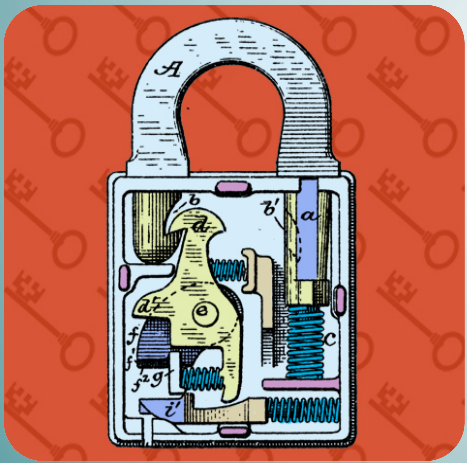
Garantía y Seguridad en Sistemas y Redes

Tema 2. Cryptographic Tools



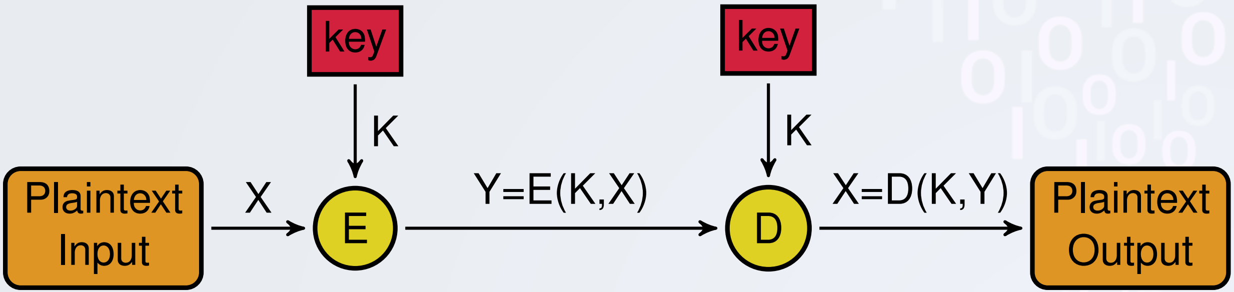
Esteban Stafford

Departamento de Ingeniería
Informática y Electrónica

Contents

What can cryptography do?

- Confidentiality ✓
- Integrity ✓
- Availability ✗
- Authenticity ✓
- Accountability ✓



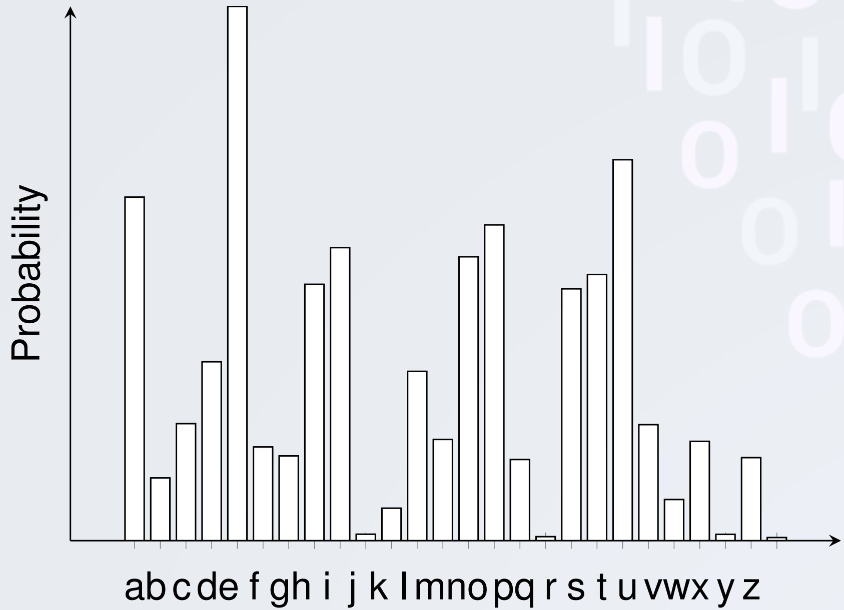
Caesar Cypher

- Named after Julius Caesar, although used long before.
- Representative of the substitution cypher algorithms.
- The encryption process shifts each letter a number of places. (key)
- Easily attackable by brute force.

Substitution Cypher

- The key is a substitution table.
- The encryption changes each letter by the corresponding in the table.
- Infeasible to break by brute force.
- Breakable by cryptanalysis.

Substitution Cypher



- Working examples of old cyphers
  - http://simonsingh.net/The_Black_Chamber/chamberguide.html

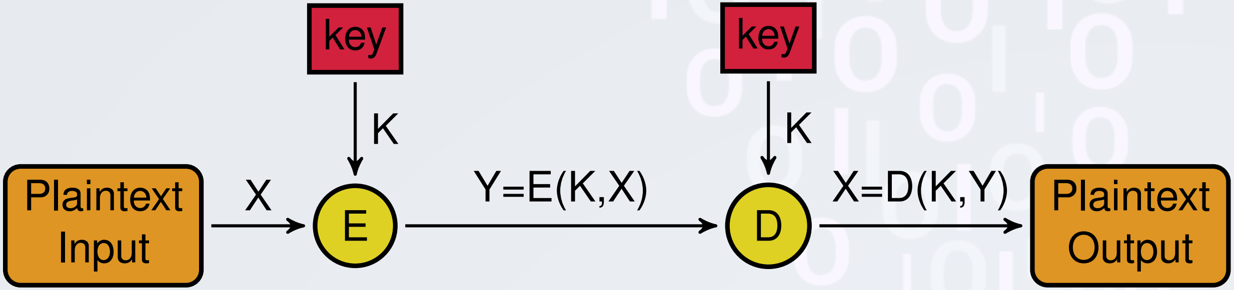
Vernam cipher

- Commonly known as One-time-pad.
- Proven to be unbreakable (Go Shannon!)
- Key must be as long as plain text and shared by peers.
- Key must me truly random and can be used only once.

Randomness

- Cryptography relies heavily on random numbers.
- Quality of random numbers
  - Uniform distribution
  - Independence
- Pseudo-random numbers
  - Mathematical modular expression derives number from the last.
  - Good distribution and price, but bad independence.
- True-random numbers
  - Monitor random or chaotic physical process.
  - Good distribution and independence, but expensive.

Symmetric Encryption

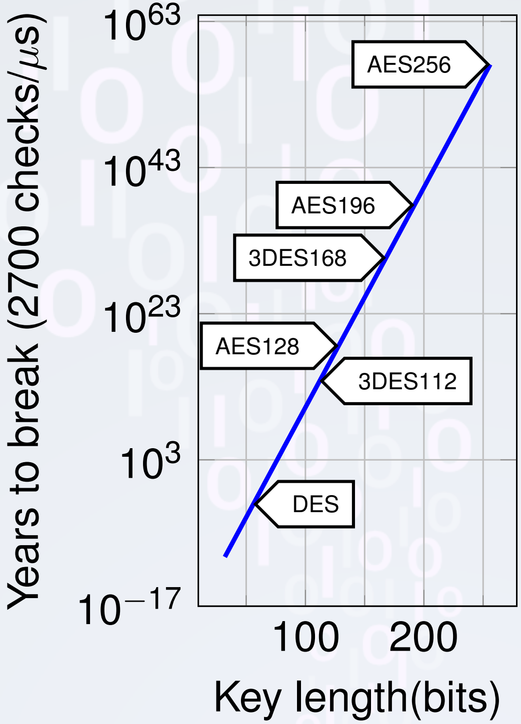


How robust is this?

- Strong encryption algorithm.
- **Cryptanalysis**: Mathematically derive X and/or K from Y. Or simplify brute-force.
- Keys subject to brute-force attacks
- Sender and receiver must obtain keys in secure fashion.

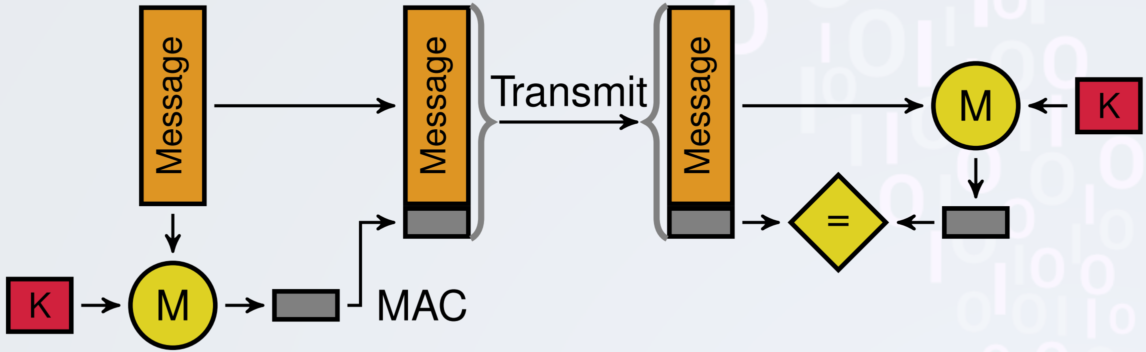
Data Encryption Standard (DES)

- 64 bit blocks, 56 bit keys. Adopted NIST 1977
- Cryptanalysis not yet successful.
- 1997: call for replacement proposals.
- July 1998: $250,000 machine cracks DES in 56h.
- Advanced Encryption Standard (AES) 128 bit blocks, 128,192,256 bit keys. Adopted 2001



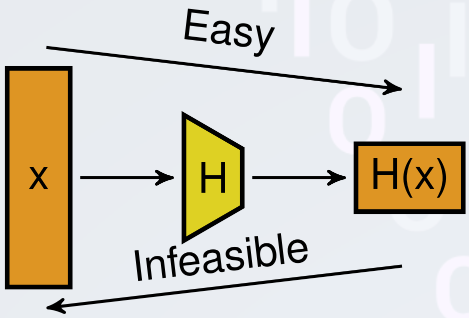
Message Authentication with Symmetric Encryption

- No confidentiality.
- Protection against falsification, alteration, delay or replay.
- Message must contain metadata: error-detection code, sequence number, timestamp.



- Message Authentication Code (MAC)
- Last 16-32 bits of DES encrypted message.

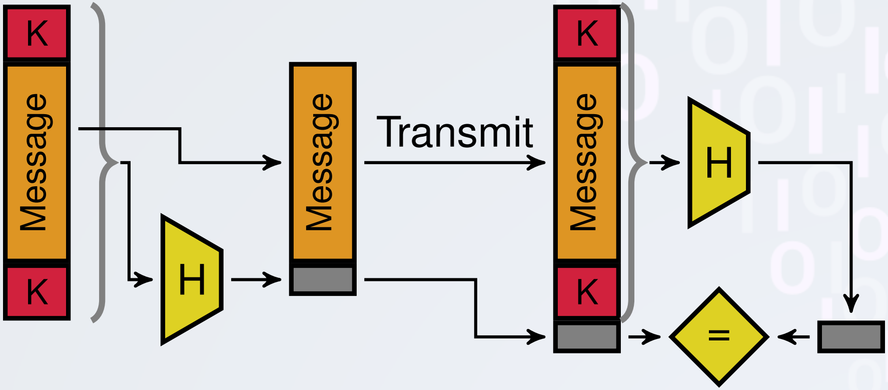
One-way Hash Functions



- x: “unlimited” size, H(x): fixed length.
- Preimage resistant: guess x from H(x).
- 2^{nd} preimage resistant: find $y \neq x$ such that H(x)=H(y).
- Collision resistant: find any x and y such that H(x)=H(y).
- Hash function crisis: RIPMED-160, SHA-256 and SHA-512.

Message Authentication with One-way Hash Functions

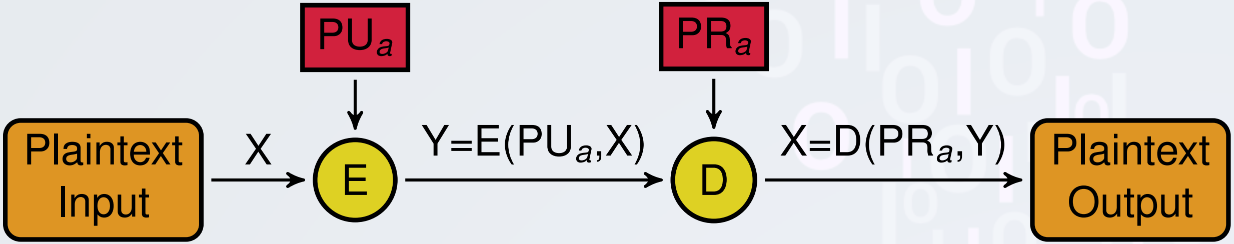
- One-way Hash Functions are faster than Symmetric Encryption
- Using shared secret value (K).



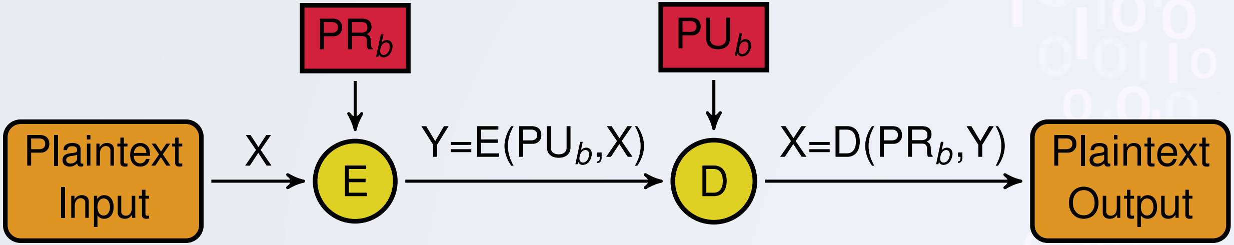
- Secure Hash Algorithm(SHA): SHA-1 160 bit long, used but weaker than expected. Currently 256, 384, 512 bit long.
- Use in password storage and intrusion detection.

Public-Key Encryption

- Proposed by Diffie and Hellman in 1976.
- Keys are created in pairs. One reverses the other.
- Bob sends confidential message to Alice.



- Bob sends authentic message to Alice.

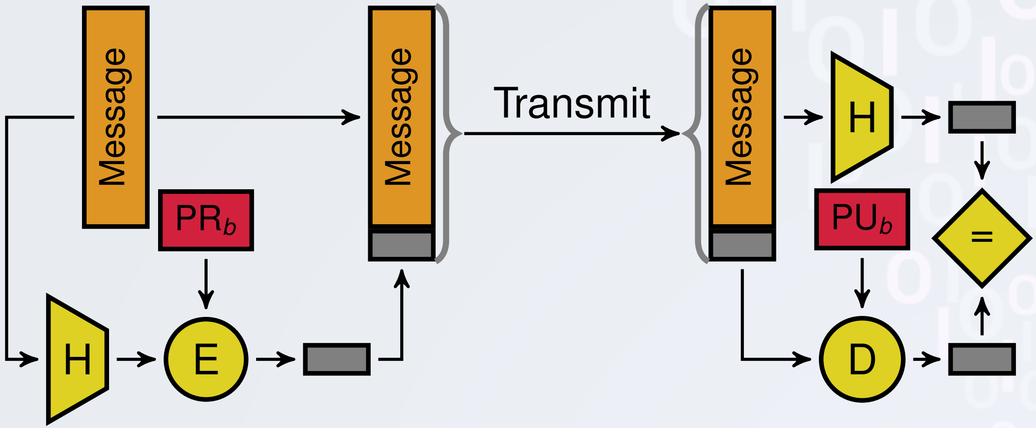


Public-Key Cryptography

- Myths:
  - Public-key encryption is more secure than Symmetric-key encryption.
  - Public-key encryption makes symmetric obsolete.
  - Public-key distribution is easier than Symmetric-key distributions.
- Implementations:
  - Rivest, Shamir and Adleman (RSA) Proposed in 1978.
  - Digital Signature Algorithm (DSA) Proposed in 1991. Stronger than RSA. Faster signing, but slower verifying.
  - Elliptic Curve Cryptography (ECC) Stronger than RSA. Allows shorter keys.

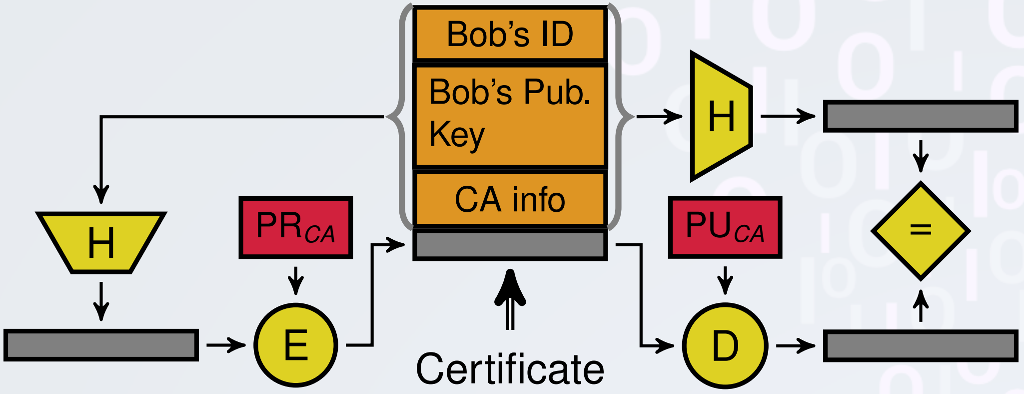
Digital Signature

- Messages can be signed by encrypting MAC with private key.



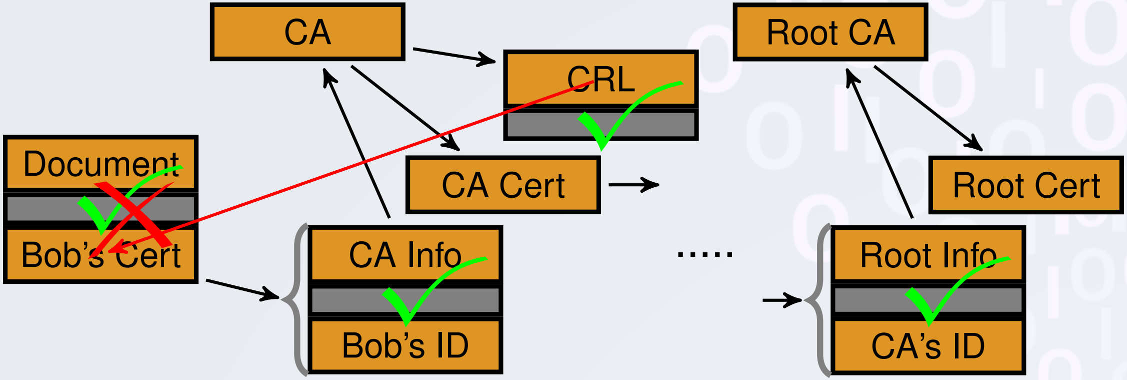
Distribution of public keys

- **Certificate Authority**(CA) signs public keys (Certificate)



- Who certifies the CA? Chicken-and-egg problem.
- **Root CAs** distribute their public keys self-signed.
- Applications and OS ship with common root certificates.

Certificate Chain of Trust



- Users can recursively validate signatures to the root CA.
- Certificate Revocation Lists(CRL) enumerate invalid certs.

SSL/TLS Handshake

Supported algorithms
Random number

Selected algorithm
Random number
Server certificate

Verify certificate
Extract server public key

Encrypt pre-master key with server public key

Decrypt pre-master key with server private key

Compute symmetric master key

Compute symmetric master key

Send checksum of handshake messages with master key

Verify checksum

Send checksum of handshake messages with master key

Verify checksum