CS 465

Cryptography Introduction

Last Updated: Aug 25, 2015

Outline

- Provide a brief historical background of cryptography
- Introduce definitions and high-level description of four cryptographic primitives we will learn about this semester
  - Symmetric Encryption (AES)
  - Public-Key Cryptography (RSA)
  - Secure One-Way Hash (SHA-1)
  - Message Authentication Code (MAC)

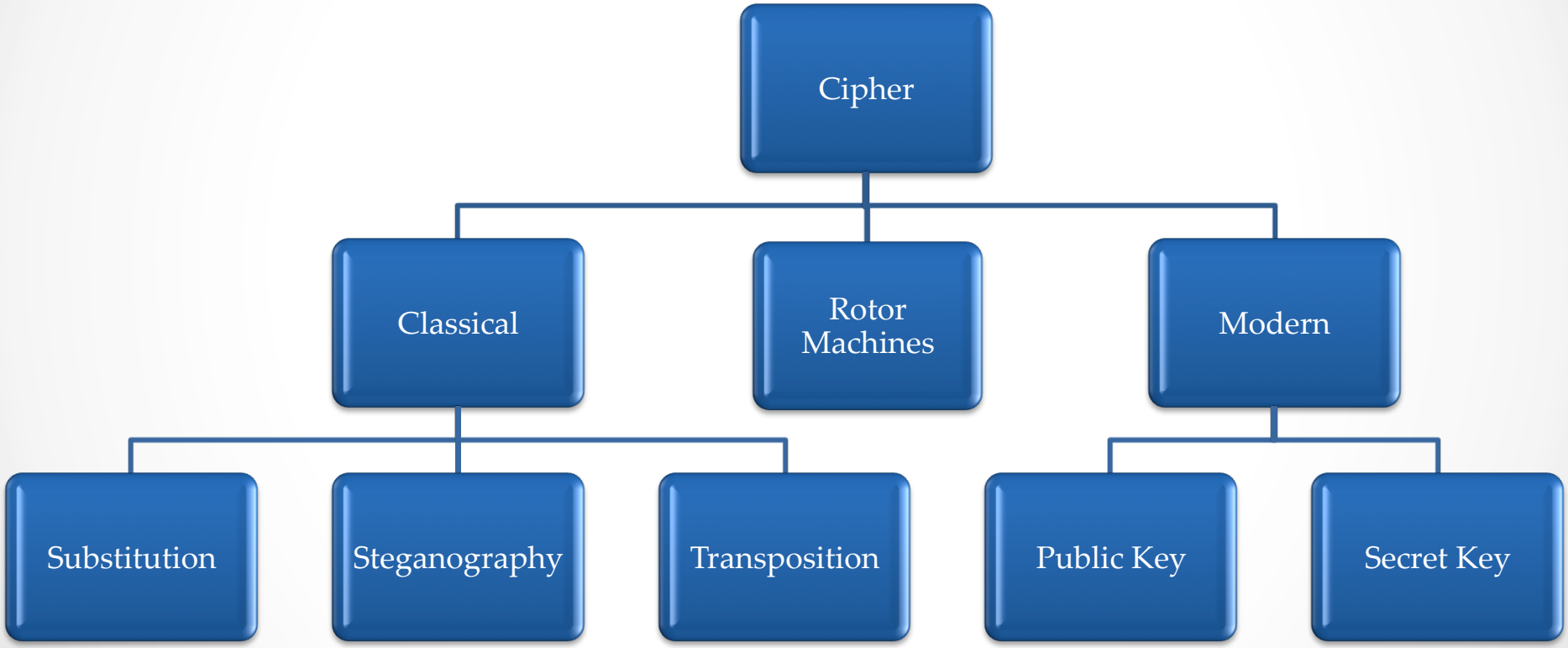
Terminology

- Access Control
  - Authentication
    - Assurance that entities are who they claim to be
  - Authorization
    - Assurance that entities have permission to perform an action
- Confidentiality
  - Prevent the disclosure of sensitive data to unauthorized entities
- Integrity
  - Prevent modification of sensitive data by unauthorized entities
- Non-repudiation
  - Prevent the ability to later deny that an action took place
  - Usually involves cryptographic evidence that will stand up in court

What is Encryption?

- Transforming information so that its true meaning is hidden
  - Requires “special knowledge” to retrieve
- Modern encryption algorithms use transposition and substitution in complex ways that are hard to reverse
- Examples from history that are easy to break
  - ROT-13 (aka Caesar Cipher) is easy to break, simple substitution cipher
  - Vigenere cipher – polyalphabetic substitution cipher
- Examples of strong encryption
  - AES
  - 3DES
  - RC4

Types of Encryption Schemes



GOOD DOG
PLLX XLP
PLSX TWF

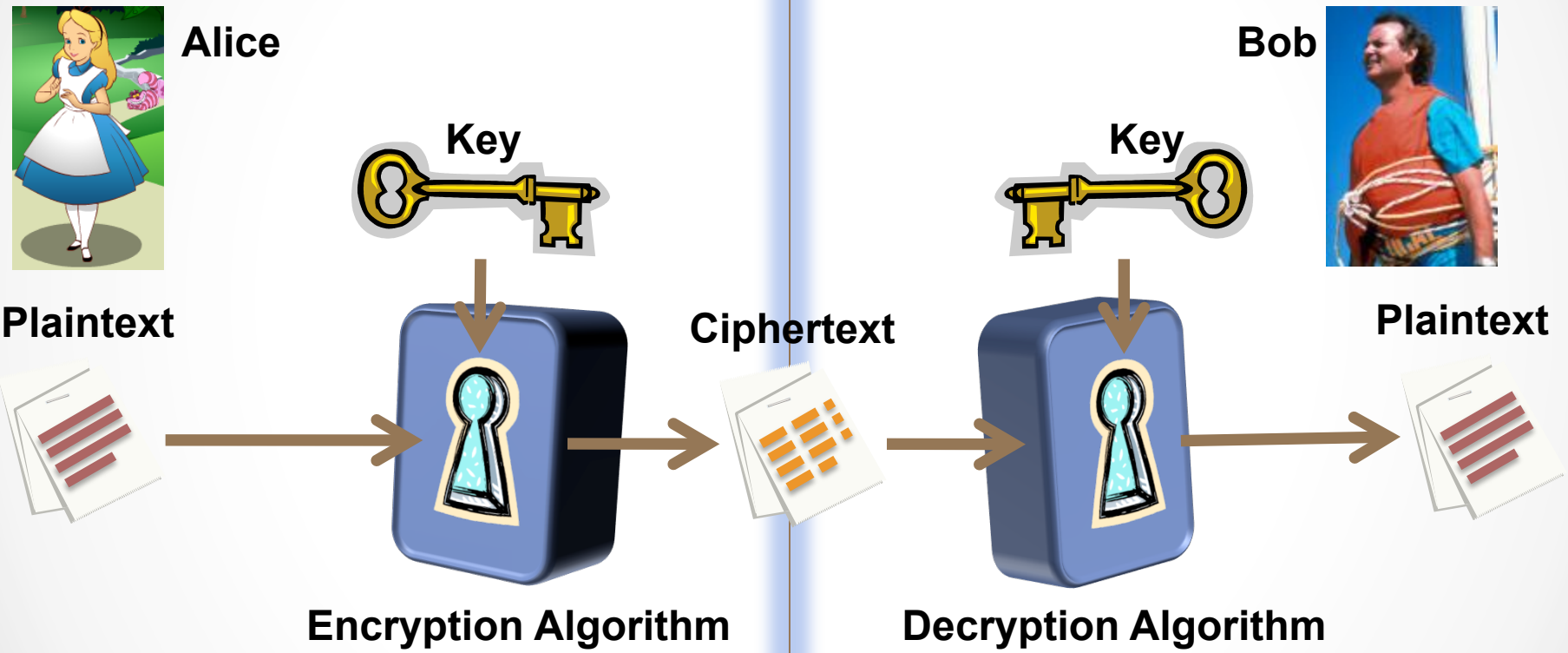
GOOD DOG
DGOGDOO

Hierarchy & Examples based on:
http://en.wikipedia.org/wiki/Cipher

Symmetric Encryption

- Also known as
  - Conventional encryption
  - Secret-key encryption
  - Single-key encryption

Symmetric Encryption Model



Requirements

- Two requirements for strong symmetric encryption
  1. Strong algorithm (cipher)
     - Attacker is unable to decrypt ciphertext or discover the key even if attacker has samples of ciphertext/plaintext created using the secret key
  2. Sender and receiver must securely obtain and store the secret key

Kerckhoffs' Principle

- The security of the symmetric encryption depends on the secrecy of the key, not the secrecy of the algorithm

Dr. Auguste Kerckhoffs (1835-1903)
Dutch linguist and cryptographer

Types of Ciphers

- Block cipher (3DES, AES)
  - Plaintext is broken up into fixed-size blocks
  - Typical block size (64, 128 bits)
- Stream cipher (RC4)
  - Process plaintext continuously
  - Usually one byte at a time

What can go wrong?

- Algorithm
  - Relying on the secrecy of the algorithm
    - Example: Substitution ciphers
  - Using an algorithm incorrectly
    - Example: WEP used RC4 incorrectly

- Key
  - Too big
    - Slow
    - Storage
  - Too small
    - Vulnerable to compromise

Big Numbers

- Cryptography uses REALLY big numbers
  - 1 in 2^{61} odds of winning the lotto and being hit by lightning on the same day
  - 2^{92} atoms in the average human body
  - 2^{128} possible keys in a 128-bit key
  - 2^{170} atoms in the planet
  - 2^{190} atoms in the sun
  - 2^{233} atoms in the galaxy
  - 2^{256} possible keys in a 256-bit key

Thermodynamic Limitations*

- Physics: To set or clear a bit requires no less than kT
  - k is the Boltzman constant ($1.38*10^{-16}$ erg/ºK)
  - T is the absolute temperature of the system
- Assuming T = 3.2ºK (ambient temperature of universe)
  - kT = $4.4*10^{-16}$ ergs
- Annual energy output of the sun $1.21*10^{41}$ ergs
  - Enough to cycle through a 187-bit counter
- Build a Dyson sphere around the sun and collect all energy for 32 years
  - Enough energy to cycle through a 192-bit counter.
- Supernova produces in the neighborhood of 10^{51} ergs
  - Enough to cycle through a 219-bit counter

*From Applied Cryptography (Schneier)

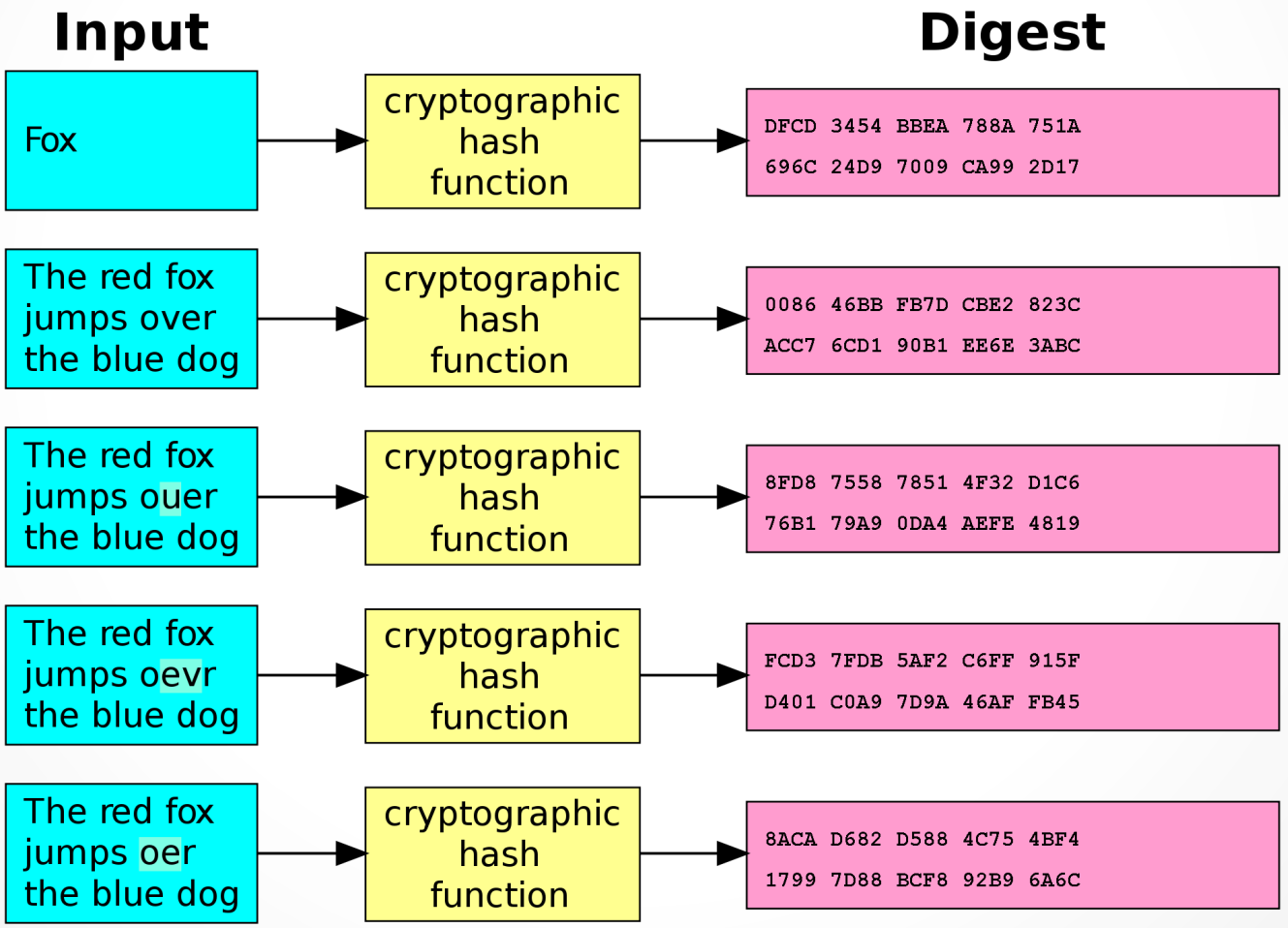
Perfect Encryption Scheme?

- One-Time Pad (XOR message with key)
- Example*:
  - Message: `ONETIMEPAD`
  - Key: `TBFRGFARFM`
  - Ciphertext: `IPKLPSFHGQ`

  - The key `TBFRGFARFM` decrypts the message to `ONETIMEPAD`
  - The key `POYYAEAAZX` decrypts the message to `SALMONEGGS`
  - The key `BXFGBMTMXM` decrypts the message to `GREENFLUID`

*From Applied Cryptography (Schneier)

Cryptographic Hash Function



Source: http://en.wikipedia.org/wiki/Cryptographic_hash_function

Message Authentication Code (MAC)

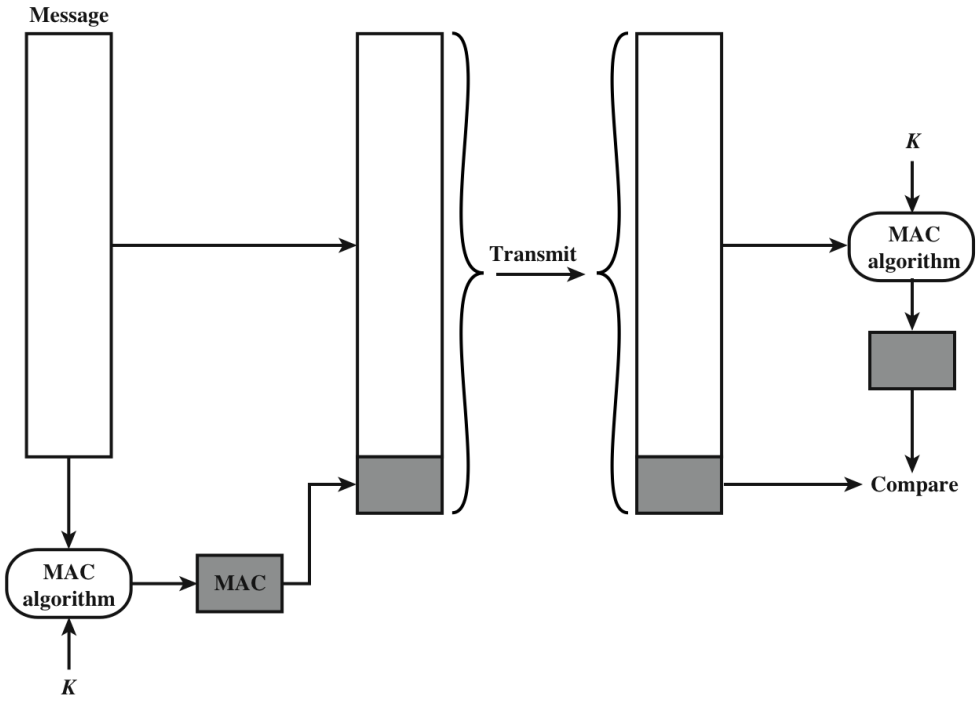


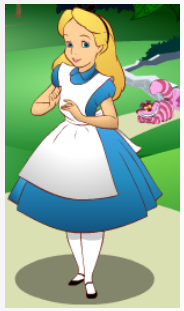
Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Source: Network Security Essentials (Stallings)

Public Key Cryptography

- Terminology
  - Public Key
  - Private Key
  - Digital Signature
- Confidentiality
  - You encrypt with a public key, and you decrypt with a private key
- Integrity/Authentication
  - You sign with a private key, and you verify the signature with the corresponding public key
- Examples
  - Diffie-Hellman
  - RSA
  - Elliptic Curve Cryptography (ECC)
  - Identity-based Encryption (IBE)

Model for Encryption with Public Key Cryptography



Alice

Bob's Public Key

Bob's Private Key

Bob

Plaintext

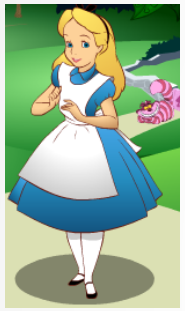
Ciphertext

Plaintext

Encryption Algorithm

Decryption Algorithm

Model for Digital Signature with Public Key Cryptography



Alice

Alice's Private Key

Bob

Alice's Public Key

Plaintext

Ciphertext

Plaintext

Signing Algorithm

Verification Algorithm