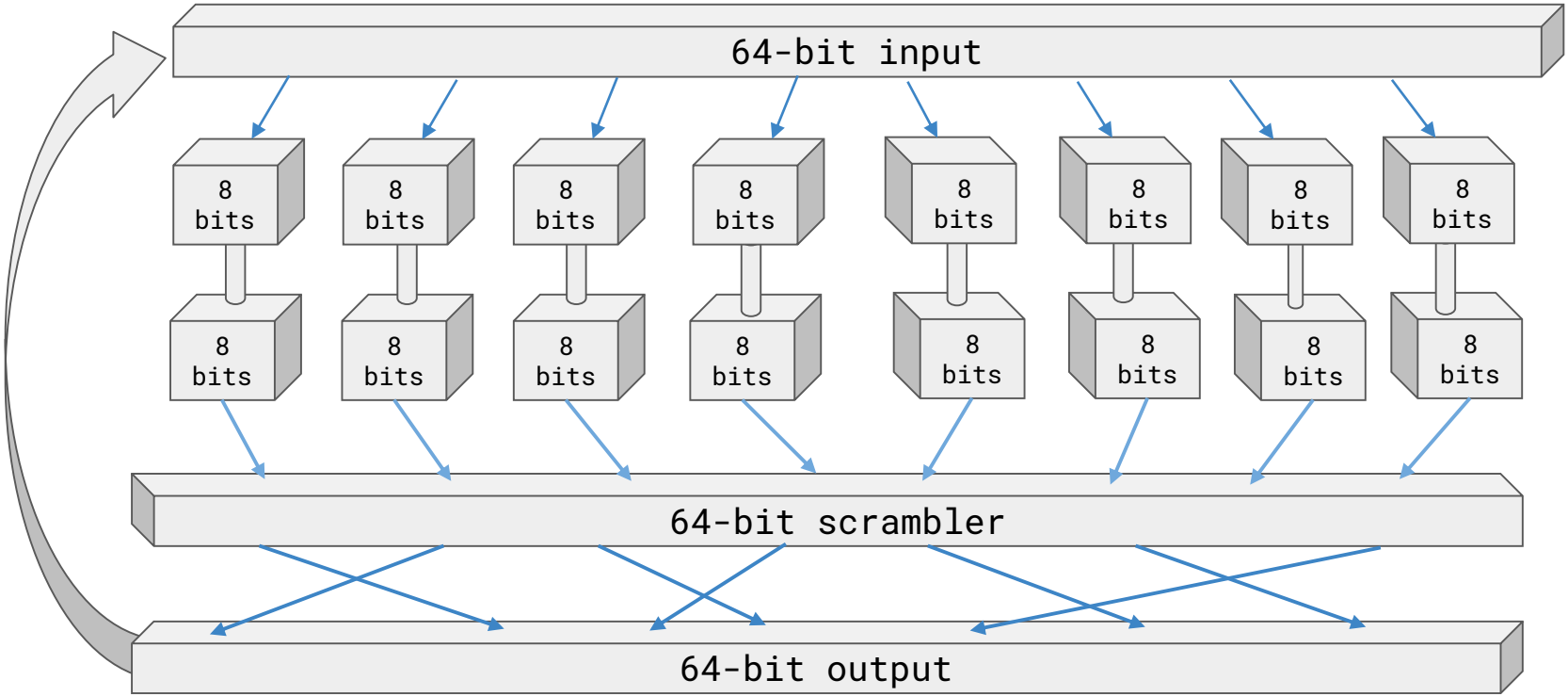
Modern ciphers can operate on bits in either block mode or stream mode.

Block cipher mode breaks input data into a block of fixed size, perform encryptions on the bits of each block separately, and then combine the results to generate their final output.

Stream cipher mode encrypts each bit mone at a time without decomposing the input stream into blocks.

Block Ciphers

Block ciphers breaks input data into fixed-sized blocks and then encrypt each block separately.



The larger the block size, the stronger the encryption.

Padding

Sometime, you'll want to encrypt 254 bits in a 256-bit block size encryption, But block ciphers must work with data that fits exactly within a block algorithm.

Padding bits is the process of adding bits to the end of a message to "fill out" the space discrepancy between a short message and the block size.

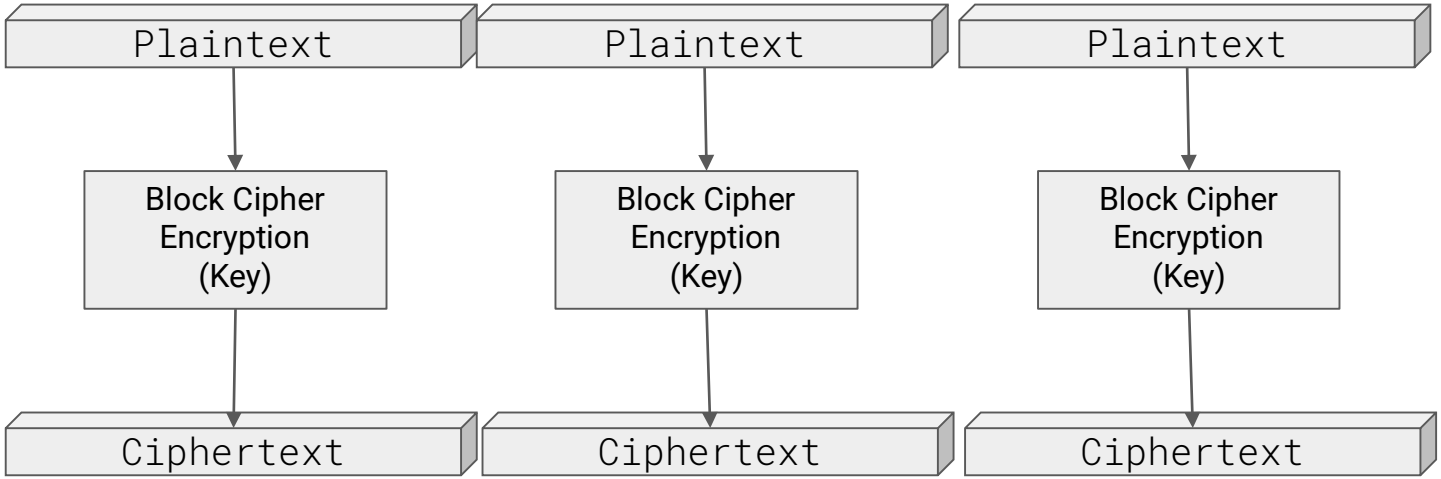
PSCK5/7 is the most common method of padding, the process of padding a short message with the number of bytes left to fill:

Padding a 6-bit message in an 8-bit block: `hello!\x02\x02`

Padding a 4-bit message in an 8-bit block: `hey!\x04\x04\x04\x04`

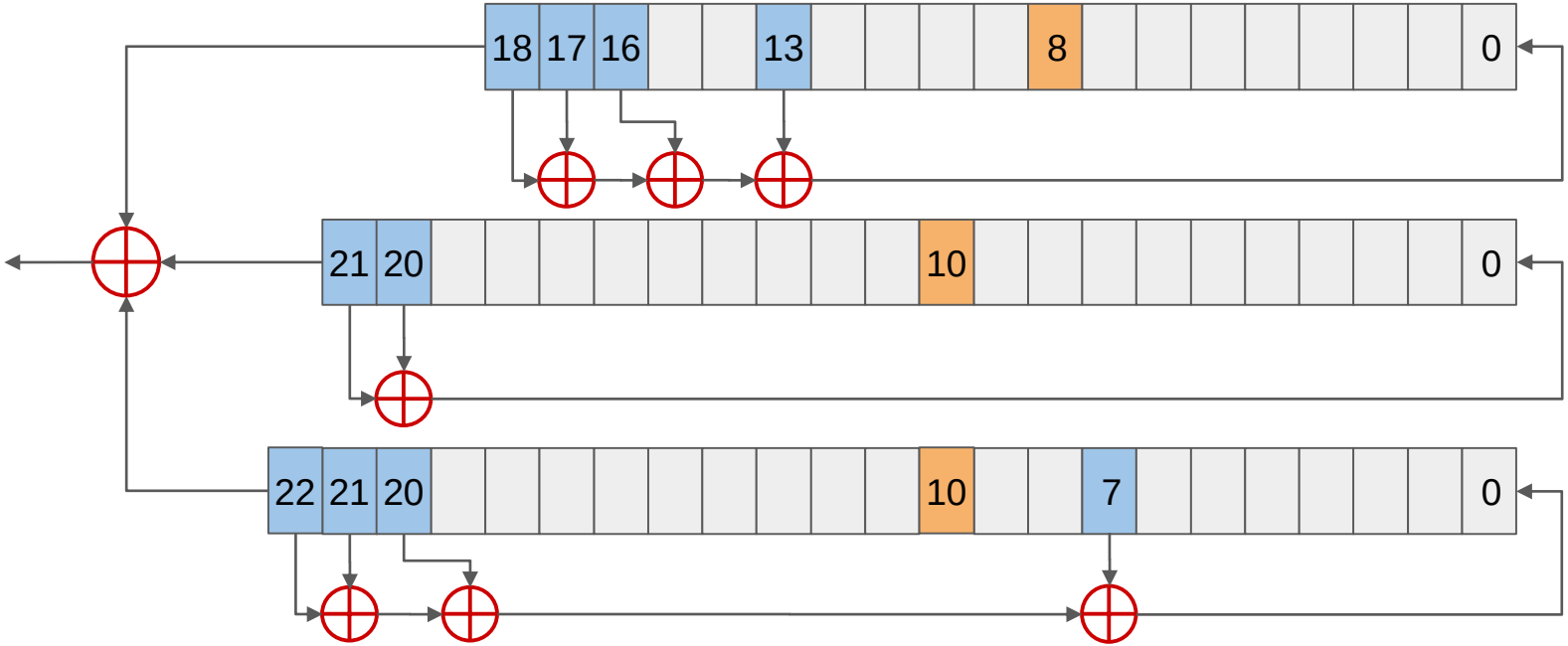
Block Ciphers in Stream Mode

Breaking data into chunks equal to the algorithm block size, encrypt each block, and concatenate the results.



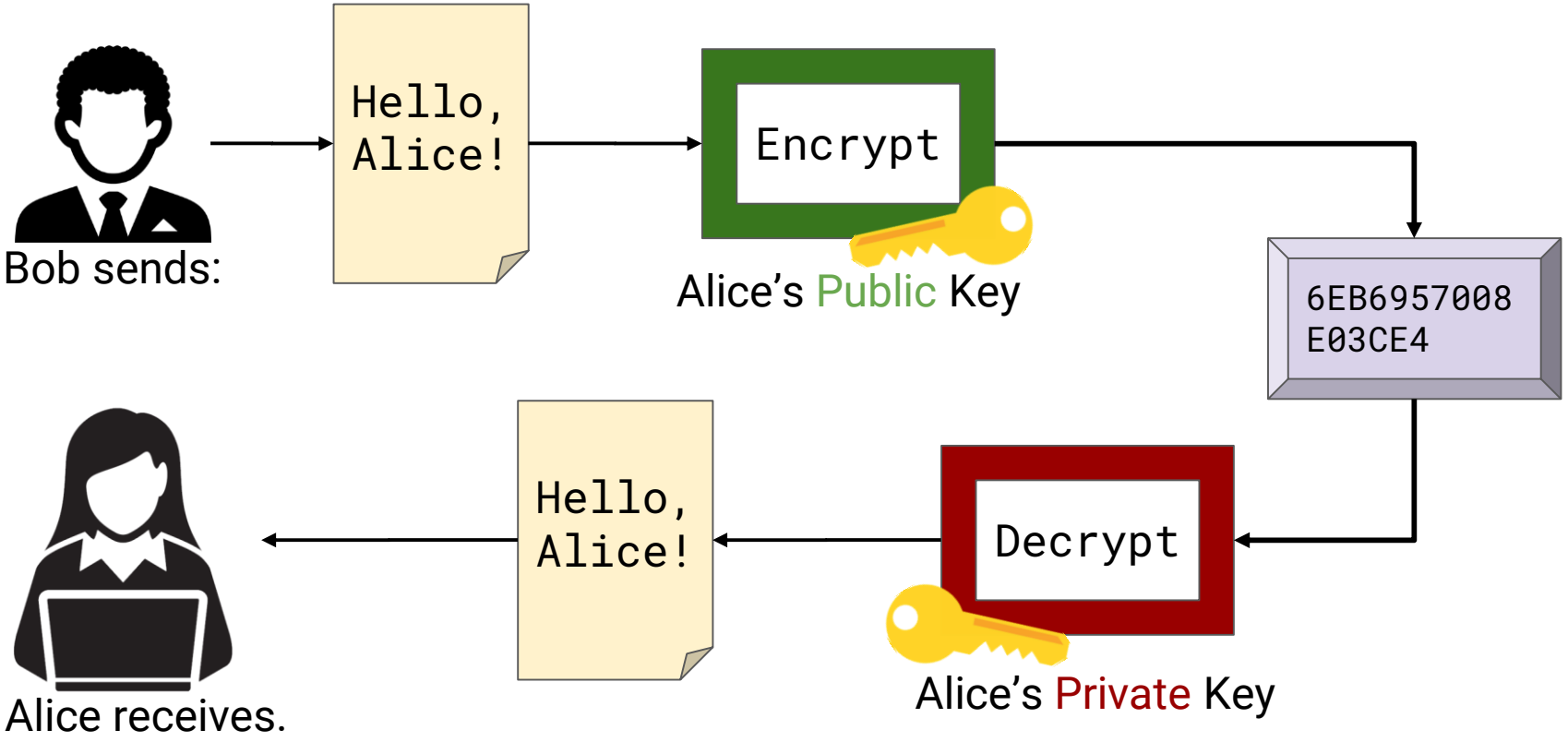
Stream Ciphers

Operates on individual bits and uses a key to generate a string of *pseudorandom* bits called a keystream.



Public-Key Cryptography

Public Key Cryptography



Activity: Public-Key Cryptography

In this activity, you will look at specific scenarios to review the structure of asymmetric algorithms. Then you will research an article overview the SSL / TLS handshake.

Activities/Stu_Public_Key_Cryptography/README.md

Suggested Time:
10 Minutes

GNU Privacy Guard (GPG)

GPG is a command line tool program that allows users to easily:

Generate public and private keys.

Manage other’s public keys

Encrypt and decrypt keys

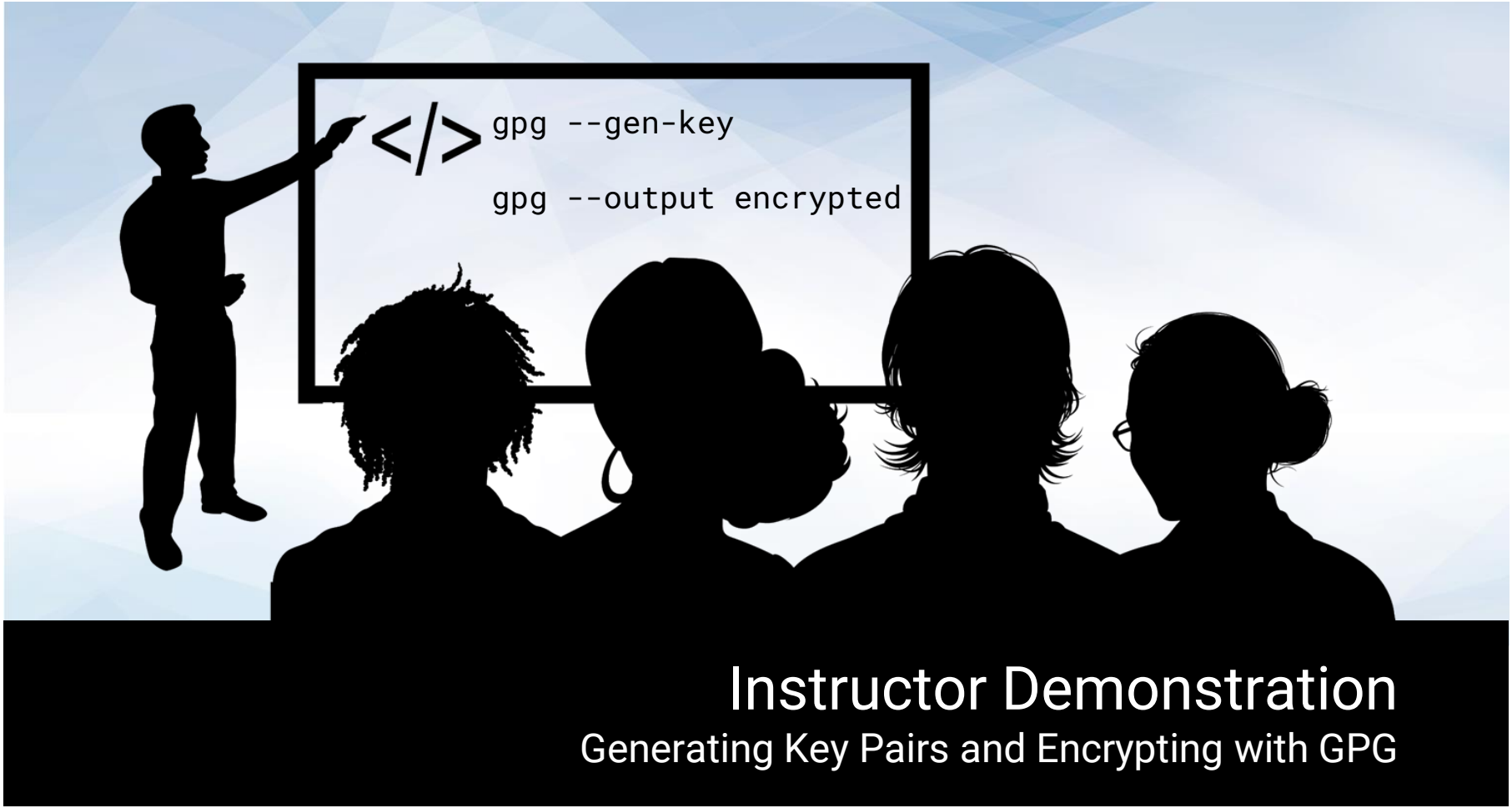
Sign documents

Activity: Installing GPG

Mac users will need to install GPG.
(Pre-installed on Windows.)

Instructions sent via Slack.

Suggested Time:
5 Minutes



Instructor Demonstration

Generating Key Pairs and Encrypting with GPG

Activity: Encrypting with GPG

In this activity, you will use GPG to generate a public/private key pair, generate a revocation certificate, and encrypt / decrypt data.

Activities/Stu_Encrypting_with_GPG/README.md

Suggested Time:
15 Minutes

Take a Break!

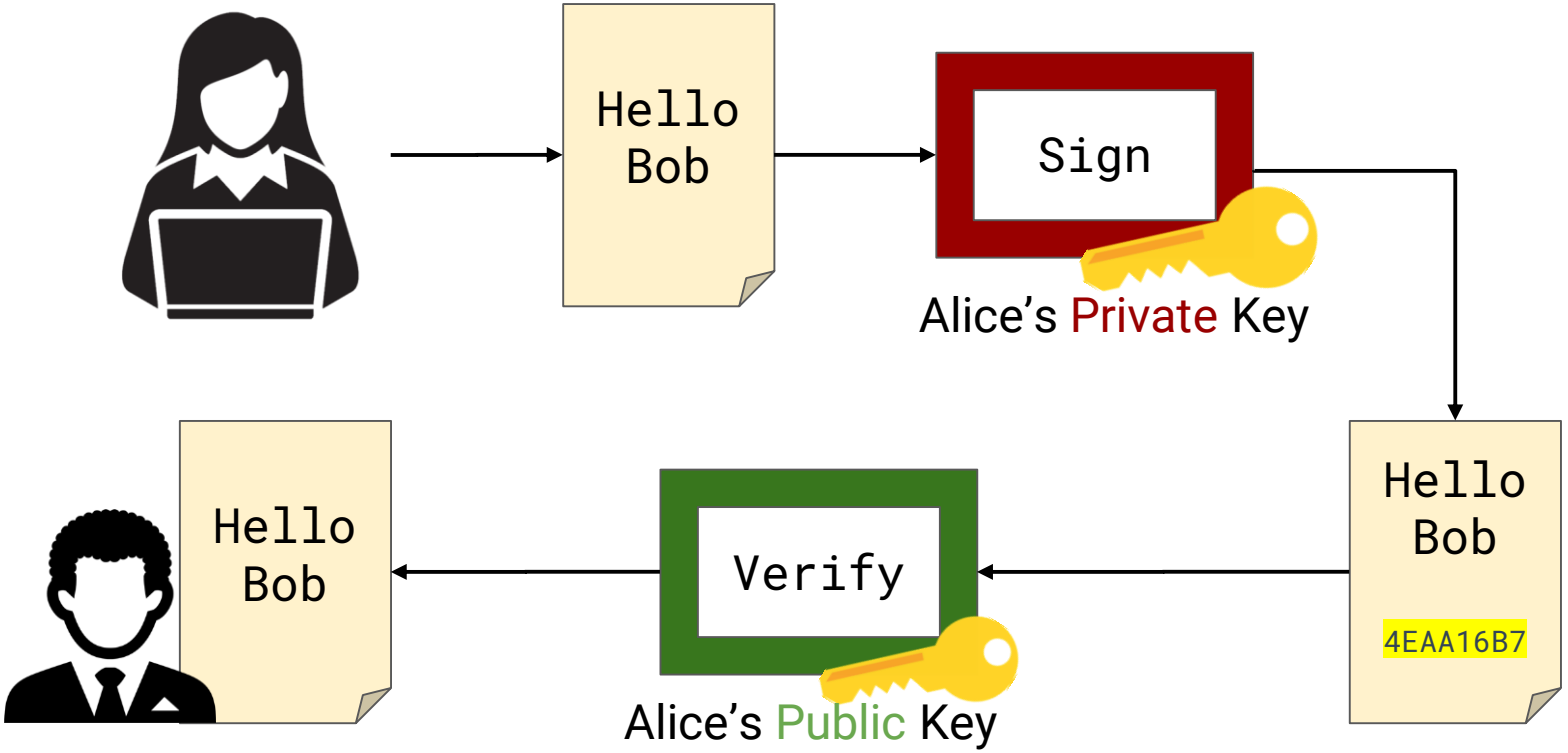
Today’s Objectives

By the end of class, you will be able to:

- [x] Compare and contrast block and stream ciphers.
- [x] Describe how public-key cryptography uses a key pair for encryption and decryption.
- [x] Use the command line program GPC to encrypt and sign documents with public and private keys.
- [ ] Determine how digital signatures use private and public keys to generate and verify signatures.
- [ ] Describe how digital certificates verify digital entities.

Digital Signatures

Digital Signature



Signing with GPG

GPG provides three different ways to sign documents:

All at once: GPG generates an encrypted message with an appended signature.

Clearsigned: GPG generates a signature, which it attaches to the unencrypted message.

Detached signatures: GPG generates an encrypted document without an appended signature as well as a separate file containing the signature.

Activity: Signing Documents

In this activity, you will use GPG to sign documents, verify signatures, and generate clearsigned documents and detached signatures.

Activities/Stu_Signing_Documents

Suggested Time:
15 Minutes

Digital Certificates

Digital Certificates

We need a system for verifying the identity of digital servers...

Digital Certificates are a collection of data regarding the certificate owner's identity, at minimum consisting of the digital signature and verification of the name associated with the certificate owner.

When you connect to a web server and attempt to open an encrypted connection, your browser will use digital certificates to:

- ✔ Validate the digital signature
- ✔ Verify that the server is associated with the domain you're browsing to
- ✔ Check any other identifying information in the certificate.

Certificate Authorities

Determining domain ownership is deferred to entities that issue digital signatures.

01 A client requests a certificate from the CA and submits information verifying its identity, as well as a digital signature

02 The CA verifies this information and then issues the certificate

03 If any of the identifying information is later found to be invalid, the certificate can be revoked, or publicly invalidated.

This mode requires *everyone* to trust the certificate authority. If the CA get compromised, everyone loses.

Activity: Certificate Authorities

In this activity, you will answer questions pertaining to certificate authorities and the web of trust.

Activities/Stu_Certificate_Authorities/README.md

Suggested Time:
15 Minutes

Activity: Inspecting Certificates

In this activity, you will work with a partner to research, inspect, and answer questions about different types of certificates.

Activities/Stu_Inspecting_Certificates

Suggested Time:
15 Minutes

Times Up! Let’s Review.

Certificate Authorities

Today’s Objectives

By the end of class, you will be able to:

- Compare and contrast block and stream ciphers.
- Describe how public-key cryptography uses a key pair for encryption and decryption.
- Use the command line program GPC to encrypt and sign documents with public and private keys.
- Determine how digital signatures use private and public keys to generate and verify signatures.
- Describe how digital certificates verify digital entities.