(Un)Usability of Email Encryption

Ann Fry, standing in for Anil Somayaji

School of Computer Science
Carleton University

Ottawa, Canada

Carleton
UNIVERSITY

Outline

How Email Works: Email Insecurity

Current Technologies

Mail Setup Walkthrough

- S/MIME

- PGP

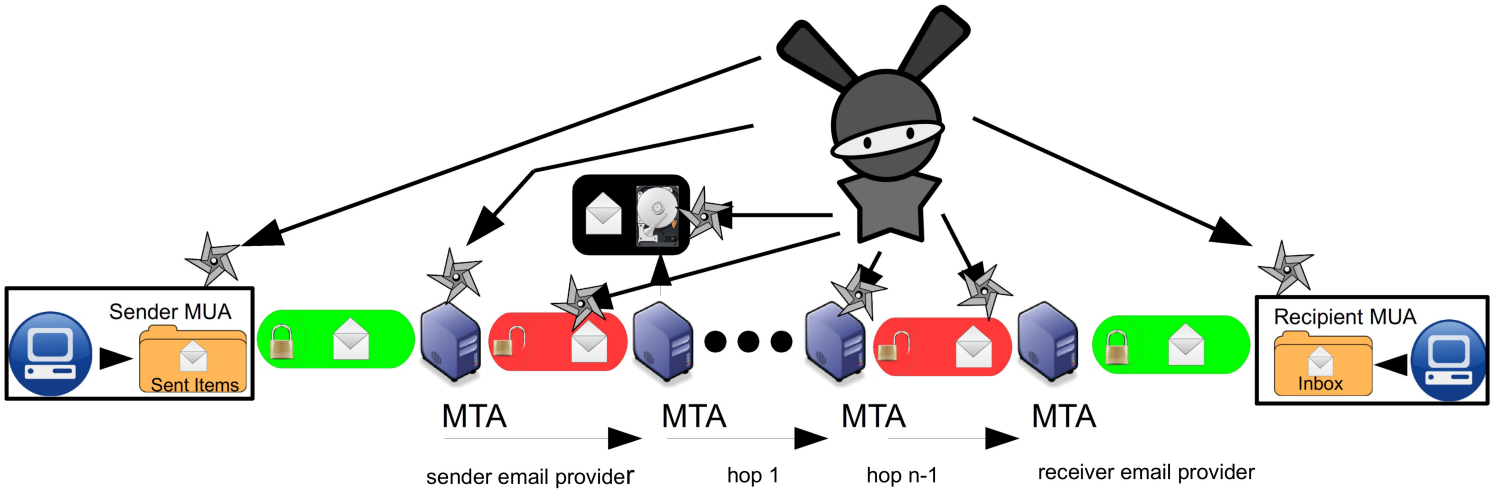
Insecurity of Email

- Most email is sent in plaintext
- SMTP is a store and forward protocol
- Hops may use point-to-point encryption
- Analog days: passing notes in class

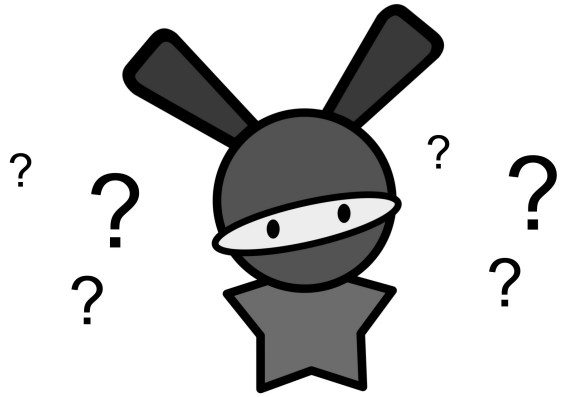
Basic Technologies, aka the Acronyms

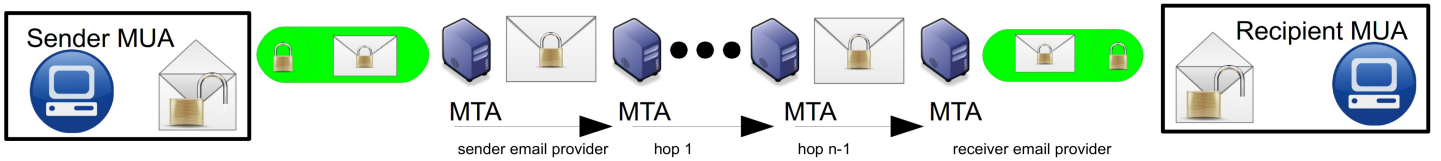
- End to End Encryption: PGP (Zimmerman, 1993) and S/MIME (Ramsdell, V.3, 2004)

- Point to Point Encryption: SSL/TLS



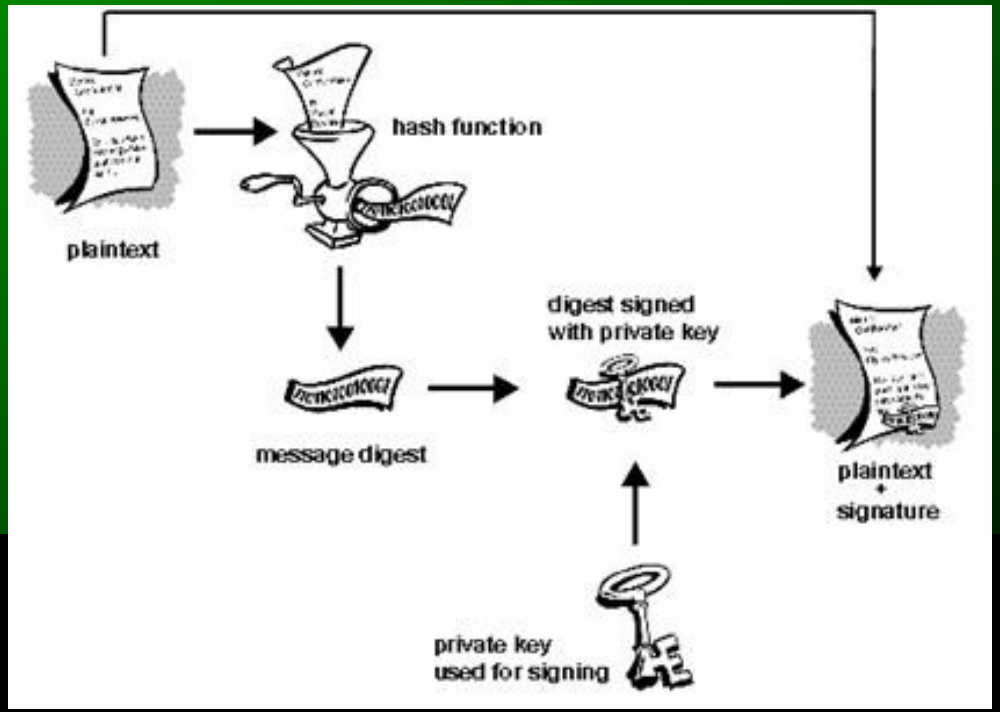
Point to Point vs. End to End



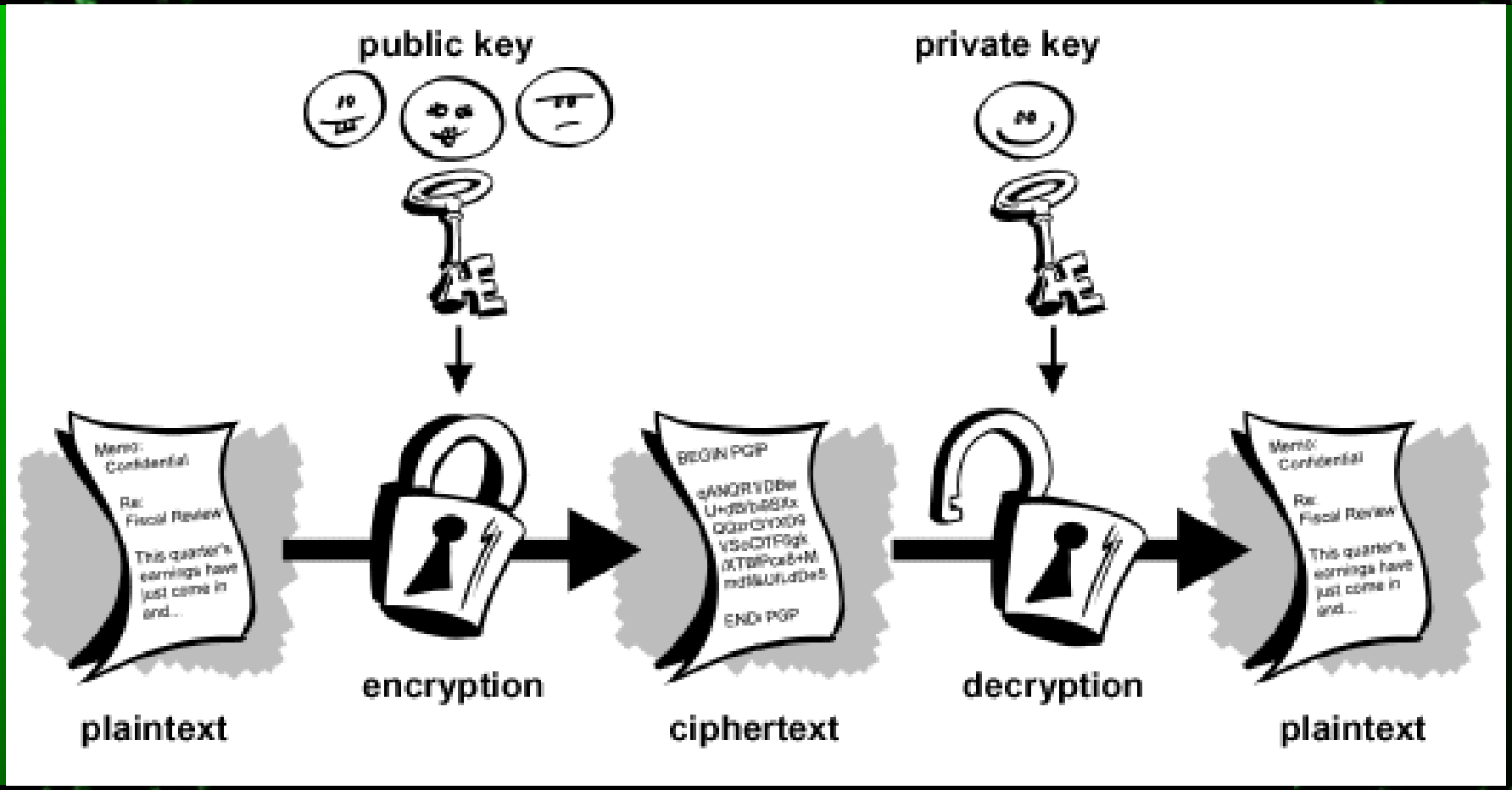


Public Key Cryptography

- asymmetric – a public key and a private key
- encryption schemes (e.g. RSA, El-Gamel)
- Digital signature



Mail Encryption



Edward Snowden / NSA

- Current events warn “netizens” how to preserve both privacy and integrity of communications.
- Links:
  - http://www.huffingtonpost.com/zachary-graves/the-nsas-war-against-encr_b_3901328.html
  - http://news.nationalpost.com/2013/09/06/nsa-secret-supercomputers-broke-encryption-codes-partnered-with-tech-companies-for-software-back-doors-reports/

Why don't we encrypt email?

- Although the technology is there, no one is using it

- 13 years later, we are still asking why users do not encrypt their email?

Questions & Thanks :)

Thank you for listening.

Any Questions?