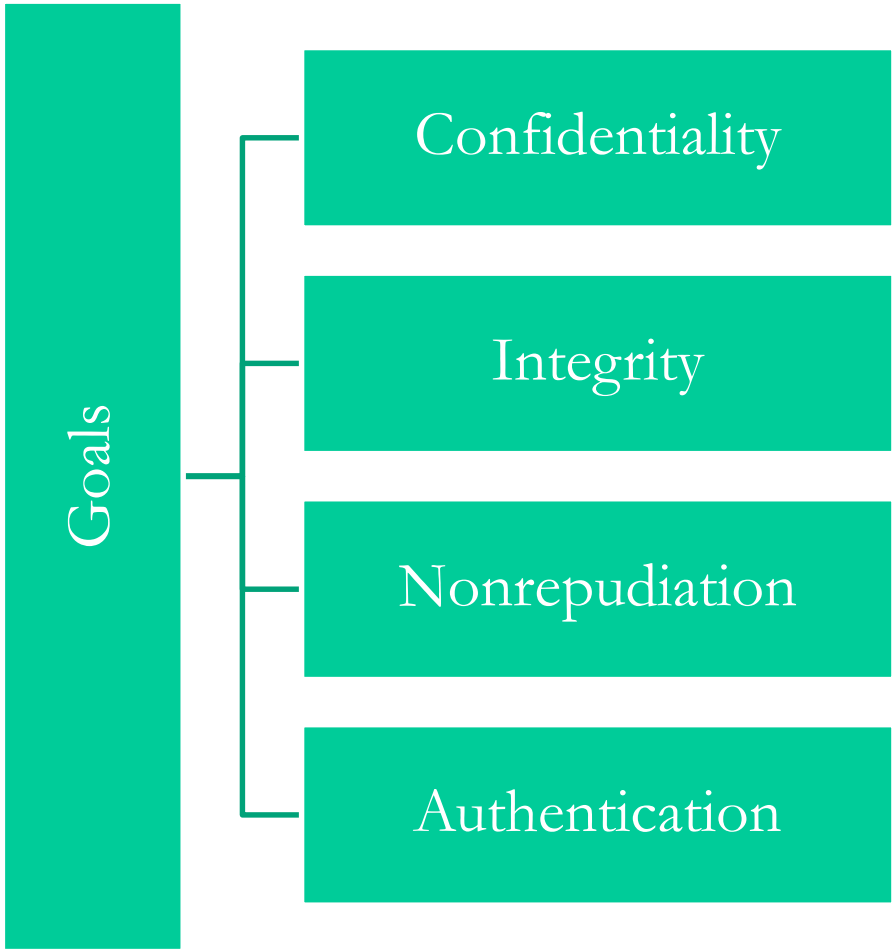
Cryptography

Chapter 3

SYBEX

Goals of Cryptography



SYBEX

Uses of Cryptography

- Applications of cryptography
- Symmetric and asymmetric cryptography
- Working with hashing
- Purposes of keys
- Types of algorithms
- Key management issues

SYBEX

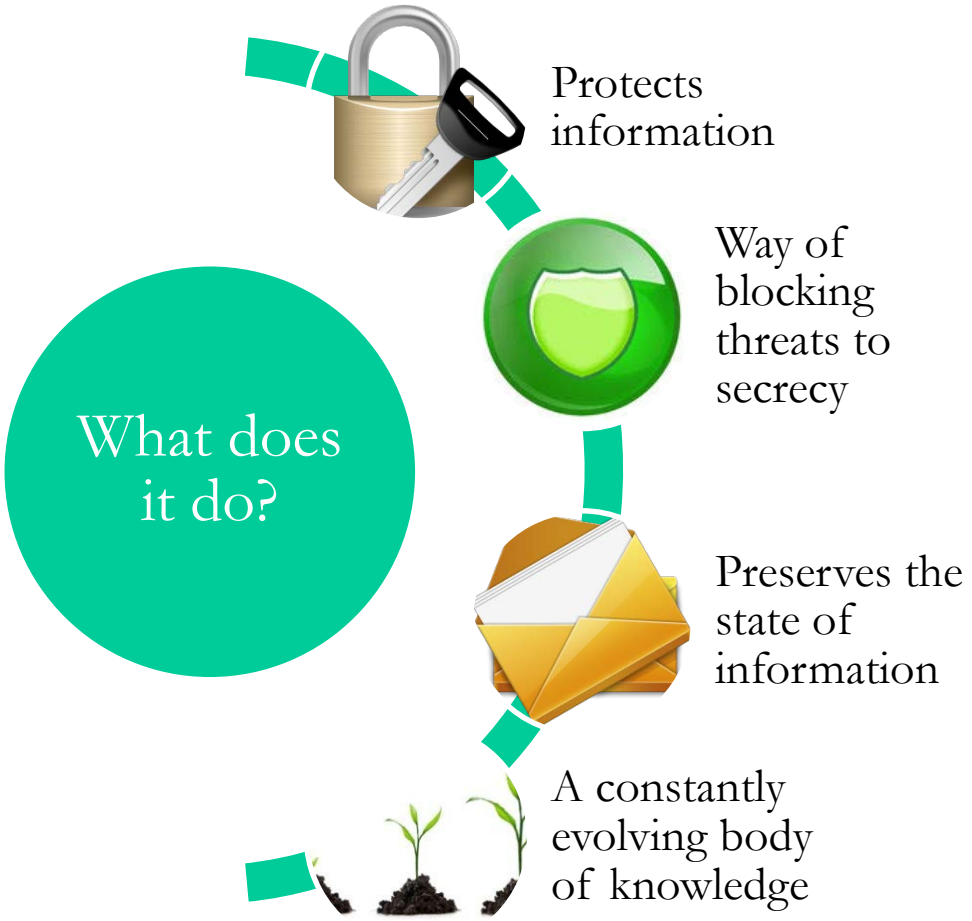
Understanding Cryptography

- Legal issues
- Financial compliance
- Healthcare regulations
- Defense industries
- Acceptable algorithms
- Key strengths

SYBEX

What Is Cryptography?

As information has changed and human beings have gotten smarter, the technology has become substantially more advanced to keep up with changing issues and threats.



Hieroglyphics as an Example

Intricate patterns and glyphs used in Egyptian hieroglyphics were commonly used for spiritual and religious reasons.

- Egyptian hieroglyphics had spiritual and religious significance
- Not designed to preserve secrets
- Used to commune with other world
- Usage restricted to royal family and religious orders
- Could not be deciphered again until 1799 and discovery of Rosetta stone

SYBEX

Modern Applications of Cryptography

Cryptography has even made some of the everyday technologies that you use possible.

E-commerce applications

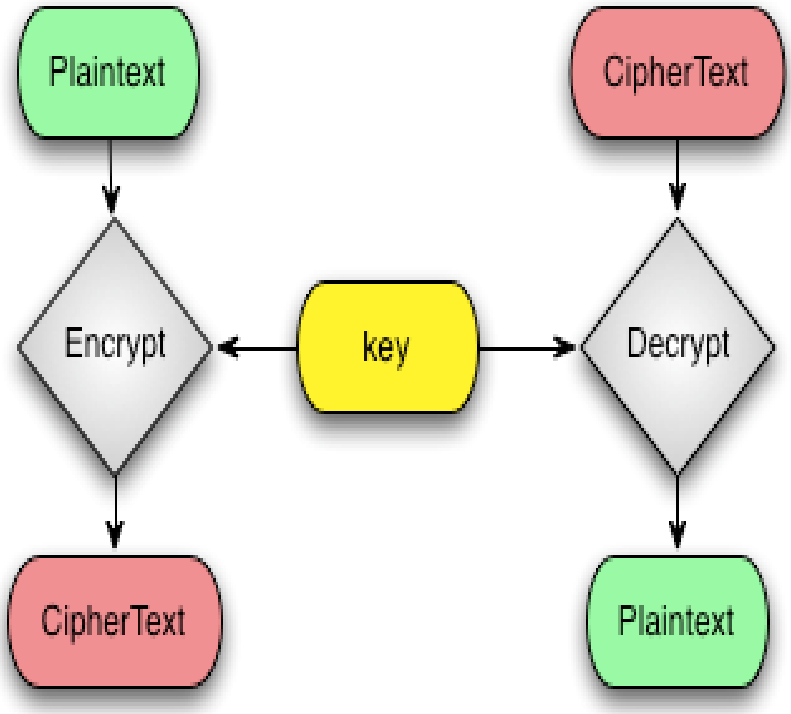
- Couldn't exist in current form without cryptography
- Provides secrecy, integrity, and authentication

Mobile technologies

- Prevents identity theft
- Stops device duplications
- Prevents eavesdropping

SYBEX

Important Terms and How They Work



- Plaintext or cleartext
- Ciphertext
- Algorithms
- Keys

SYBEX

Introducing Symmetric Cryptography

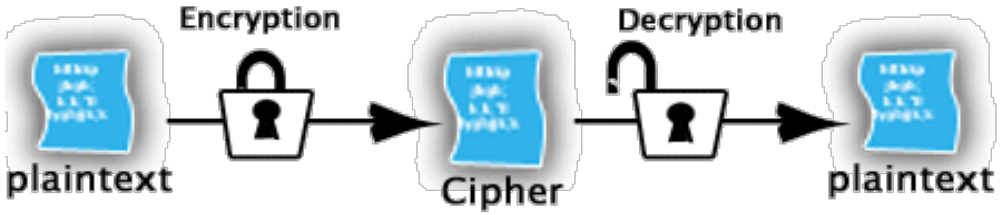
All algorithms that fit into the symmetric variety use a single key to both encrypt and decrypt (hence the name symmetric).

Symmetric systems are great at

- Confidentiality
- Speed
- Overall simplicity
- Providing authenticity

Drawbacks of symmetric systems

- Key management
- Lack of non-repudiation capability



SYBEX

Examples of Symmetric Algorithms

There are currently a myriad of symmetric algorithms available; a Google search turns up an endless sea of alphabet soup of algorithms.

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Blowfish
- International Data Encryption Algorithm (IDEA)
- RC2, RC4, RC5, RC6
- Rijndael or Advanced Encryption Standard (AES)
- Twofish

SYBEX

Asymmetric or Public Key Cryptography

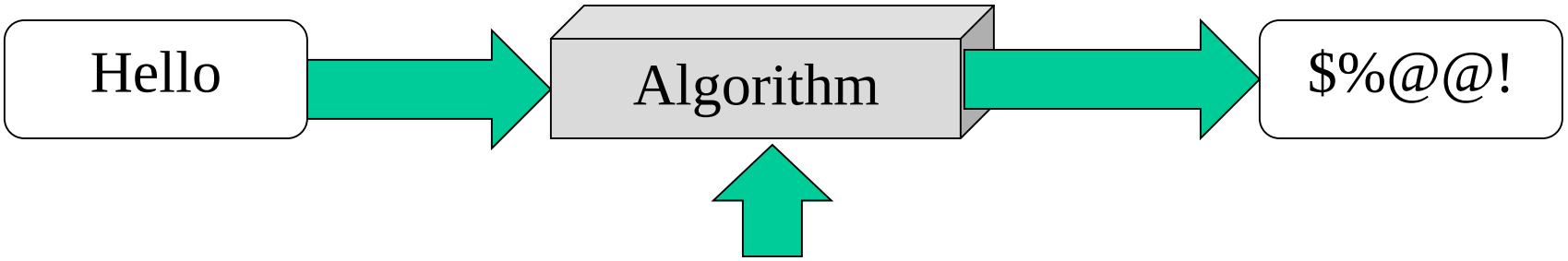
The concept of public key cryptography was intended to overcome key management problems in previous systems. In the system each user receives a pair of keys called the *public key* and the *private key*. Each person's public key is published, whereas the private key is kept secret.

- Uses a key pair consisting of a public key and a private key
- Ensures non-repudiation
- Can enforce authentication
- Solves key management issues
- Is slower compared to symmetric systems

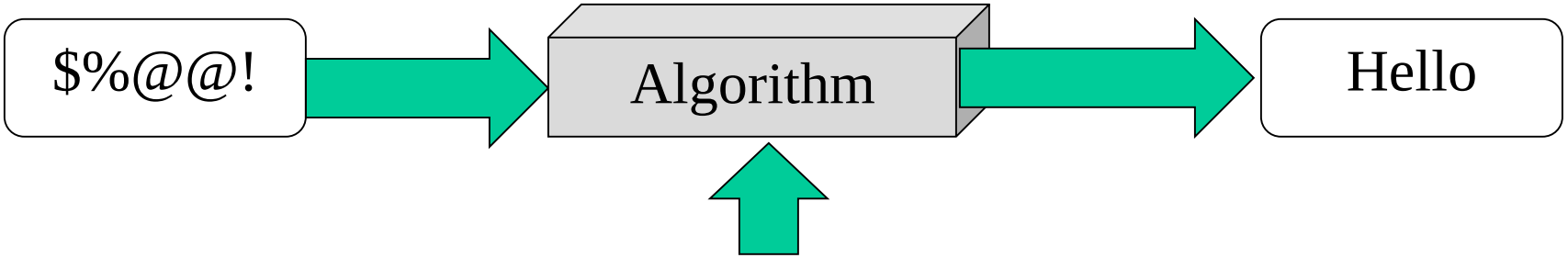
SYBEX

Asymmetric Encryption

Encryption

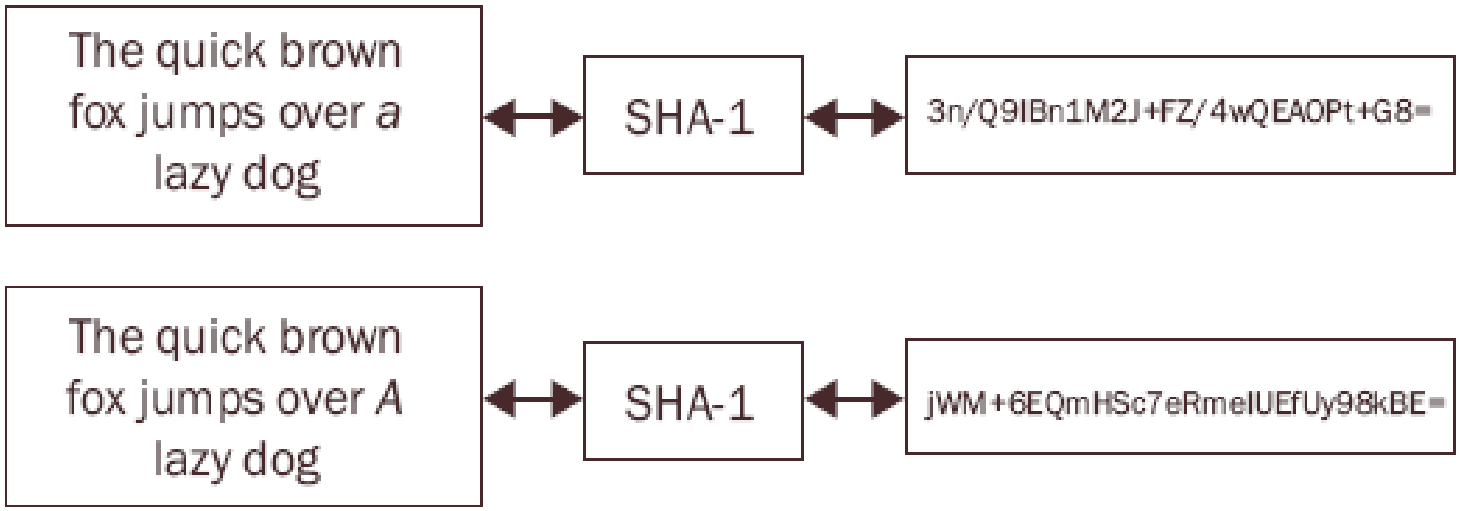


Decryption



About That Hash

- A hash is a one-way function
- Can be computed in one direction and not the other
- Is a fixed length
- Creates a unique output for every input



Hashing Algorithms

Hashing is used to detect changes in information: anything that is hashed and then changed, even a small amount, will result in an entirely different hash from the original.

- Message Digest 2 (MD2)
- Message Digest 4 (MD4)
- Message Digest 5 (MD5)
- Message Digest 6 (MD6)
- HAVAL
- RIPE-MD
- Secure Hash Algorithm-0 (SHA-0)
- Secure Hash Algorithm-1 (SHA-1)
- Secure Hash Algorithm-2 (SHA-2)

SYBEX

Hashing in Digital Signatures

Sean creates a message.

Sean hashes the message.

Sean encrypts the hash with his private key.

Sean sends the combination to Zelda.

Zelda sees that the message came from Sean.

Seeing who the sender is, Zelda retrieves Sean's public key.

Zelda decrypts the hash value, thus validating the identity of the sender.

Zelda reruns the algorithm against the plaintext and compares the two.

If the hashes match, the message has not been altered.

SYBEX

The Role of Digital Certificates

A digital certificate complements or replaces other forms of authentication. A user who presents the credential must have a method in place that allows for the credential to be validated.

- Digital certificates establish ownership of a key
- Can be attached to a person, computer, or service
- Certificates are issued under specific rules
- Used in many applications such as e-commerce

SYBEX

Certification Authorities

A certification authority (CA) handles digital certificates.

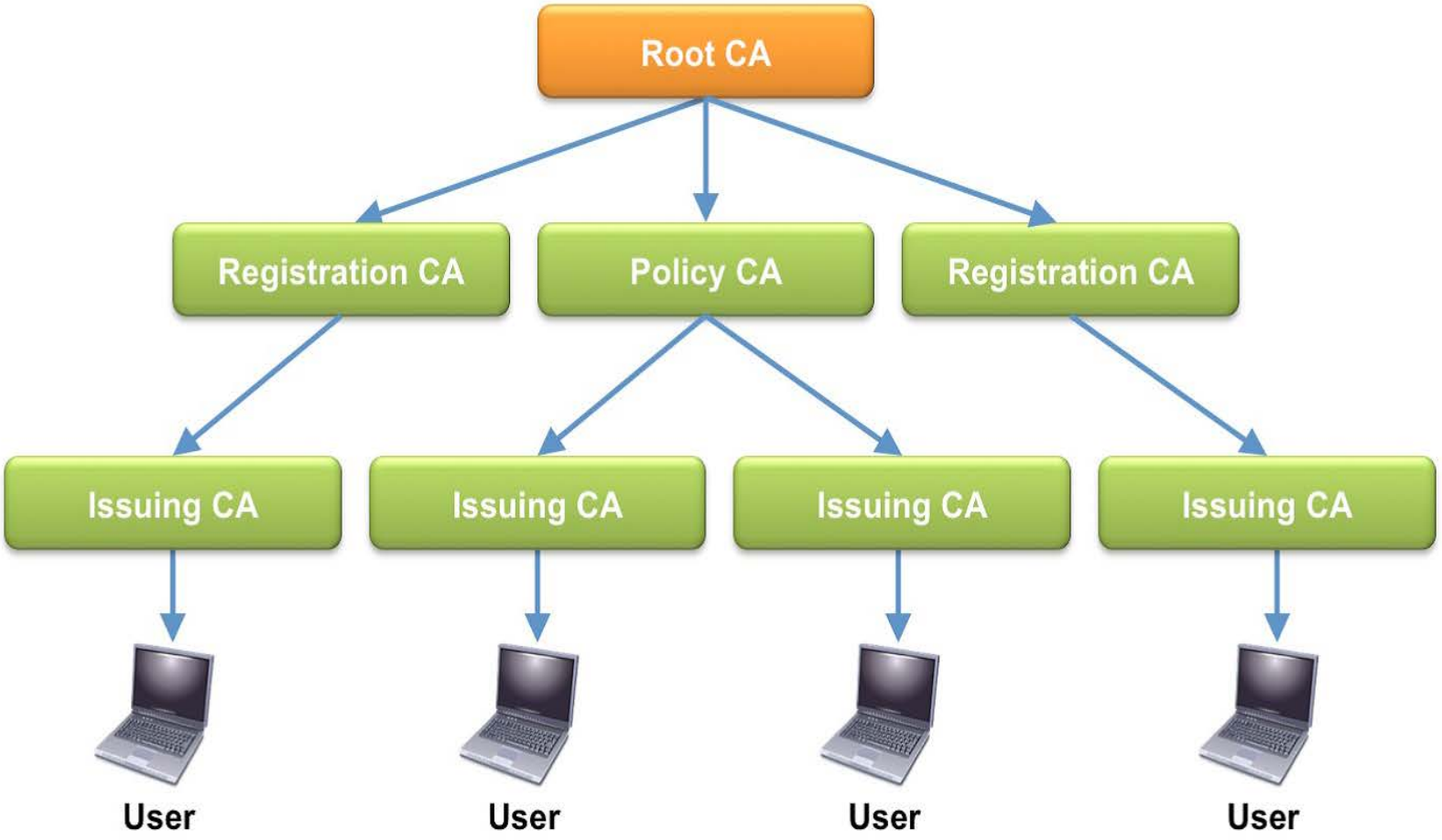
A CA can revoke a certificate.

A CA will validate a certificate.

Trusted third party is a name used to describe a CA.

SYBEX

Building a PKI System



Applications of Cryptography: IPSec

- Internet Protocol Security (IPSec) protects data during transmission
- Operates at the Network layer
- Very widely used
- Present in virtual private networks (VPN)

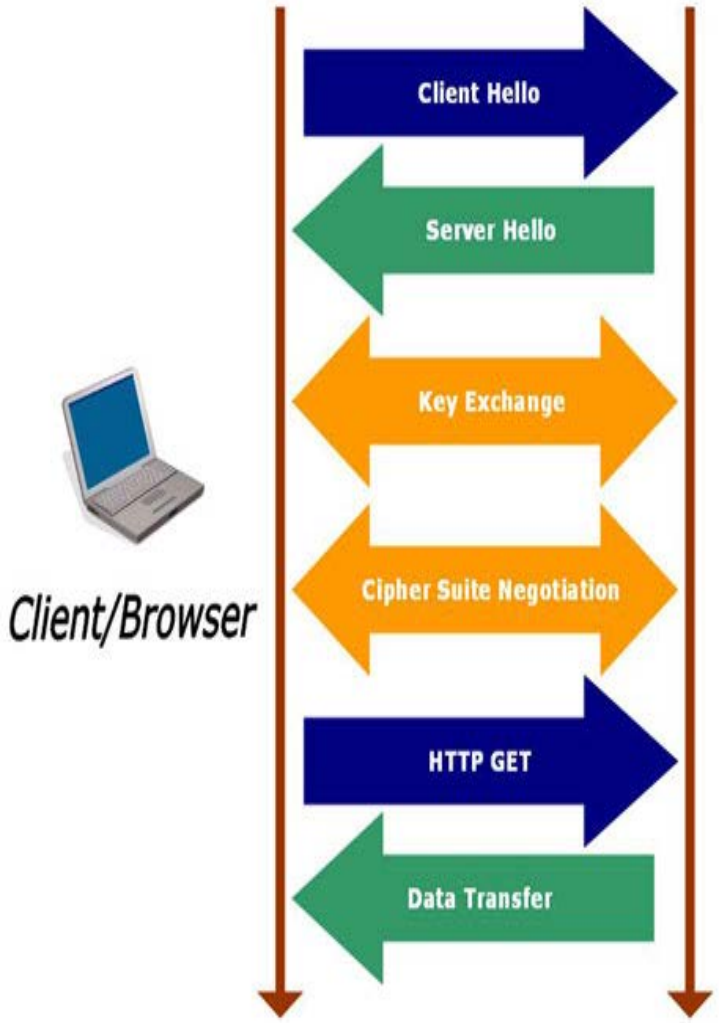
SYBEX

Applications of Cryptography
PGP

- Designed to provide security in online communications
- Similar to public and private key encryption
- Is used to both sign and encrypt communications
- Can be used to protect data files on hard drive or other media

SYBEX

Applications of Cryptography: Secure Sockets Layer



- Developed by Netscape in 1990s
- Standard for exchanging secure data
- Encrypts information prior to transmission
- Decrypts upon receipt
- Combines asymmetric and symmetric systems

SYBEX

Summary

- Understanding cryptography is important to progressing into pen testing.
- Cryptography keeps data and services safe.
- Cryptography provides confidentiality, integrity, non-repudiation, and authentication services.
- Technologies such as SSL, IPSec and others would not be possible without cryptography.

SYBEX