Digital Signatures & Encryption for Email

Gary Windham
Systems Integration & Architecture
UITS

Topics

- Why should I care?
- How does it work?
- Demos

What does “secure email” mean?

- Message confidentiality
- Message integrity
- Sender verification
- Non-repudiation

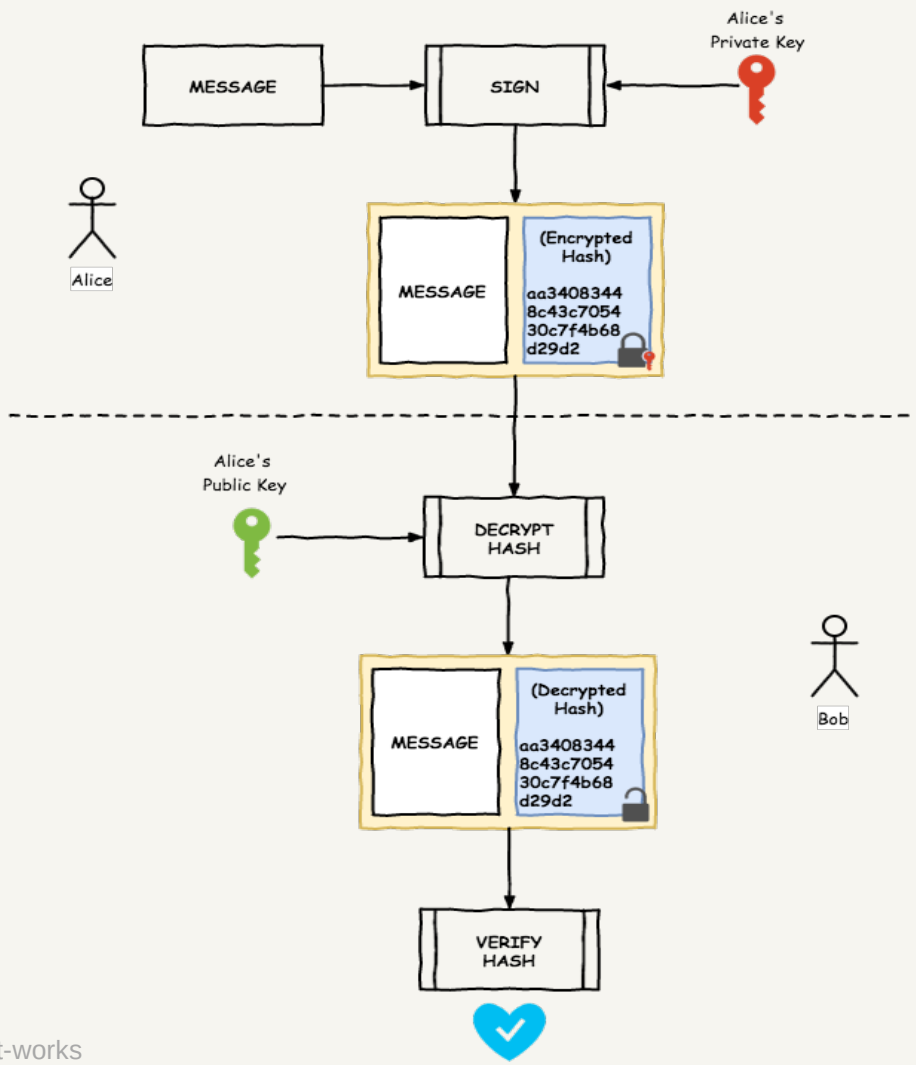
What are the benefits?

- Enhanced trust (sender verification)
- End-to-end protection of sensitive/private data
- Message contents are opaque — protect message from spam and attachment filtering

A (very) brief intro to S/MIME

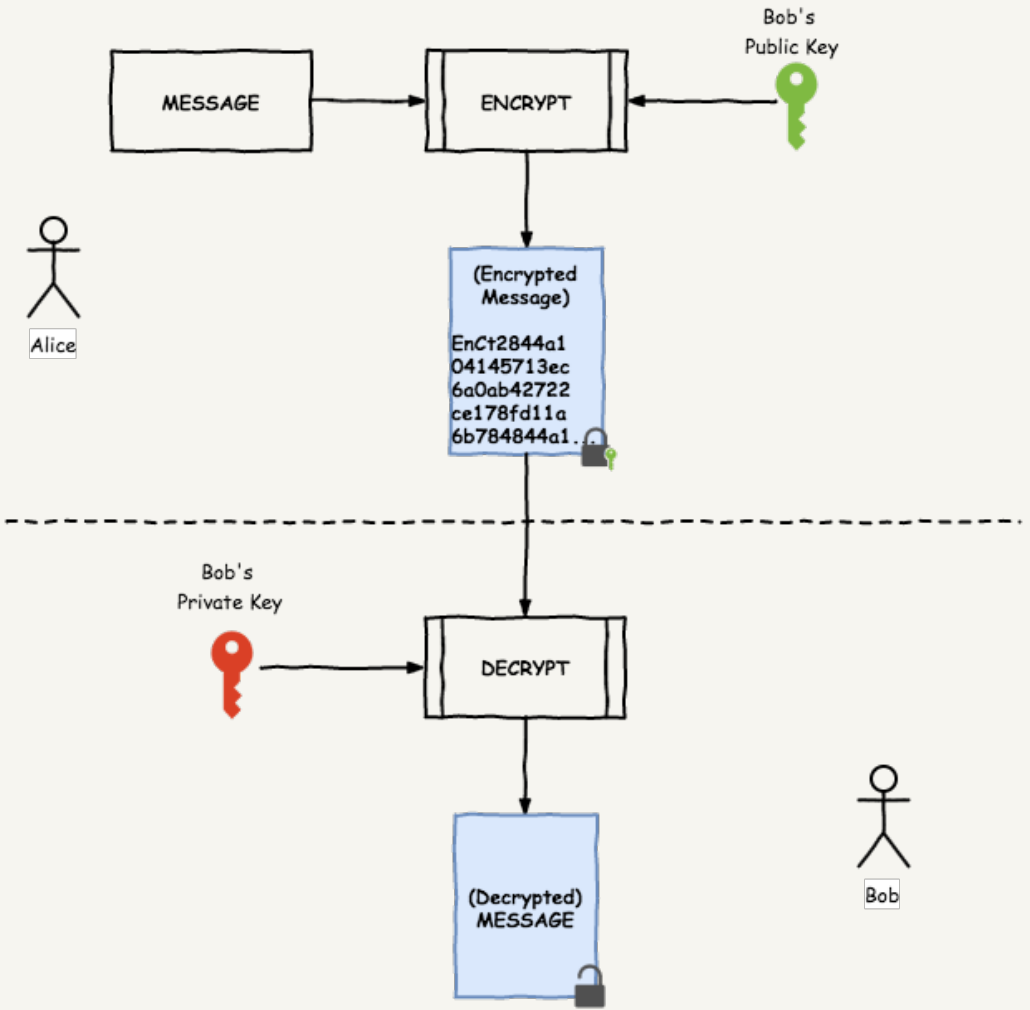
- **S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions
- Introduced by RSA Data Security in 1994
- IETF standard, relying on other IETF standards
- Predicated on PKI
- Supported by most modern desktop email clients

Signing



Credit: https://www.vikramrao.in/12/SMIME-:-How-it-works

Encryption



Source: https://www.vikramrao.in/12/SMIME-:-How-it-works

Where are my keys?

- *Public* key carried in X.509 certificate
- *Private* key stored in separate file, typically password-protected
- For client convenience, these two components are usually stored together in PKCS #12 file

How do I find my contacts' public keys (and vice-versa)?

- Two main approaches:
  - Sending signed (but not encrypted) email to contact
  - Retrieving pubic key from directory service (e.g., Exchange GAL)

Which email clients support S/MIME?

- Most major desktop email clients
- Web-based email:
  - Outlook Web App (Internet Explorer only)
- Mobile email clients
  - iOS Mail app
  - Android – varies by mail client, OS version, device

Where do I get a certificate?

Installing and using a certificate

(Demo)

Resources

- https://certificates.arizona.edu
- https://stache.arizona.edu
- https://confluence.arizona.edu/display/SIA/Digital+Certificates

Thanks!

Q & A?