

# BYU Unix Users Group

Really boring slides, relating to a presentation on:

Everything that Everyone should know about:

## Internet Security

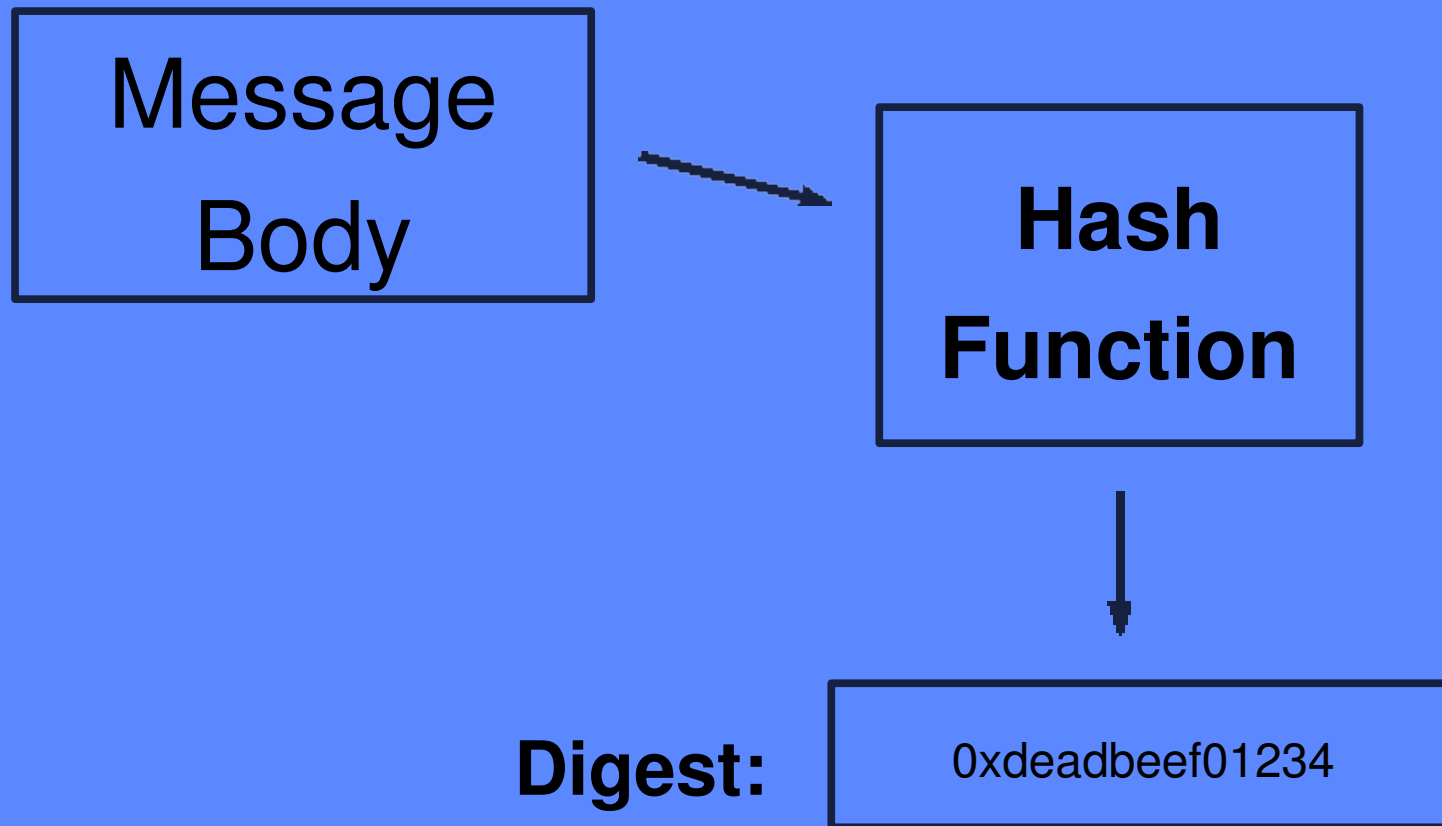
# Hash Functions

# Symmetric Key Encryption

# Public-Key Encryption

# Hash Functions

This is the important stuff.



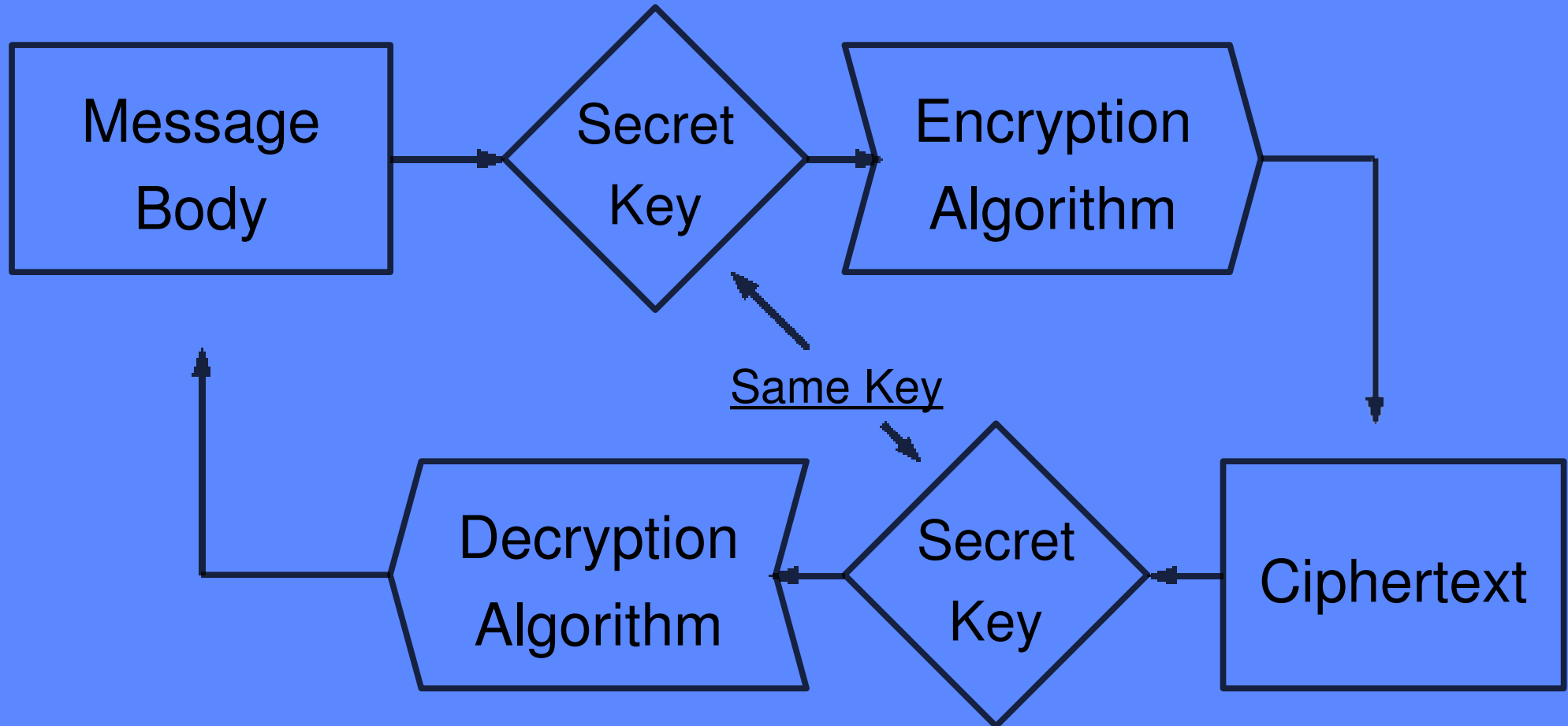
# Hash Functions

Things to think about...

## Basic Requirements of a Cryptographic Hash Function:

- Can be applied to a message of any size.
- Produces a fixed-length output.
- Is relatively easy to apply for any message.
- It is computationally infeasible to find a message, given only its digest (one-way).
- It is computationally infeasible to create a message whose digest will match a given digest.
- It is computationally infeasible to create two different messages with the same digest.

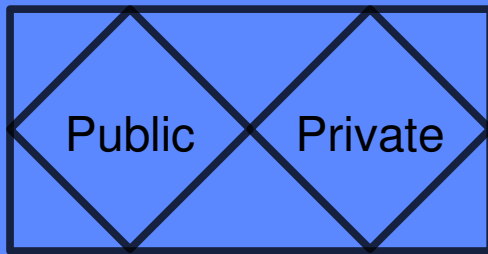
# Symmetric Key Encryption



Kerckhoff's Principle: The security of symmetric encryption depends on the secrecy of the key, not the secrecy of the algorithm.

# Public-Key Encryption

Key-Pair



Private key kept secret.

Public key is publicly distributed.

It is computationally infeasible to find the private key, given the public key.

Ciphertext created with the public key can only be decrypted with the private key.

Ciphertext created with the private key can only be decrypted with the public key.

# Putting it all to good use

Bob wants to send a message to Alice,  
with these 3 assurances:

- Data Integrity
- Authentication
- Confidentiality

# Putting it all to good use

Bob wants to send a message to Alice,  
with these 3 assurances:

- Data Integrity = Hash Function
- Authentication = Hash Function + Private Key
- Confidentiality = Symmetric Key + Public Key

# Putting it all together

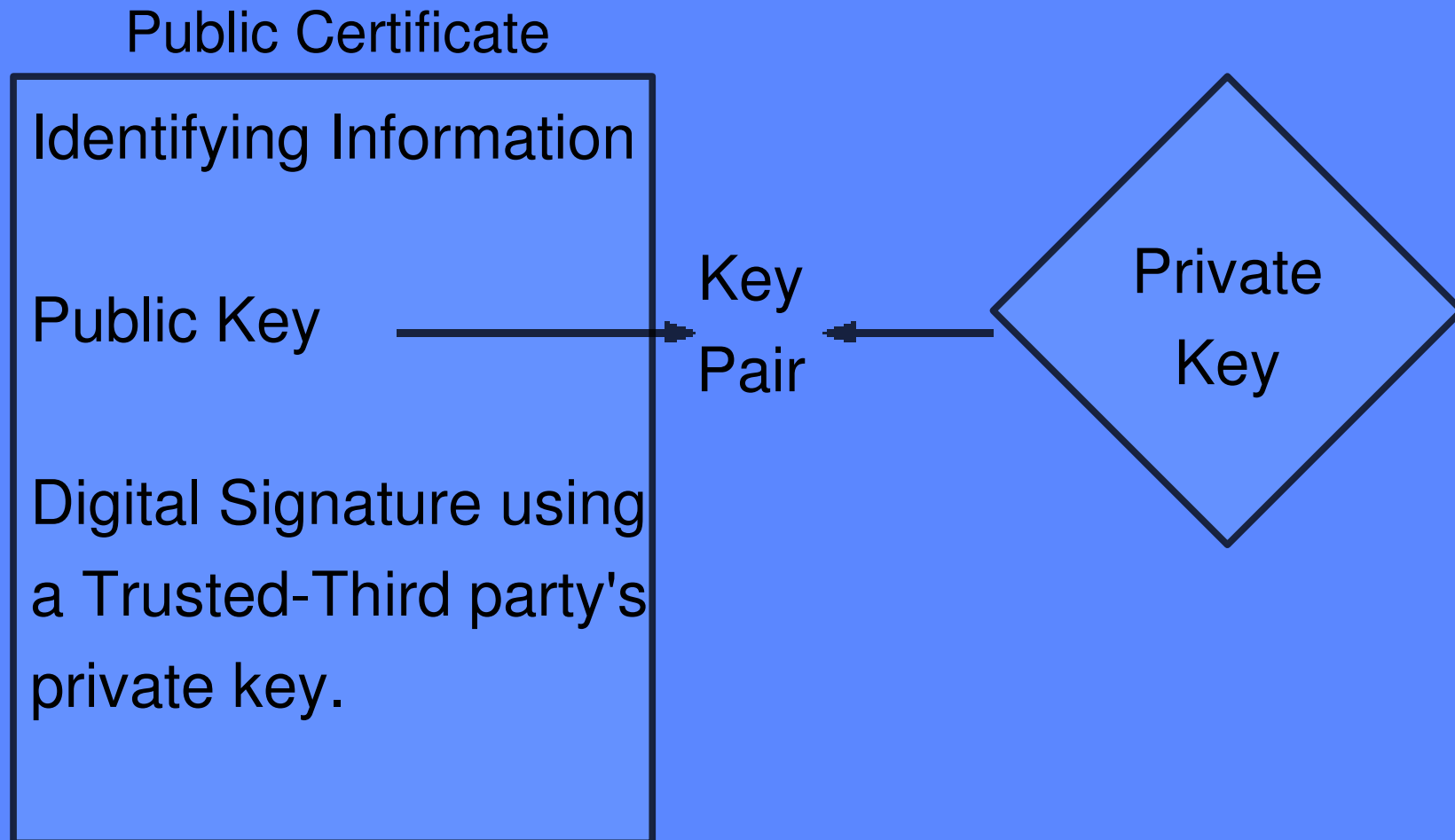
Too ugly for a slide.

Let's go to the whiteboard.

# Things to look into

- GnuPG
- Thunderbird w/ Enigmail

# The Basics



# Other important bits

Certificates are signed by a Certificate Authority.

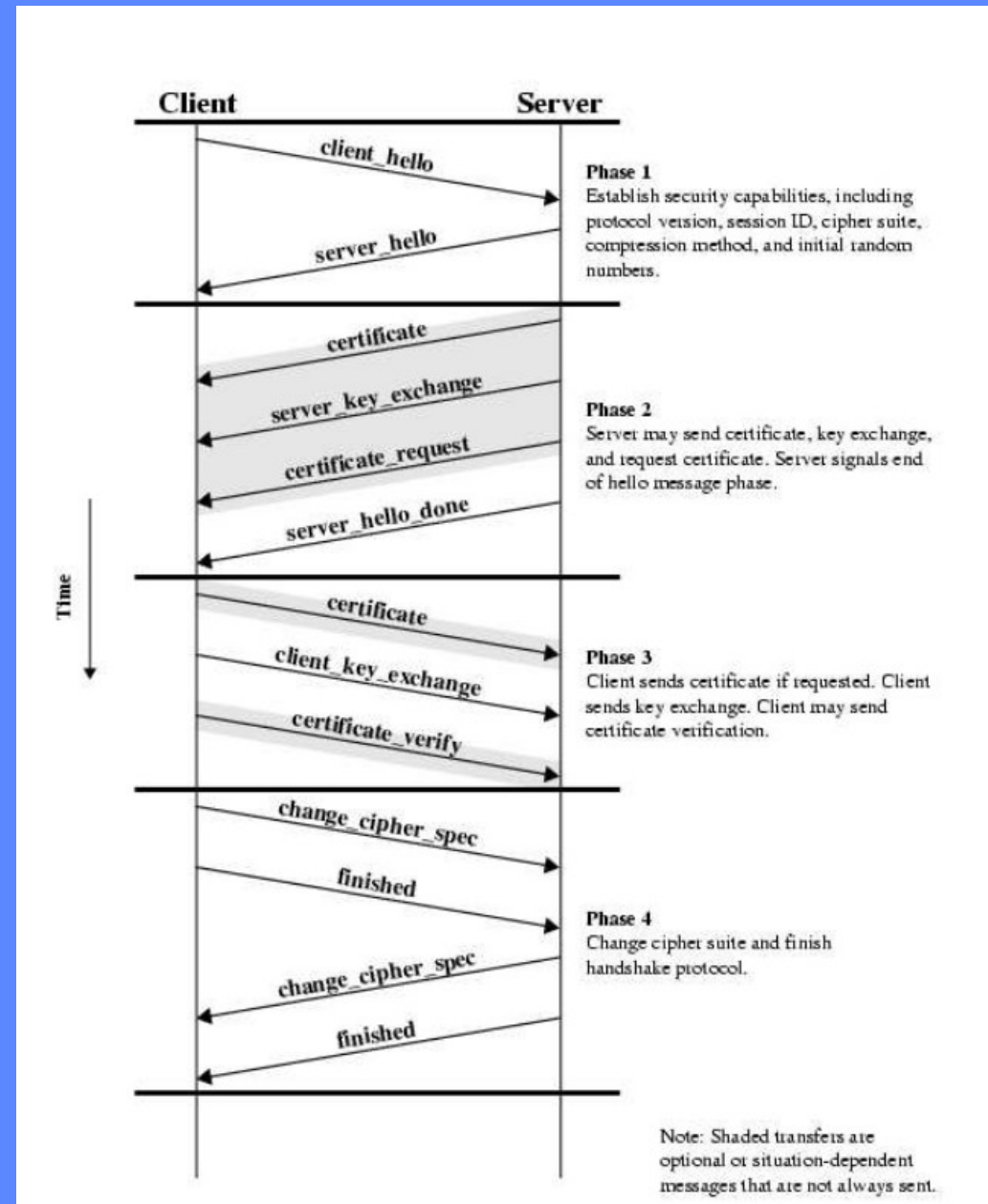
This “authority” certifies the identifying information given in the certificate.

Client programs that use certificates have a list of CAs to automatically trust.

CAs have their own certificates that can be added to a list of “Trusted Authorities.”

Uses certificates and symmetric encryption to provide:

- Authentication  
(one or two-way)
- Confidentiality
- Data Integrity



# What's out there

- Phishing Attacks
- Wireless Sniffing
- Man-in-the-Middle Attacks
  - Arpspoofing
  - DNS Poisoning
  - Router Hijacking/Misuse
- Denial-of-Service Attack