

CS 465

Computer Security

Cryptography Introduction

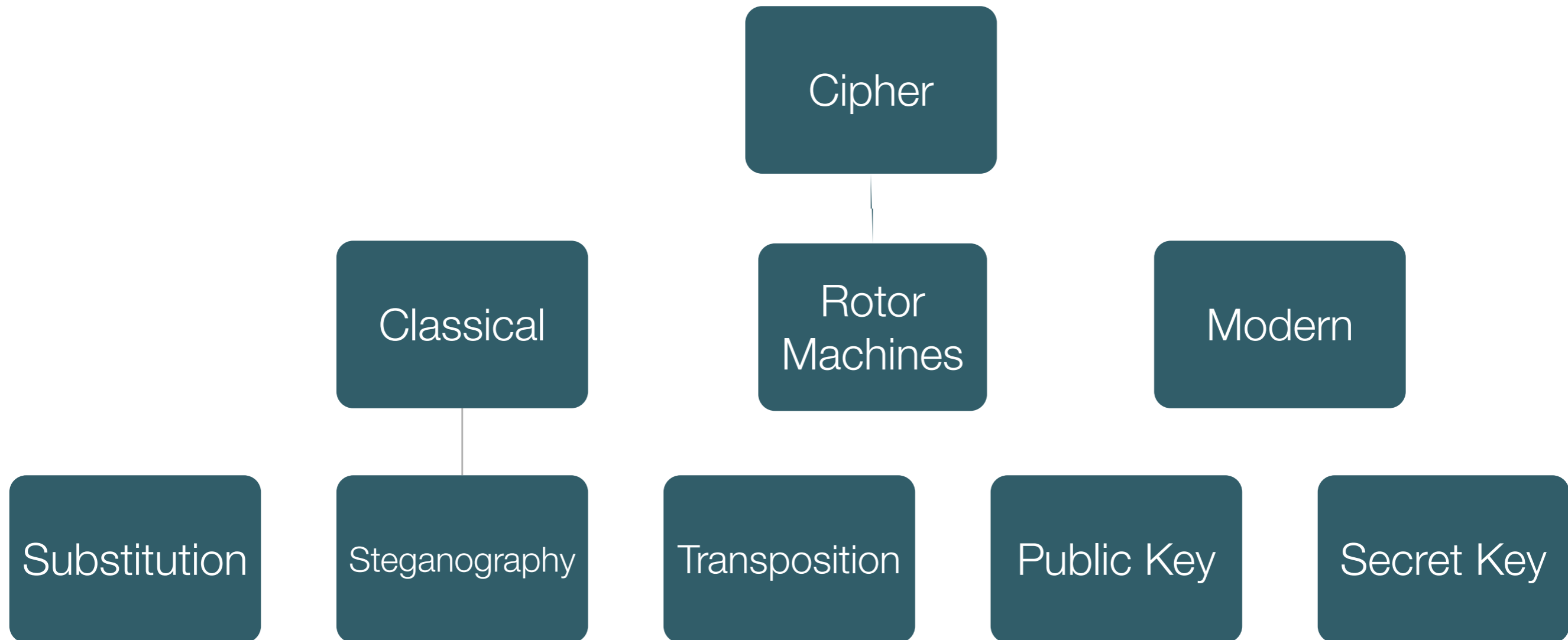
Cryptography

- Literal definition means “hidden writing”
- Until modern times, cryptography was synonymous with encryption, but the field has expanded
- This lecture reviews a 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-256)
 - Message Authentication Code (MAC)

What is Encryption?

- Transforming information so that its true meaning is hidden
 - Requires “special knowledge” to retrieve
- Textbook has good examples of early ciphers — be sure to read this, they illustrate some basic concepts
 - Caesar Cipher
 - Vigenere Cipher

Types of Encryption Schemes



Perfect Encryption Scheme?

- One-Time Pad (XOR message with key)
- Example*:

- Message: ONETIMEPAD
- Key: TBFRGFARFM
- Ciphertext: IPKLPSFHGQ

Why is this not practical?

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

Modern, strong encryption ciphers

AES (NIST standard - FIPS 140, NSA's Suite B)

RSA

Salsa20

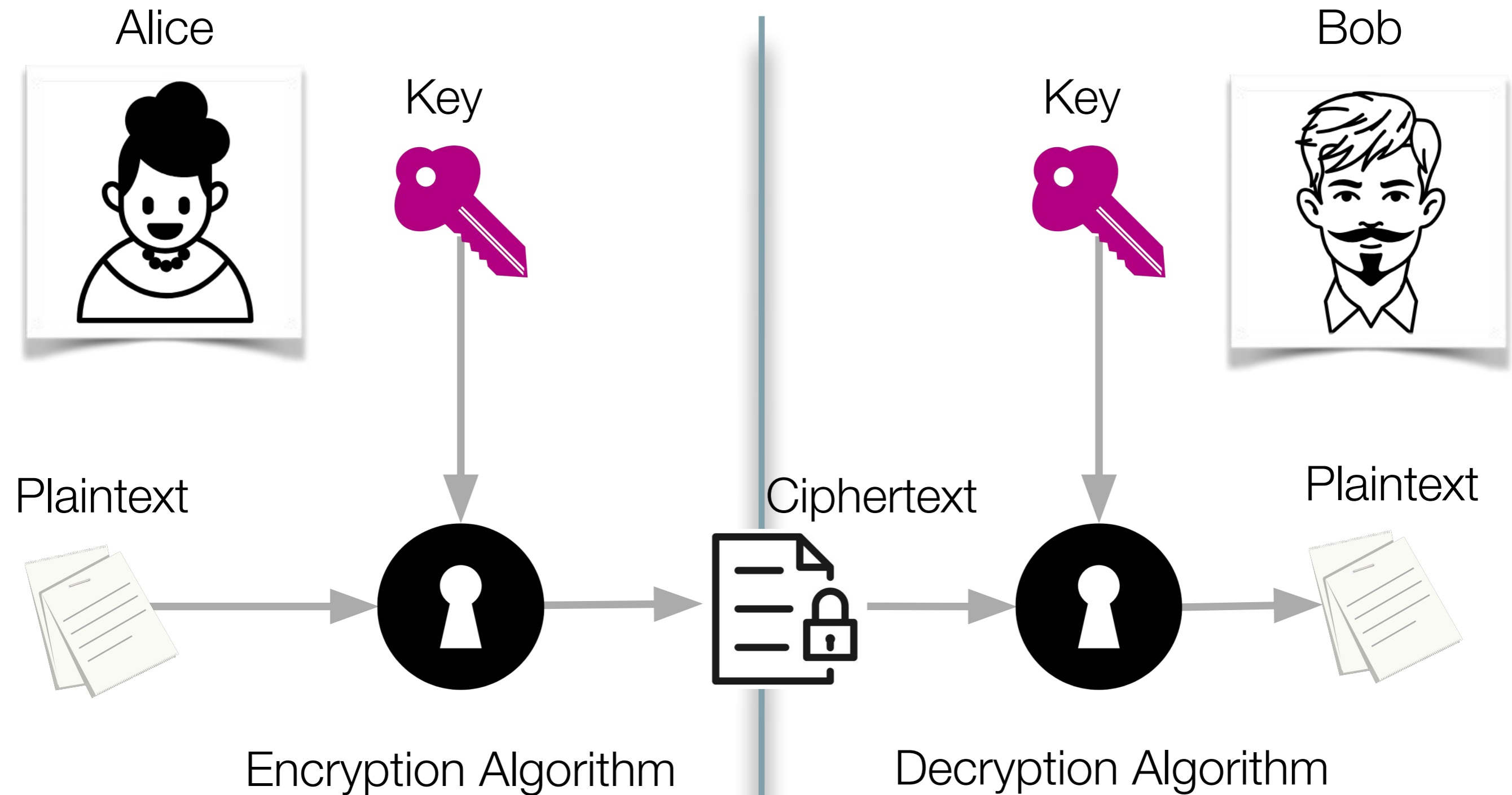
“Popular on the Internet” but no longer recommended

3DES

RC4

Symmetric Encryption

Symmetric Encryption Model

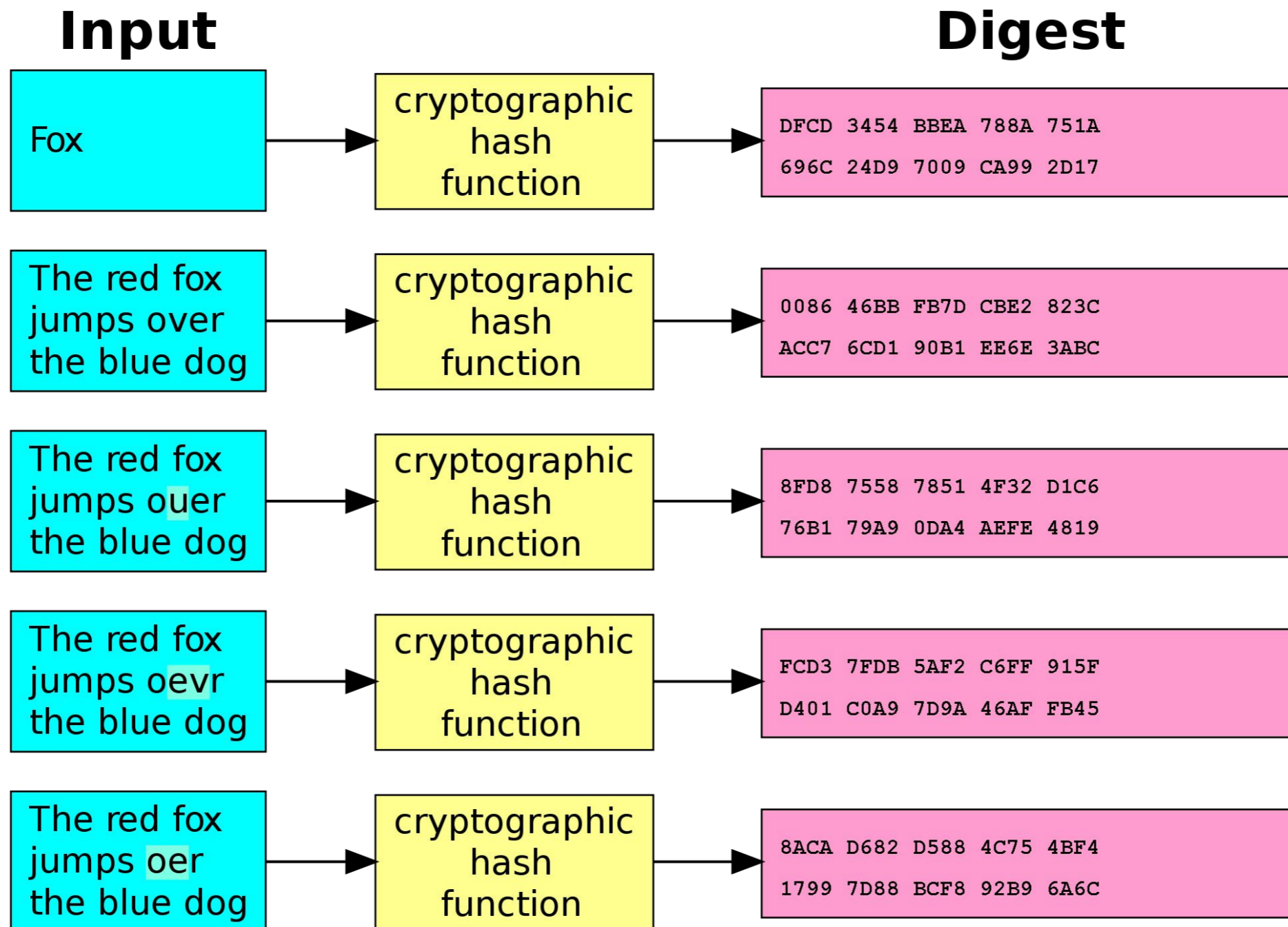


Use Cases

- Web browsing using HTTPS
- Encrypted chat (WhatsApp and Signal)
- Encrypted email (S/MIME and PGP)
- File and disk encryption

Cryptographic Hash Function

Cryptographic Hash Function



Hashing Use Cases

- Digital signature
- File integrity verification (TripWire)
- Password hashing
- Rootkit detection

MAC

Message Authentication Code (MAC)

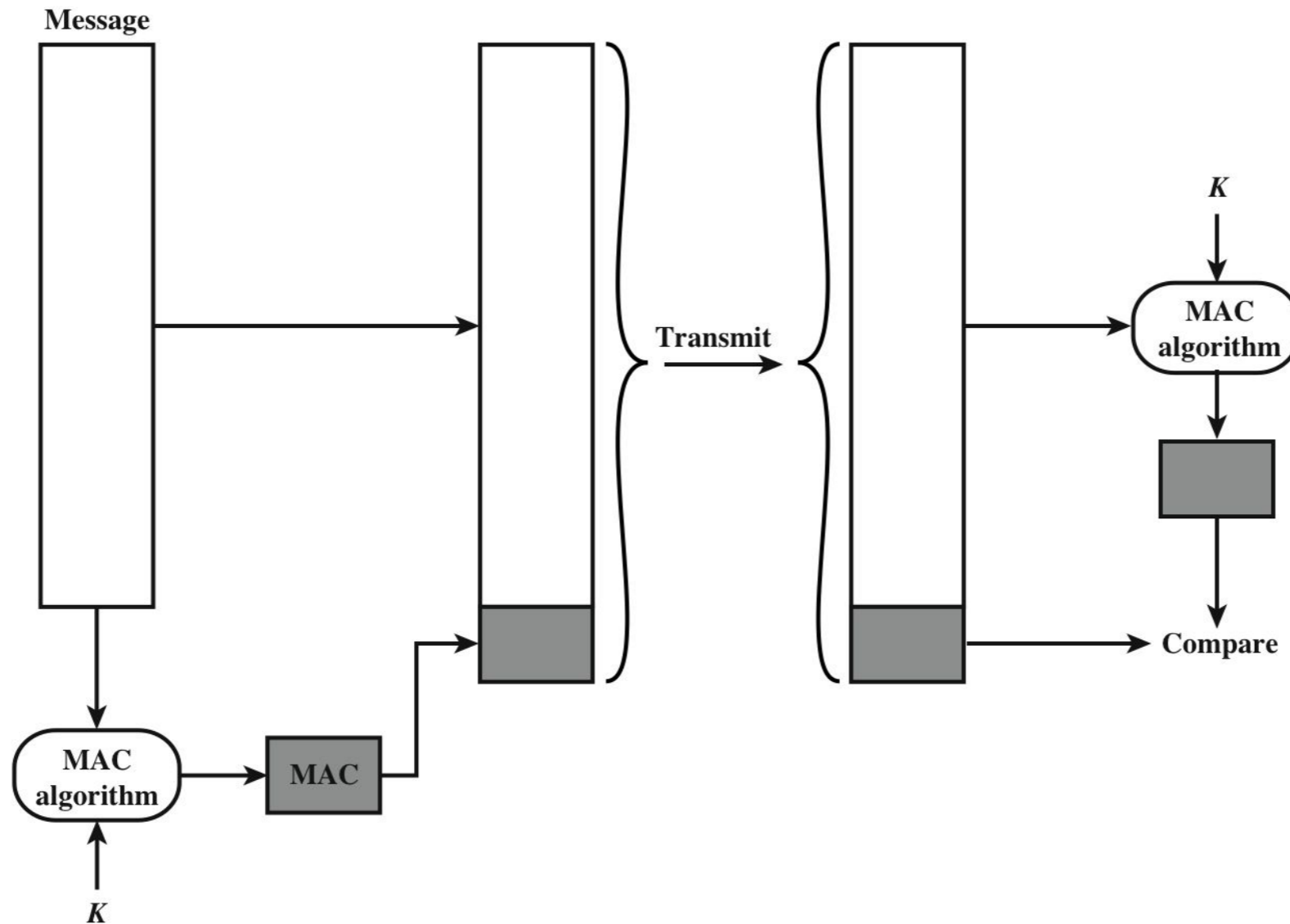


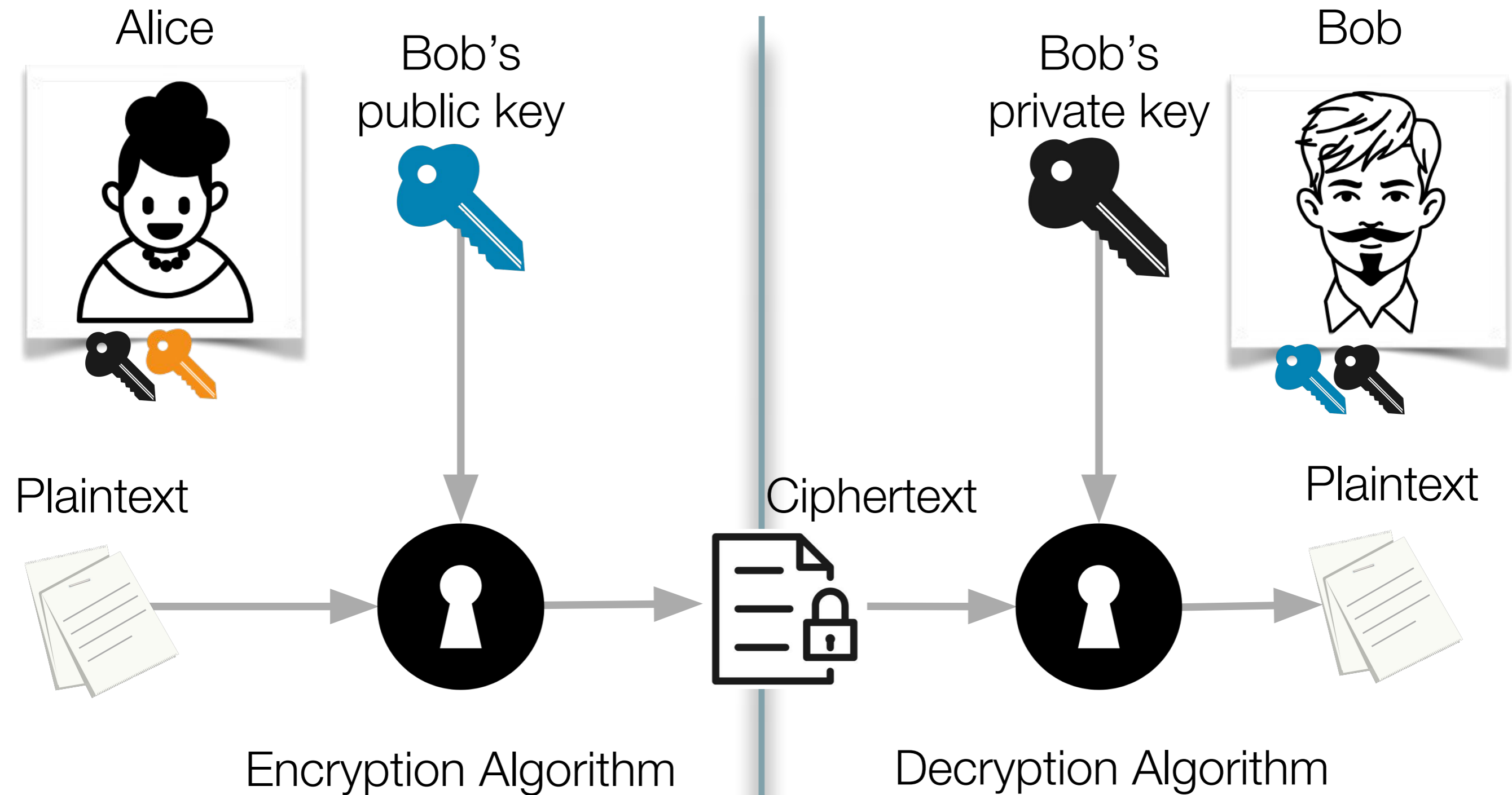
Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

HMAC Use Cases

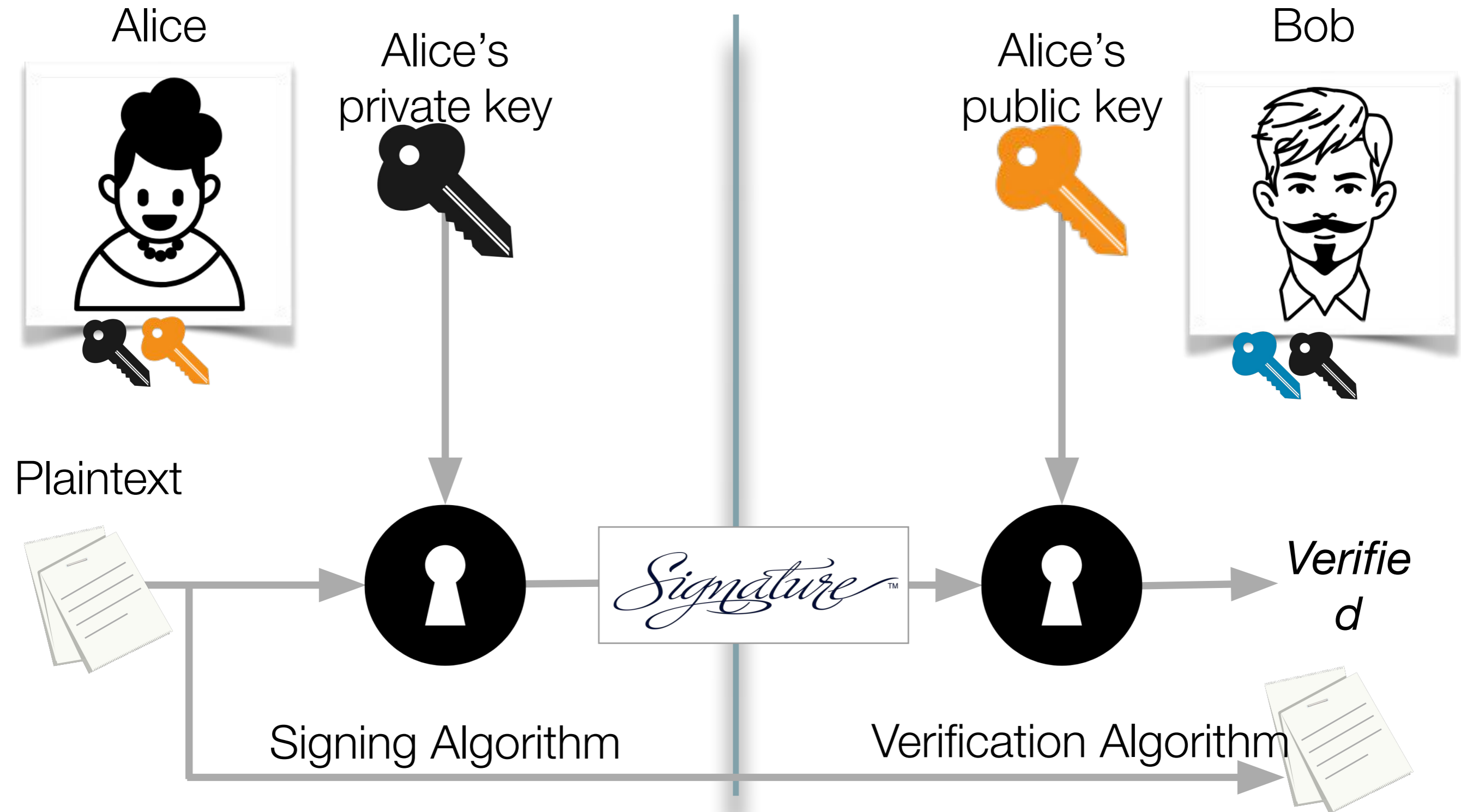
- Web browser message integrity (HTTPS)
- Integrity of messages in authentication protocols
- Cookie integrity
- Web application remote procedure calls

Public Key Encryption

Public Key Encryption Model



Public Key Digital Signature Model



Examples of Public Key Cryptography

- Diffie-Hellman
- RSA
- Elliptic Curve Cryptography (ECC)
- Identity-based Encryption (IBE)

Symmetric Encryption

Requirements

- 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

- Fast
- Assumption: 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



What can go wrong?

- Key

- Too big

- Slow

- Storage

- Too small

- Vulnerable to brute force attack – try all possible keys



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

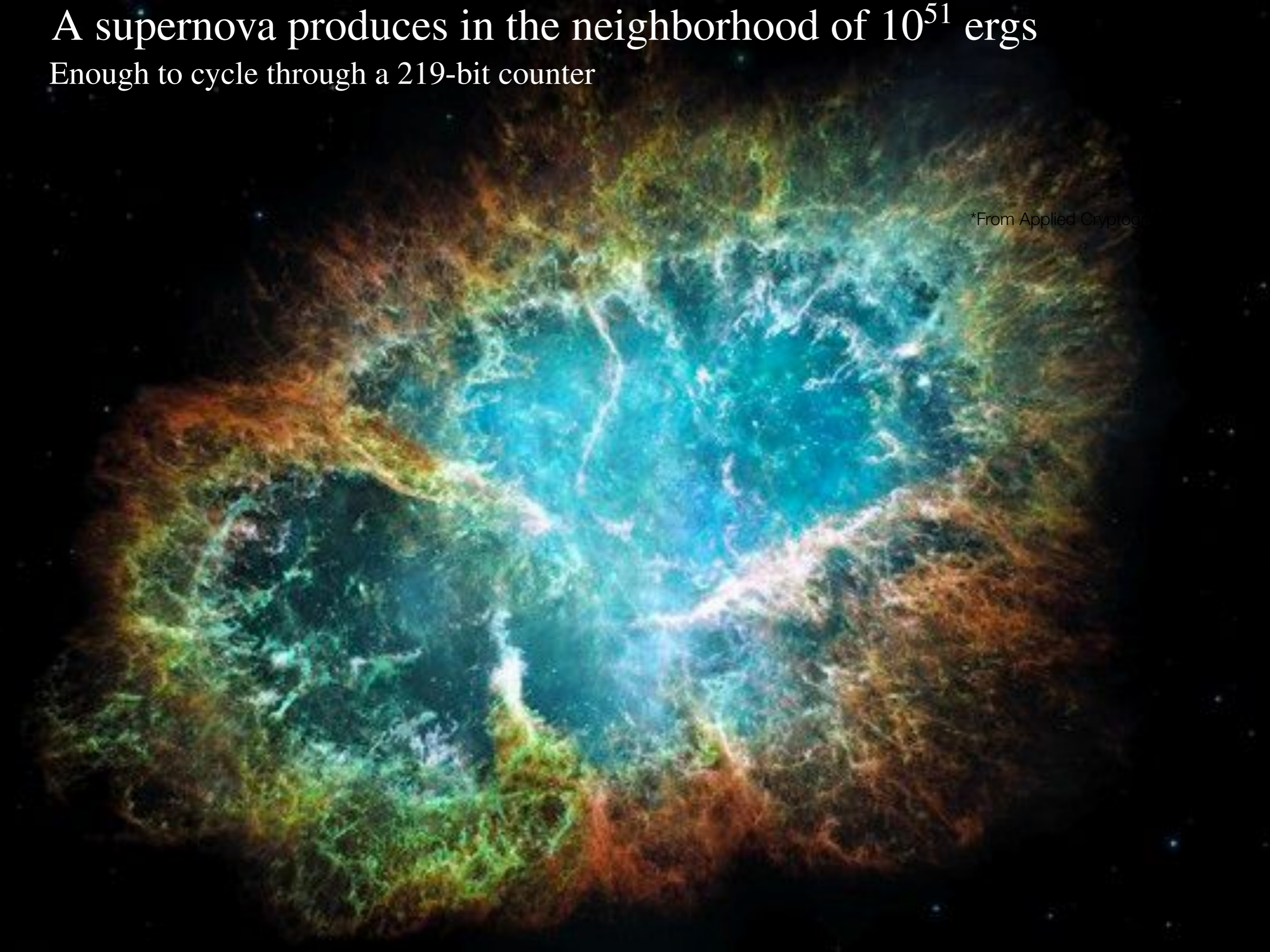
Thermodynamic Limitations*

- Physics: To set or clear a bit requires no less than kT
 - k is the Boltzmann constant (1.38×10^{-16} erg/°K), T is the absolute temperature of the system
- Assuming $T = 3.2^\circ\text{K}$ (ambient temperature of universe)
 - $kT = 4.4 \times 10^{-16}$ 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.

A supernova produces in the neighborhood of 10^{51} ergs

Enough to cycle through a 219-bit counter

*From Applied Cryptography



Assignment

- Review this slide deck regularly to learn the high level abstractions for these primitives. I'll expect you to describe them to me on an exam without any notes.
 - You don't really know something until you can teach it to someone else
- Study the AES NIST spec and watch the YouTube demo