PKI, Encryption, Certificates and You

MACTECH

Dave Hamilton

Hi, I'm Dave!

(remainder of this bio is secured)

MACTECH

Why Do People Need Encrypted Communication?

- Snoopers
  - NSA
  - Other malcontents
- Data Protection
  - At Rest
  - In Transit
  - In Use

MACTECH

Agenda

- Definitions
- Symmetric Encryption
- Assymetric Key Encryption
- PKI
- Other fun stuff

Definitions

MACTECH

Cryptography

- Techniques, technologies and protocols to secure data from all but intended parties

Encryption

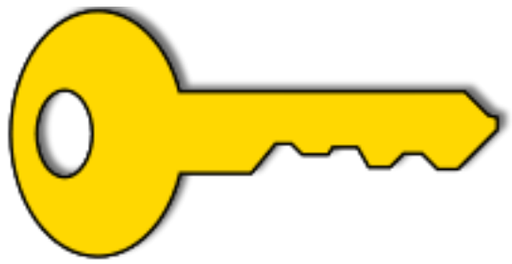
- The process of encoding data so that only intended parties can read/access it.
- Doesn't prevent hacking, just reduces the *likelihood* that a hacker can read the data.

Symmetric Encryption

MACTECH

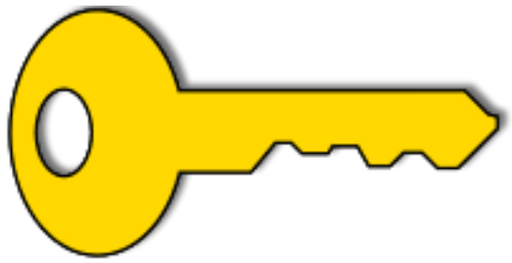
Alice and Bob

Symmetric-Key Encryption

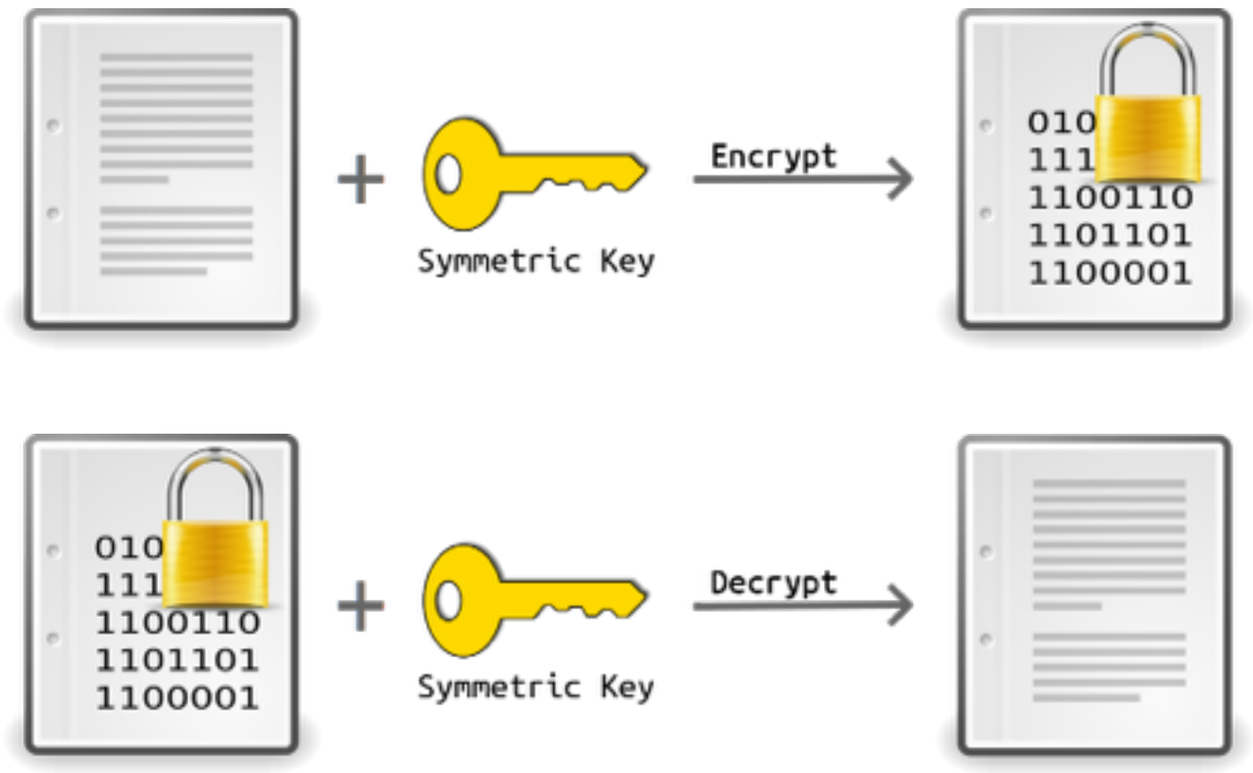


Symmetric Key

Symmetric-Key Encryption

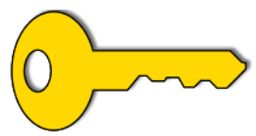


Symmetric Key



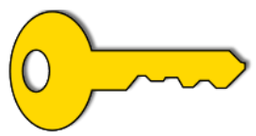
Symmetric-Key Encryption

Alice



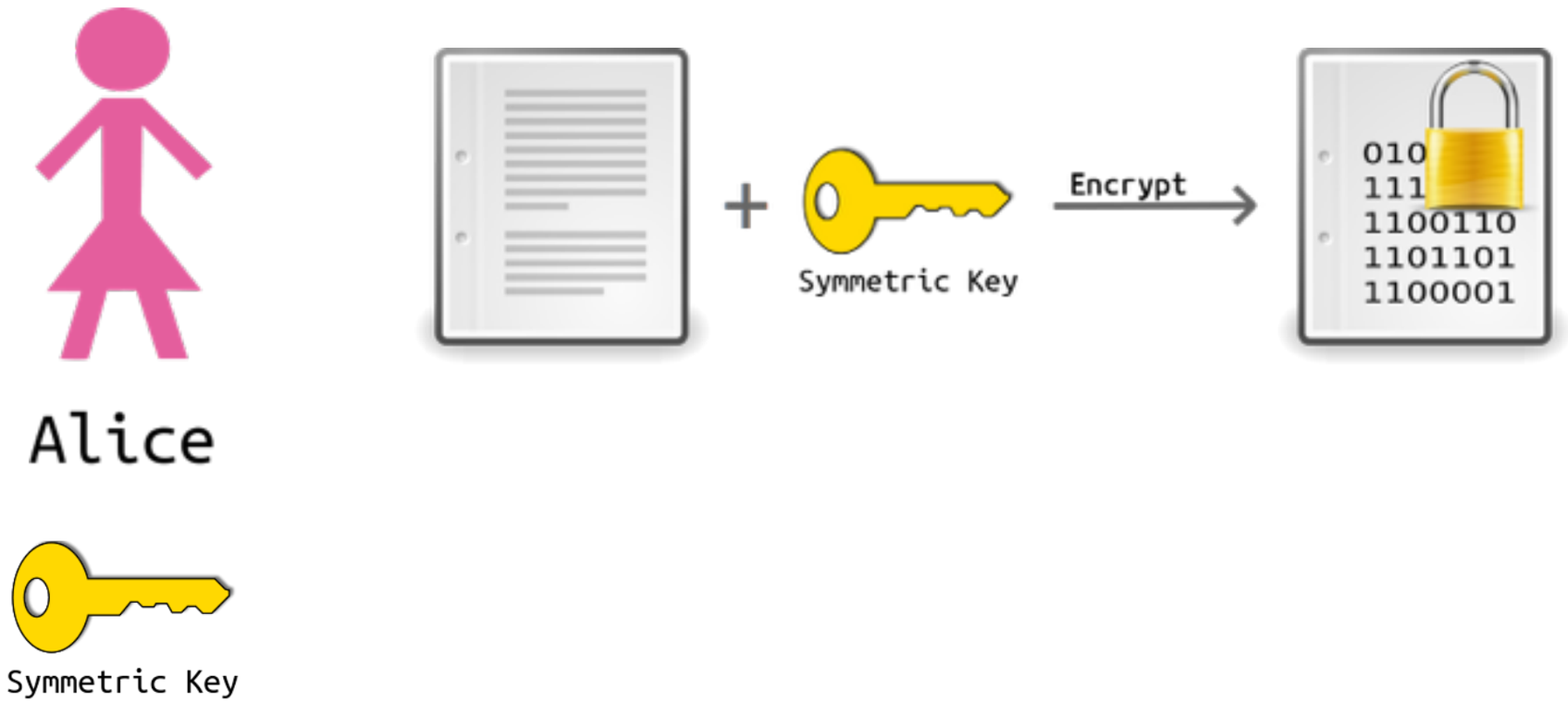
Symmetric Key

Bob



Symmetric Key

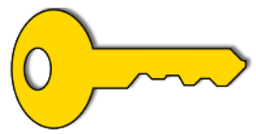
Symmetric-Key Encryption



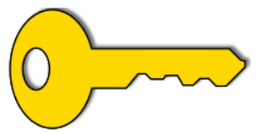
Symmetric-Key Encryption

Alice

Bob

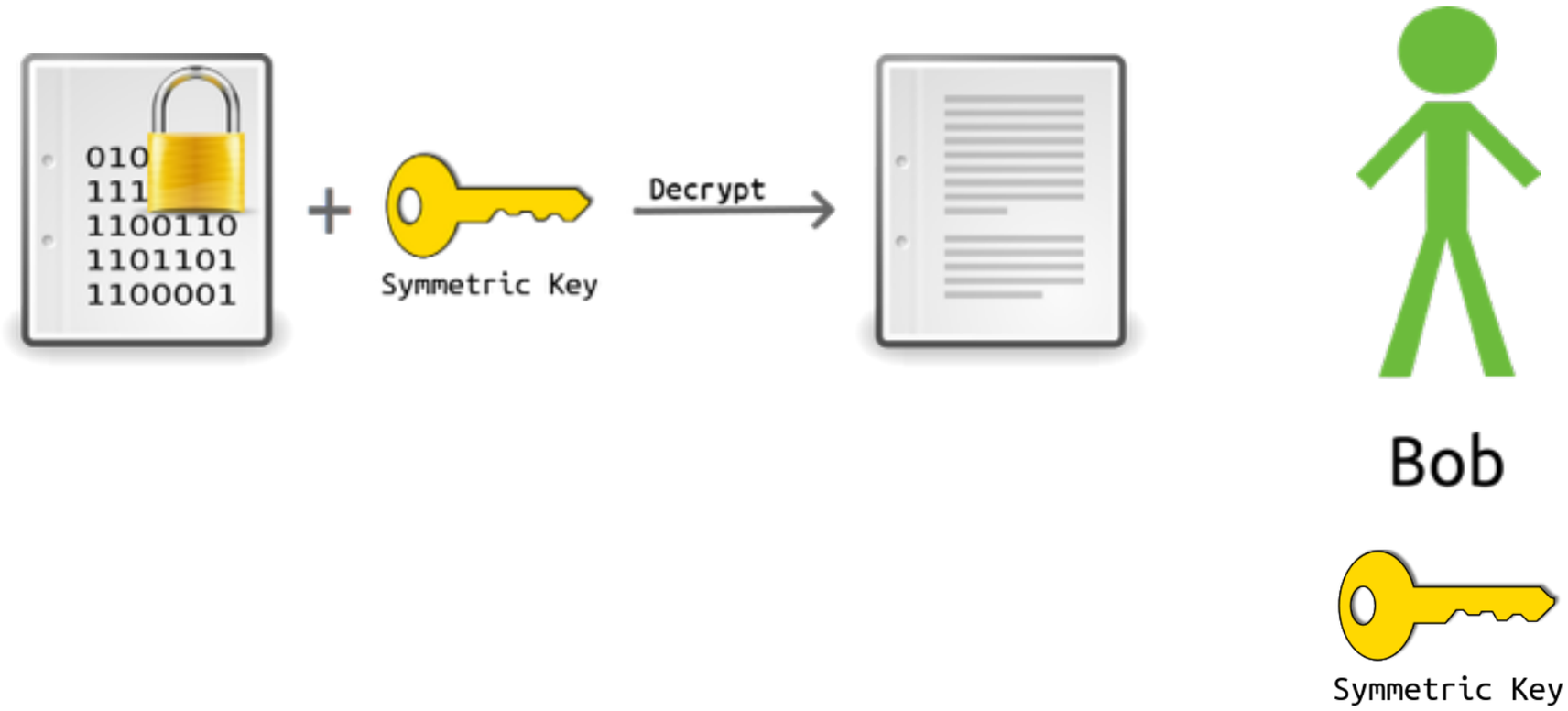


Symmetric Key



Symmetric Key

Symmetric-Key Encryption



Symmetric-Key Pros / Cons

- + Fairly Easy Math
- + Fast
- - Key Distribution

Symmetric-Key Examples

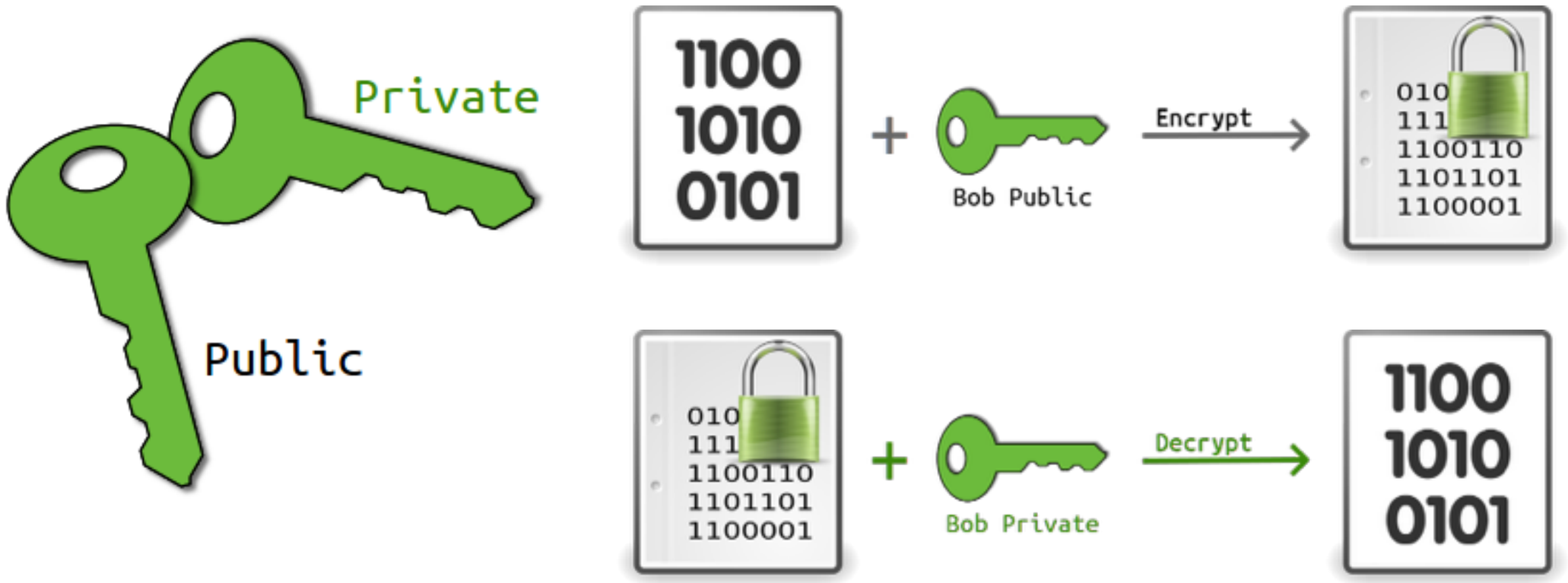
- Advances Encryption Standard (AES)
- Wi-Fi
- Secure Disk Images

Asymmetric Encryption

(a.k.a Public-Key Cryptography)

MACTECH

Public-Key Cryptography



Public-Key Cryptography

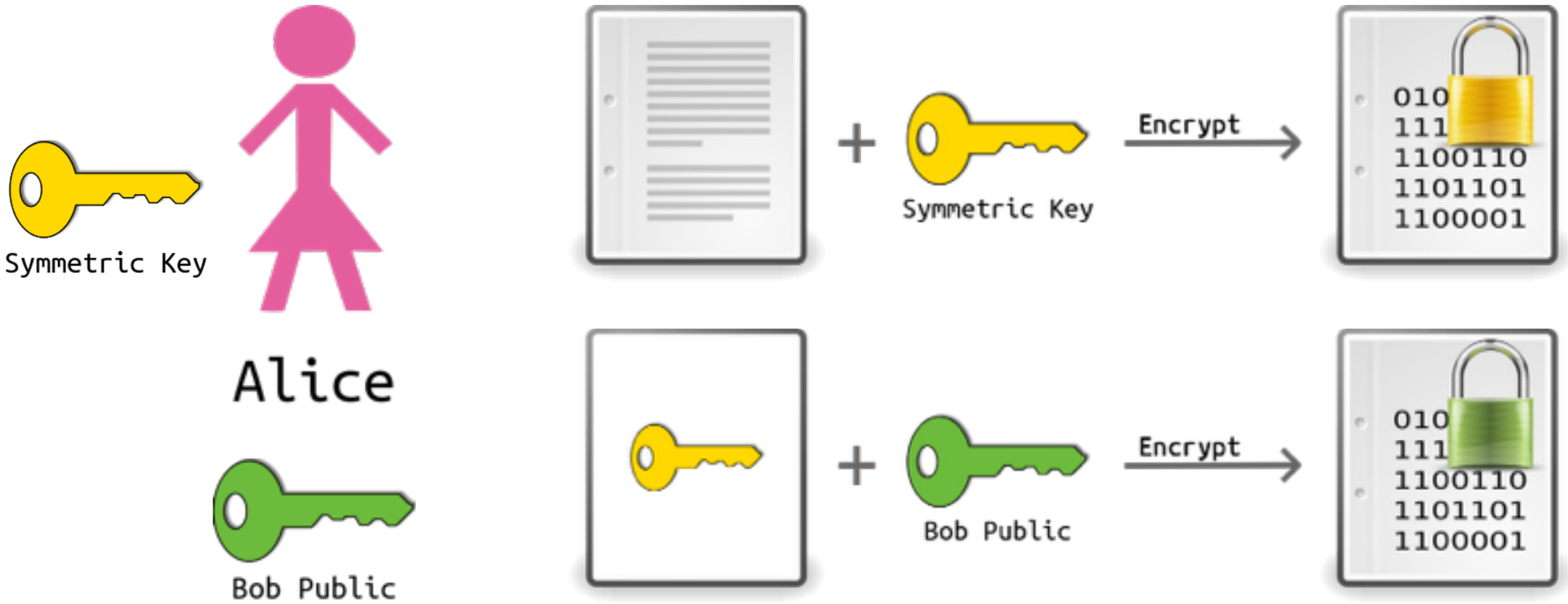
Alice

Bob Public

Bob

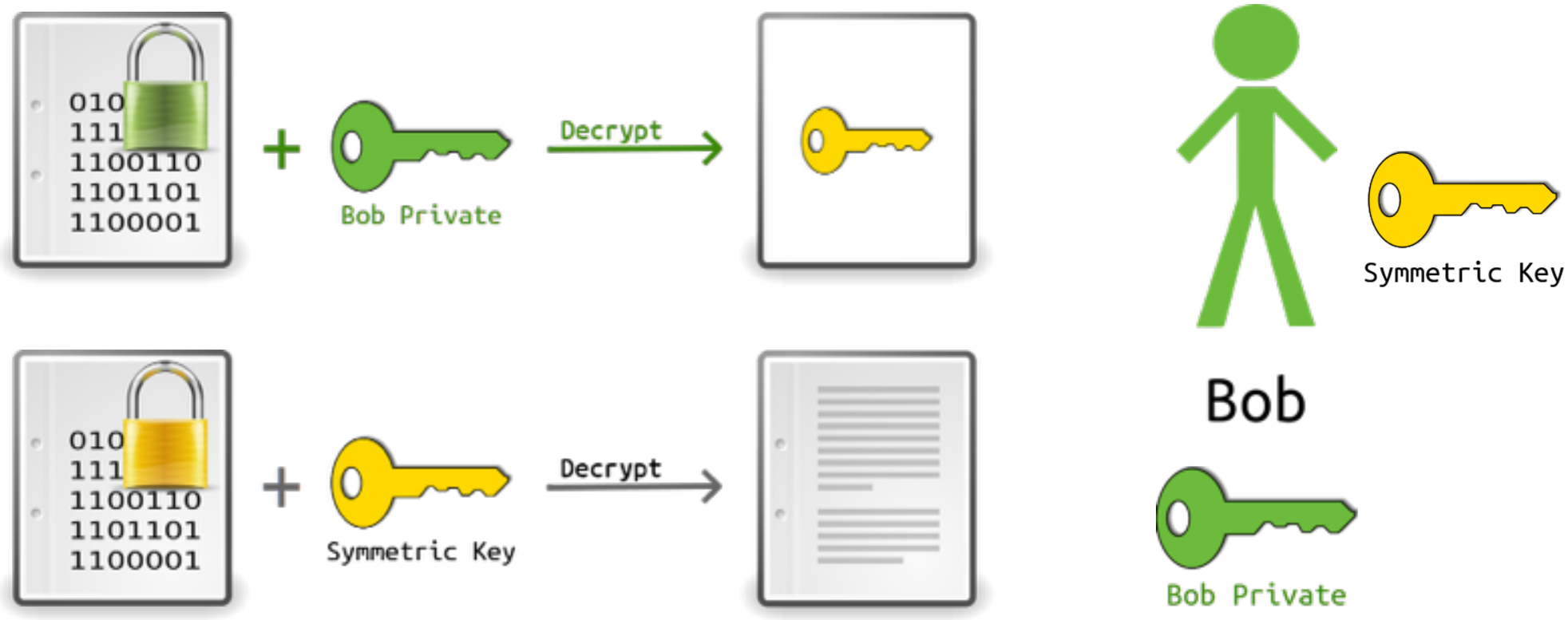
Bob Private

Public-Key Cryptography



Public-Key Cryptography

Public-Key Cryptography



Digital Signatures

(but first, let's enjoy some Hash)

MACTECH

Hash Function

Hash Function

```
1-800-977-6368
1 + 8 + 0 + 0 + 9 + 7 + 7 + 6 + 3 + 6 + 8
55
5

503-588-2941
5 + 0 + 3 + 5 + 8 + 8 + 2 + 9 + 4 + 1
45
5
```

Hash Function

Example: SHA-1 hash (20 bytes)

1-800-977-6368

859d925489b53f266a5103f168a7bdbccdf99ca2

503-588-2941

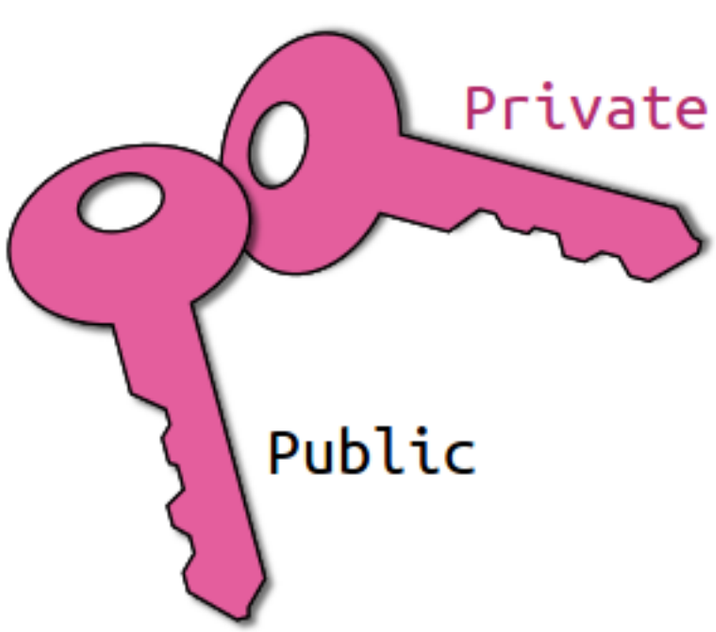
c66f132b9aaf20232afecc317f9e25c2ac692634

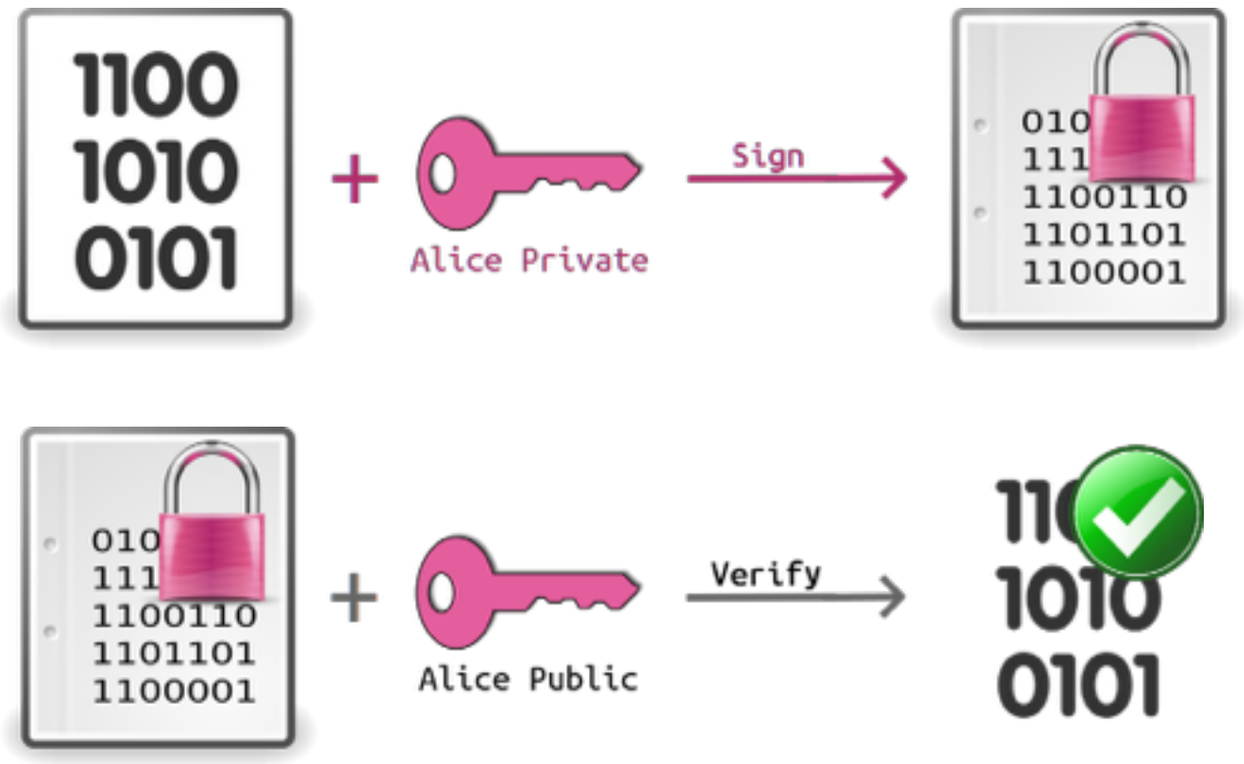
Hash Function

- With a cryptographic hash, it should be:

1. “Impossible” to change the input data without changing the output hash
2. “Impossible” to create two inputs that result in the same output hash

Digital Signature





Digital Signature

Alice

Alice Private

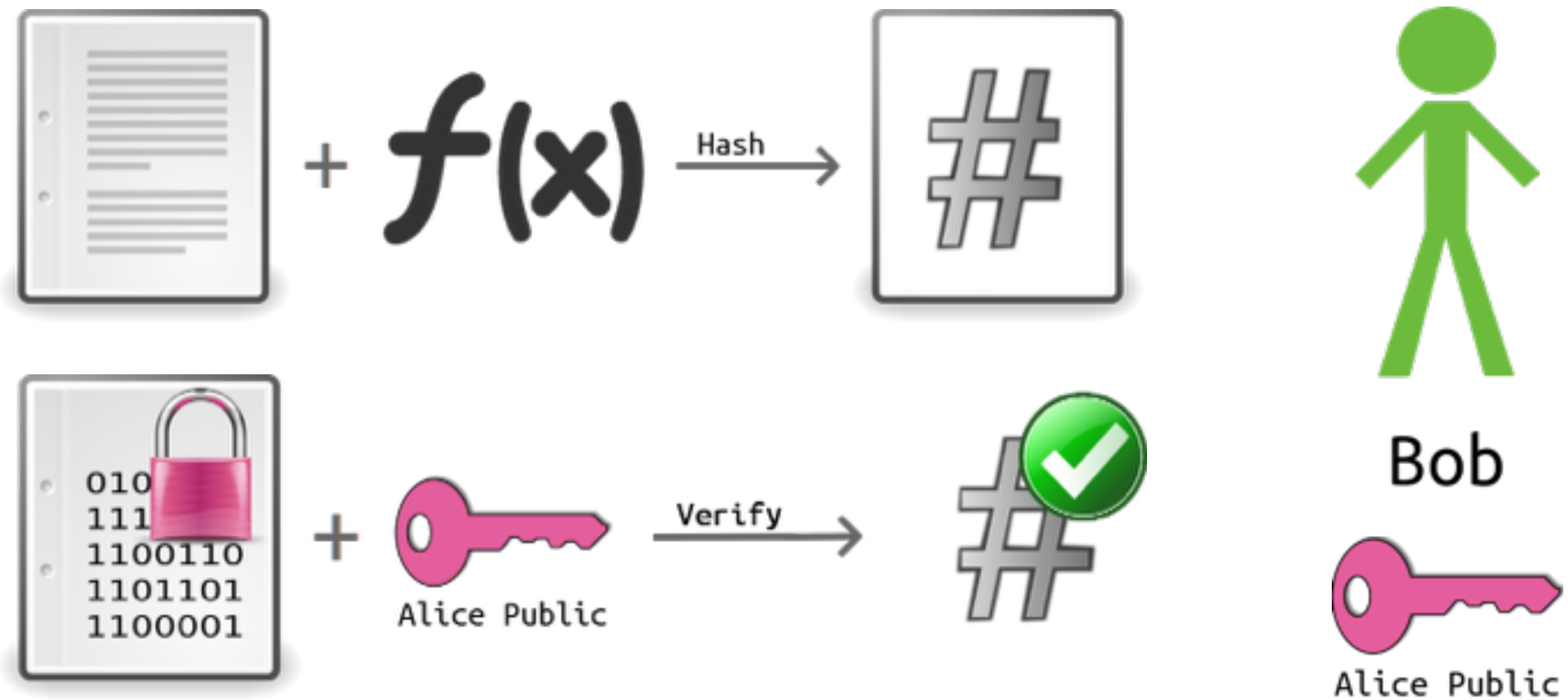
Bob

Alice Public

Digital Signature

Digital Signature

Digital Signature



Sign then Encrypt

Alice

Alice Private

Bob Public

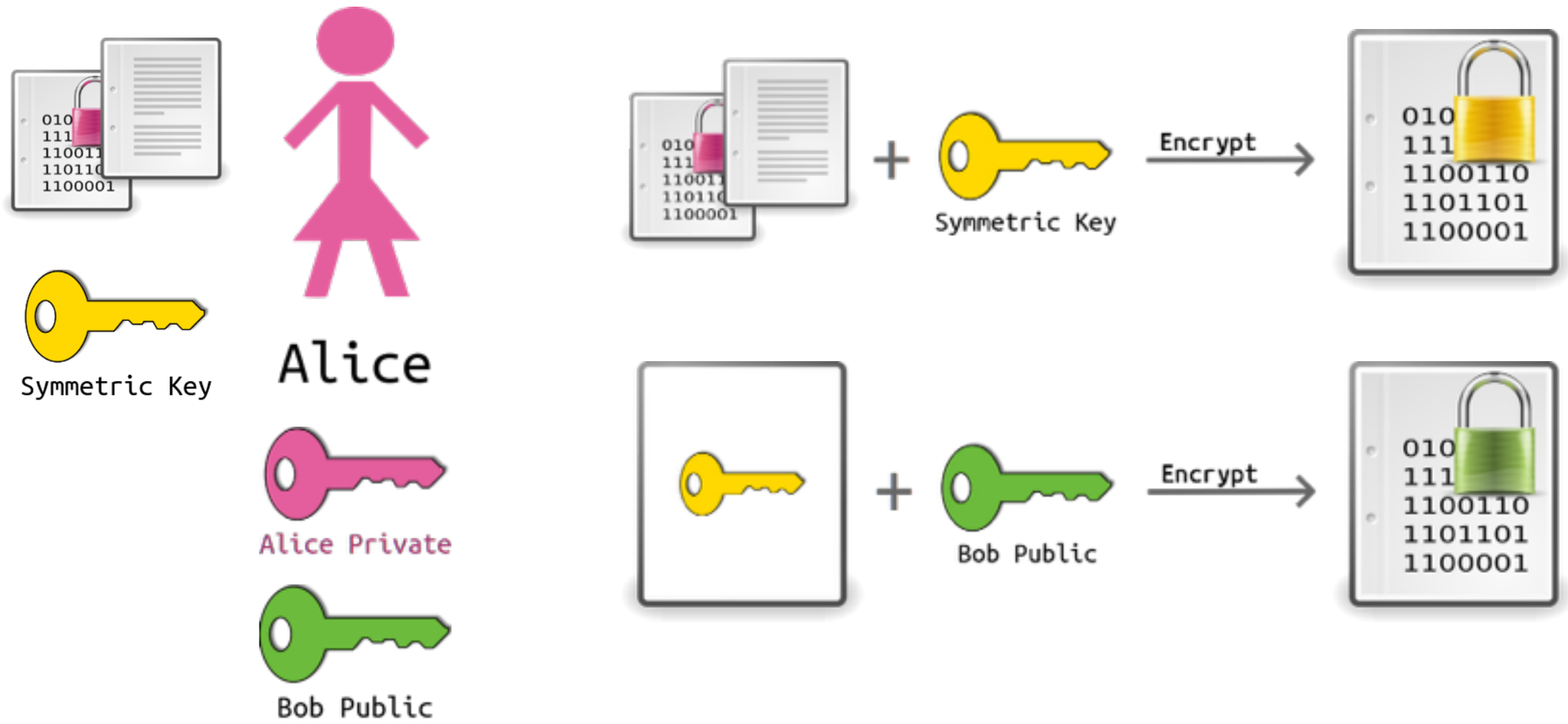
Bob

Bob Private

Alice Public

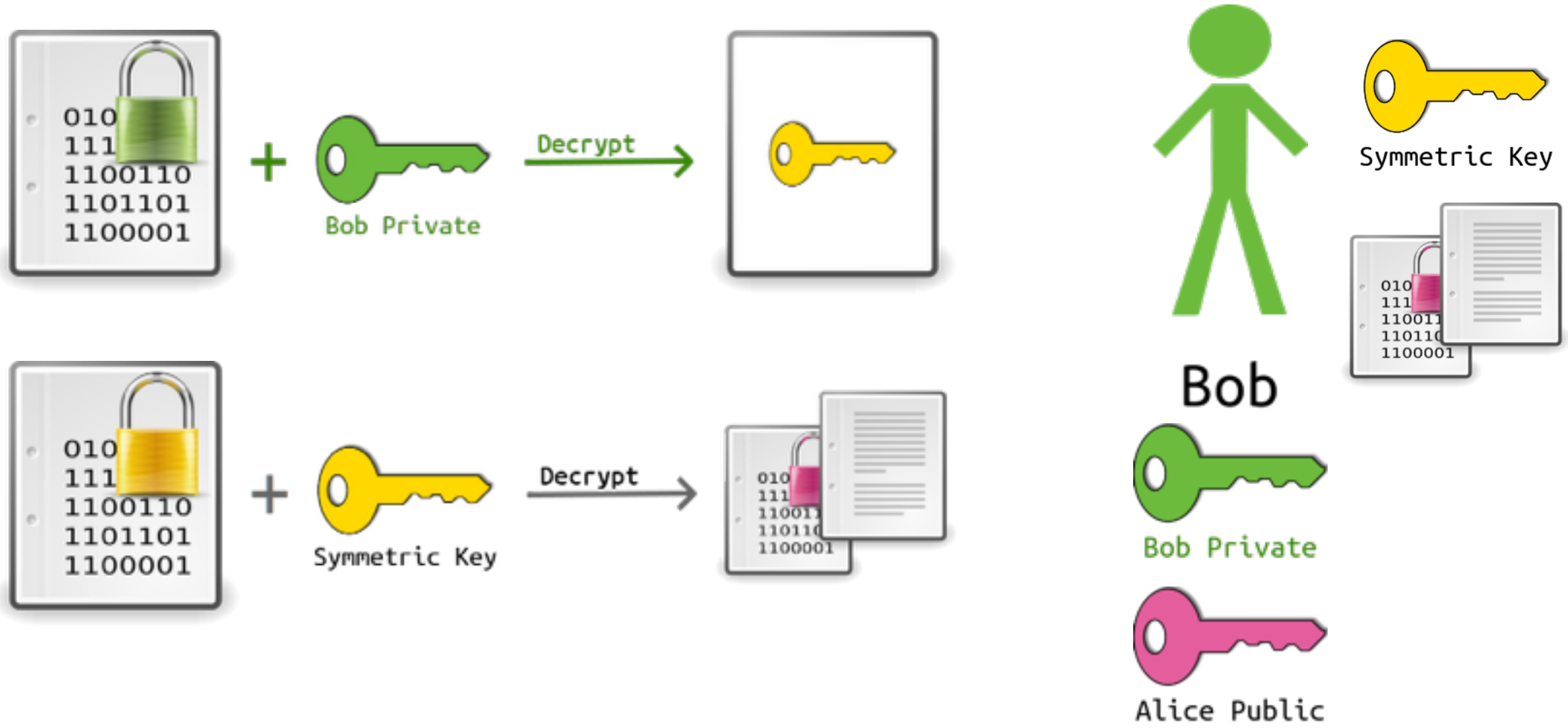
Sign then Encrypt

Sign then Encrypt

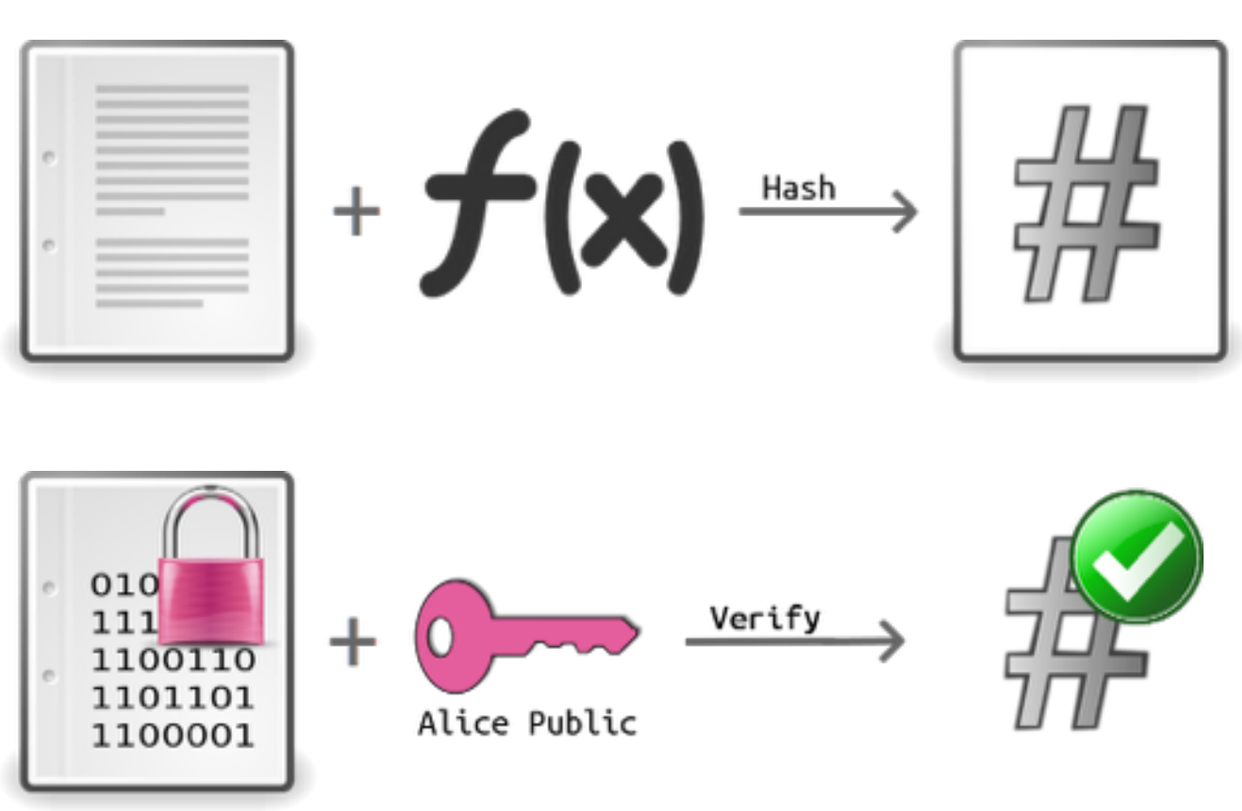


Sign then Encrypt

Sign then Encrypt



Sign then Encrypt



Sign then Encrypt

- Did somebody re-encrypt it?
- You can sign, encrypt, then sign again
- Don't encrypt then sign:
  - What did you sign?
  - Was it yours to sign?

PKI

MACTECH

What is PKI?

- Manage trust by delegation
- Technical and human
- X.509 ITU-T standard
- Public and private
- Manage certificates

MACTECH

PKI Parts

- Servers
- Services
- People
- Policies
- Procedures
- Many…

MACTECH

Relevant PKI Parts

- Certificates
- Certificate Signing Requests (CSRs)
- Certificate Authorities (CAs)
- Intermediate CAs
- Trusted roots/X.509 anchors

Certificate

- Public key
- Identity information
- Extensions
- Signed by a CA*

Certificate Signing Request

- Certificate
- No private key
- Sent to CA

Certificate Authority

- Signs certificates
- Indicates their trust in you
- “Are you who you say you are?”
- “Are you trustworthy?”
- Add identity and extensions

MACTECH

Certificate Authority

- Public/private key pair
- Signs certificates with its private key
- Signature verified with its public key
- Keys to the kingdom

Intermediate CA

- Delegate signing authority
- “Chain up” to a Root CA
- Control risk

Trusted Roots

- Well-known CAs and Intermediates
- Distributed with OS or browser
- You will trust any cert that chains up to one of your trusted roots*
- Told who to trust

MACTECH

How Certificates Work

2 Are you really https://www.pretendco.com?

www.pretendco.com

3

Yes, here is my certificate and public key.

5

Yep

Certificate granted to www.pretendco.com

1

4 Is this certificate valid?

MACTECH

http://support.apple.com/kb/HT5012

SSL/TLS

- Secure Sockets Layer (old)
- Transport Layer Security (new)
- Do you trust the identity of the server?
- Asymmetric cryptography (slow math)
- Secure key exchange
- Symmetric cryptography (fast math)

Code Signing Certificates

- Digital signature for executables and scripts
- Confirms software author
- Using cryptographic hash, guarantees code is not altered.

Code Signing vs. SSL Certificates

- SSL certificates are for website and application server authentication
- Code Signing is for authenticity and integrity verification of executables

Cool Stuff Found

MACTECH

s/mime

- Secure/Multipurpose Internet Mail Extensions
- Public key encryption and signing of MIME data
- Simply put, enables sending or receiving encrypted messages, usually via email
- Built-in to OS X and iOS
- Awesome Setup Tutorial: http://www.podfeet.com/blog/tutorials-5/how-to-set-up-signed-and-encrypted-email/

PGP and GPG

- Pretty Good Privacy and
  Gnu Privacy Guard
- Signing, Data encryption and decryption
- PGP often used for text, emails, files, etc…
- GPG Tools for Mac (integrates with Mail.app)
  - Free
- iPGMail for iOS
  - $1.99

Two-Factor Authentication

- Two step identity verification process
- Non-Computer Example: An ATM requires a card and a PIN to verify identity
- Google Example: Login (username/password) and physical possession of mobile device at time of authentication

File Vault 2

- Mac specific volume encryption method
- Entire startup volume
- Encryption and decryption done on the fly
- Limitations on backup solutions
- Not infallible

Questions?

Or Maybe we don't have time?

Dave Hamilton
dave@macobserver.com

MACTECH