The Implications of Encryption

Curtis A. Carver Jr. and John M.D. Hill
Department of Electrical Engineering and Computer Science
United States Military Academy

Agenda

Underlying Technologies

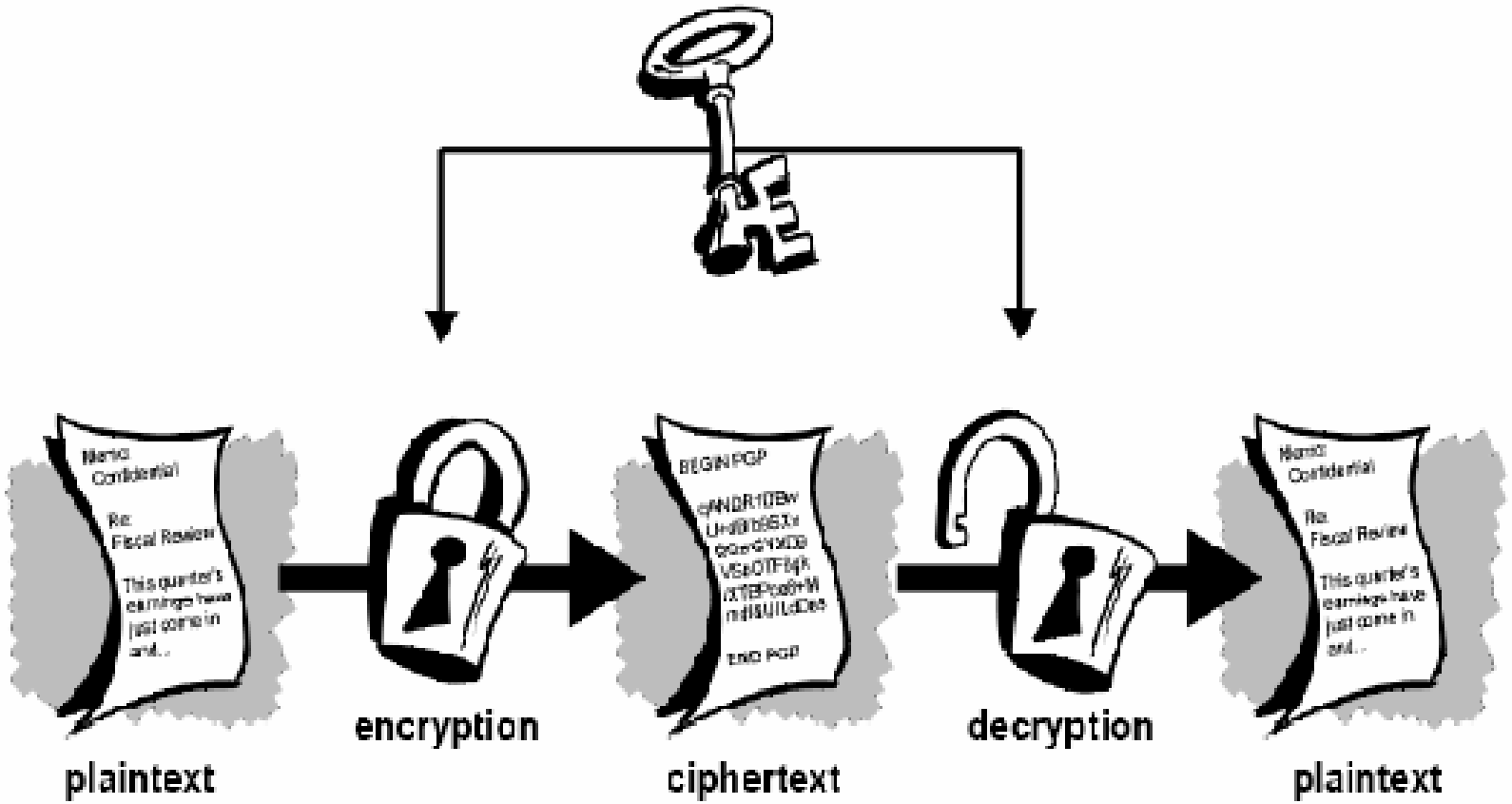
- Symmetric Encryption
- Asymmetric Encryption
- Digital Signatures
- Digital Certificate
- Hash Functions
- Public Key Infrastructure
- PGP Example

Implications

- It's everywhere, it's everywhere!
  - Encryption
  - Computing Devices
- Moore's Law, Quantum Computing, & Virtual Bears, Oh My!
- End of the Code Breakers?
- Let's Get Ready to Rumble! Privacy vs. Authentication

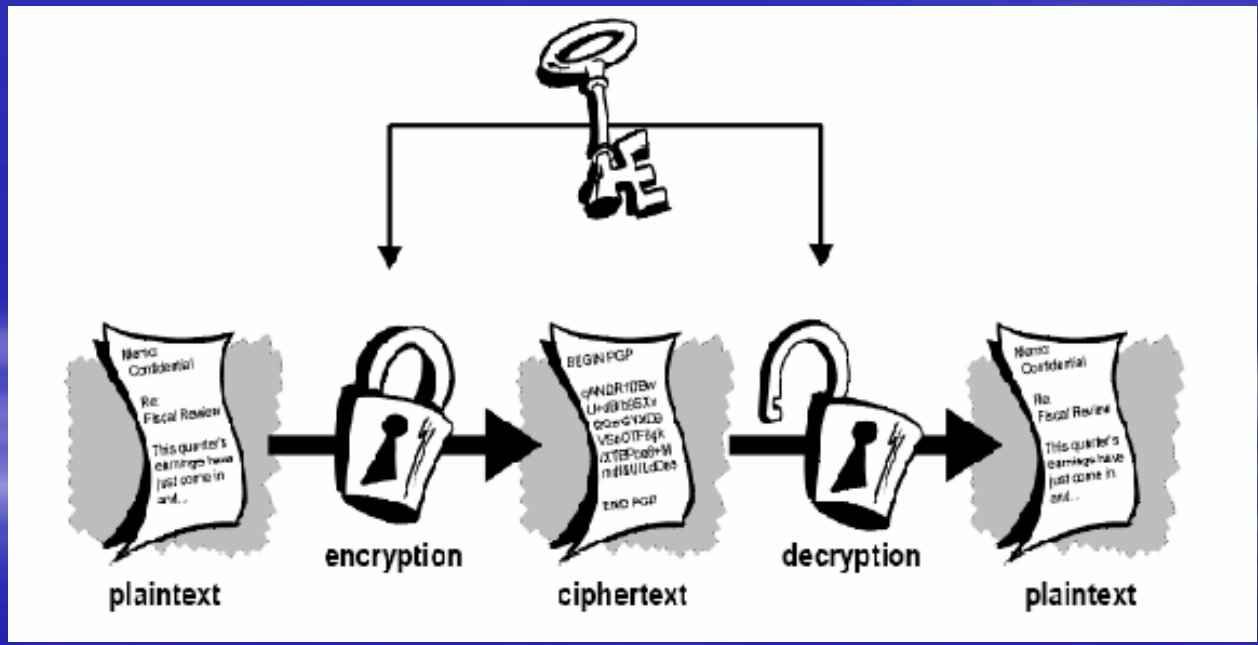
Encryption is Everywhere

Symmetric Encryption

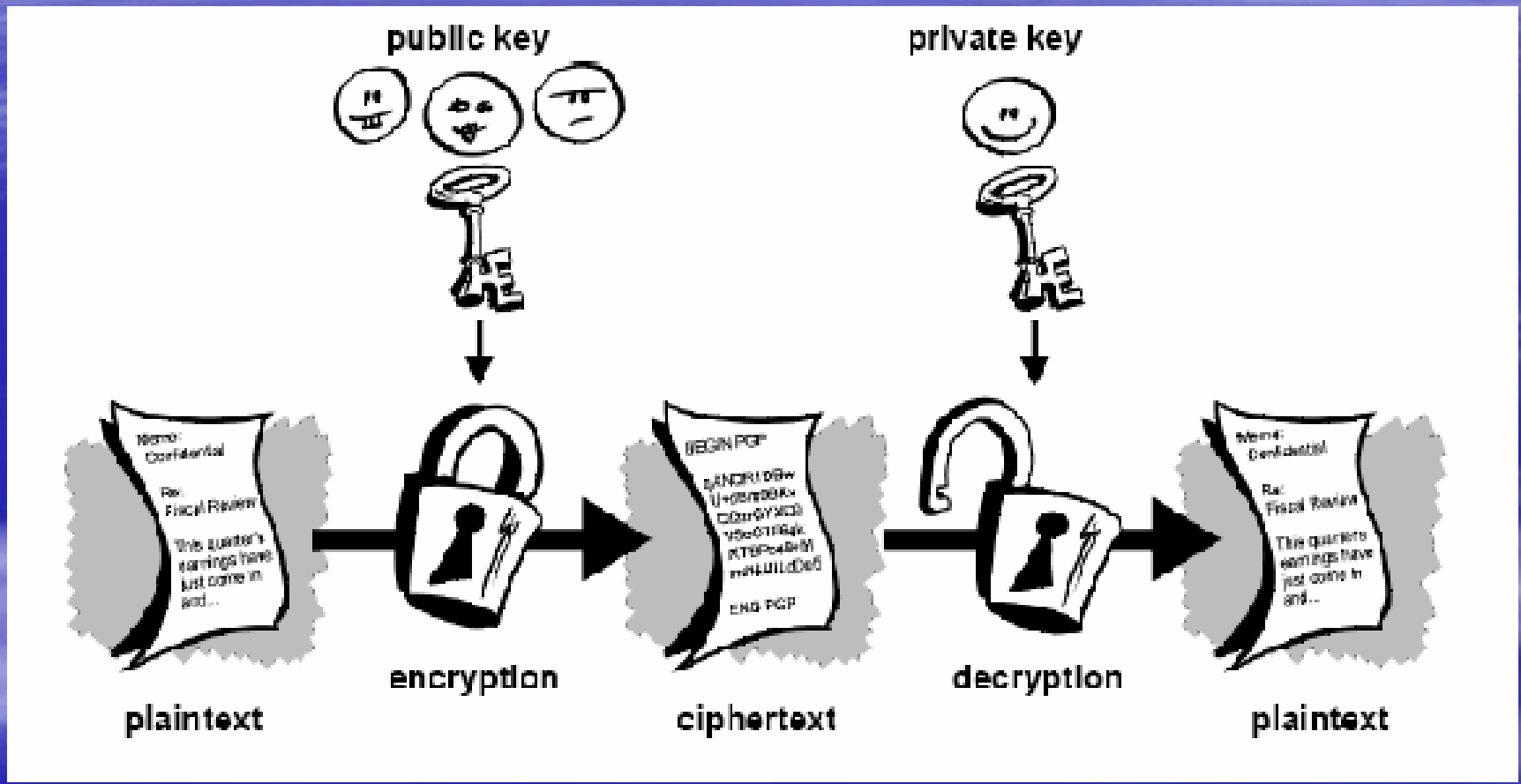


Symmetric Encryption

Fast encryption and decryption
but problematic key distribution

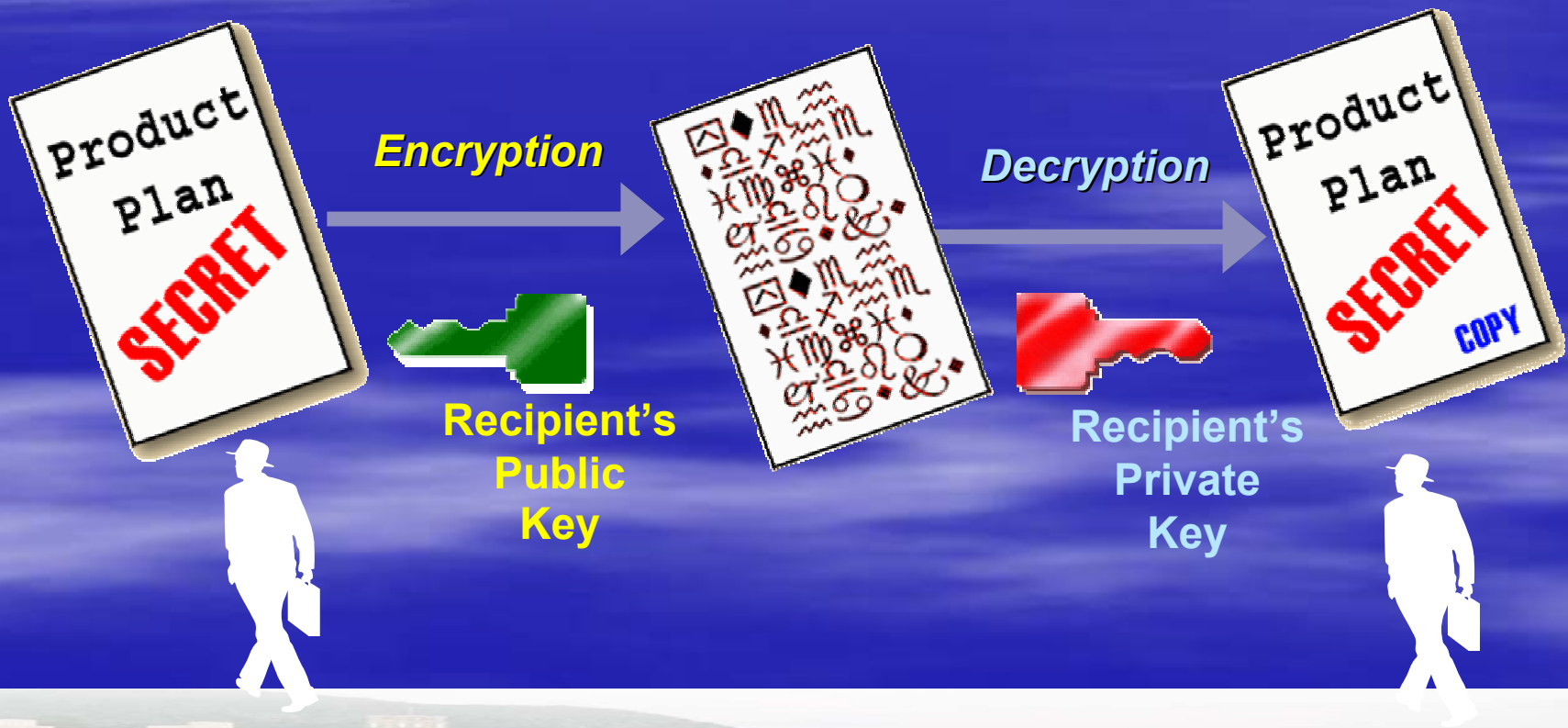


Asymmetric Encryption



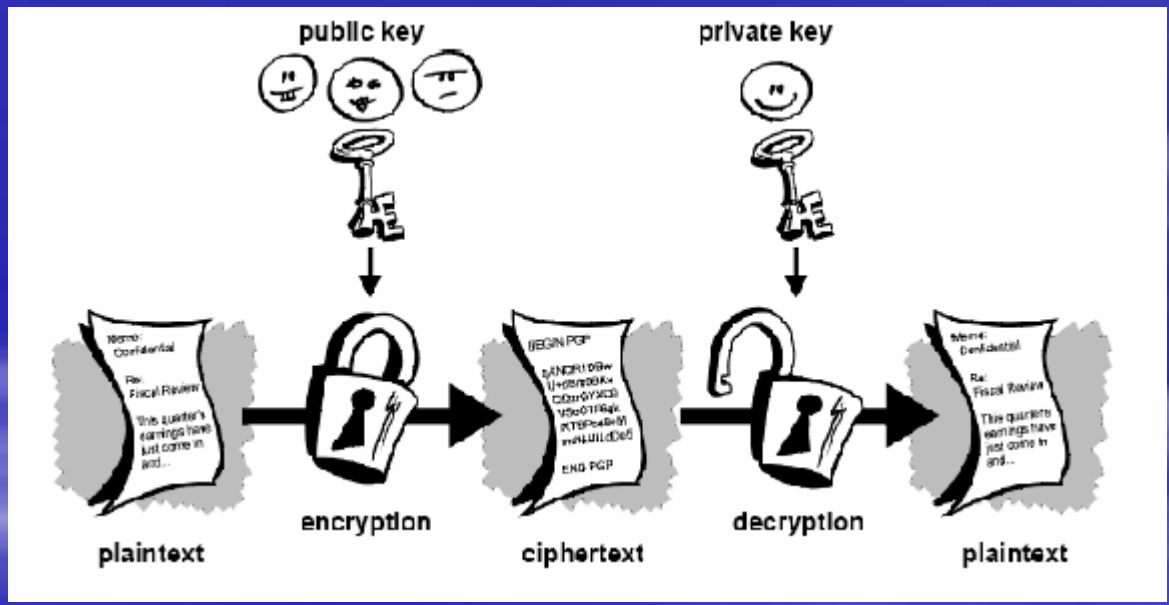
Public Key Cryptography is…

Certificates containing key pairs. One half of a key pair is used to *encrypt*, the other half is used to *decrypt*.



Asymmetric Encryption

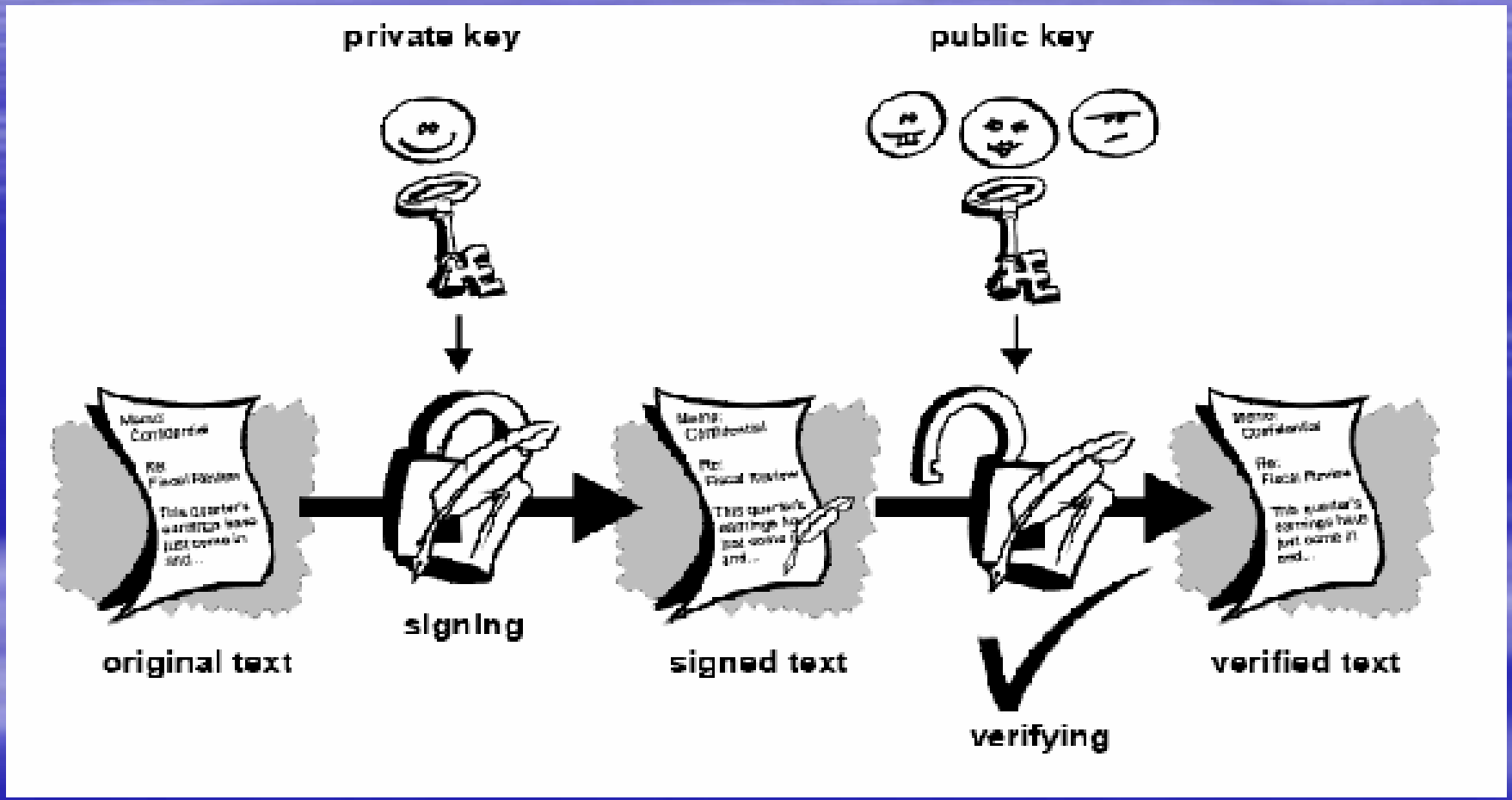
Slow performance (compared to symmetric encryption) but key distribution easier than symmetric



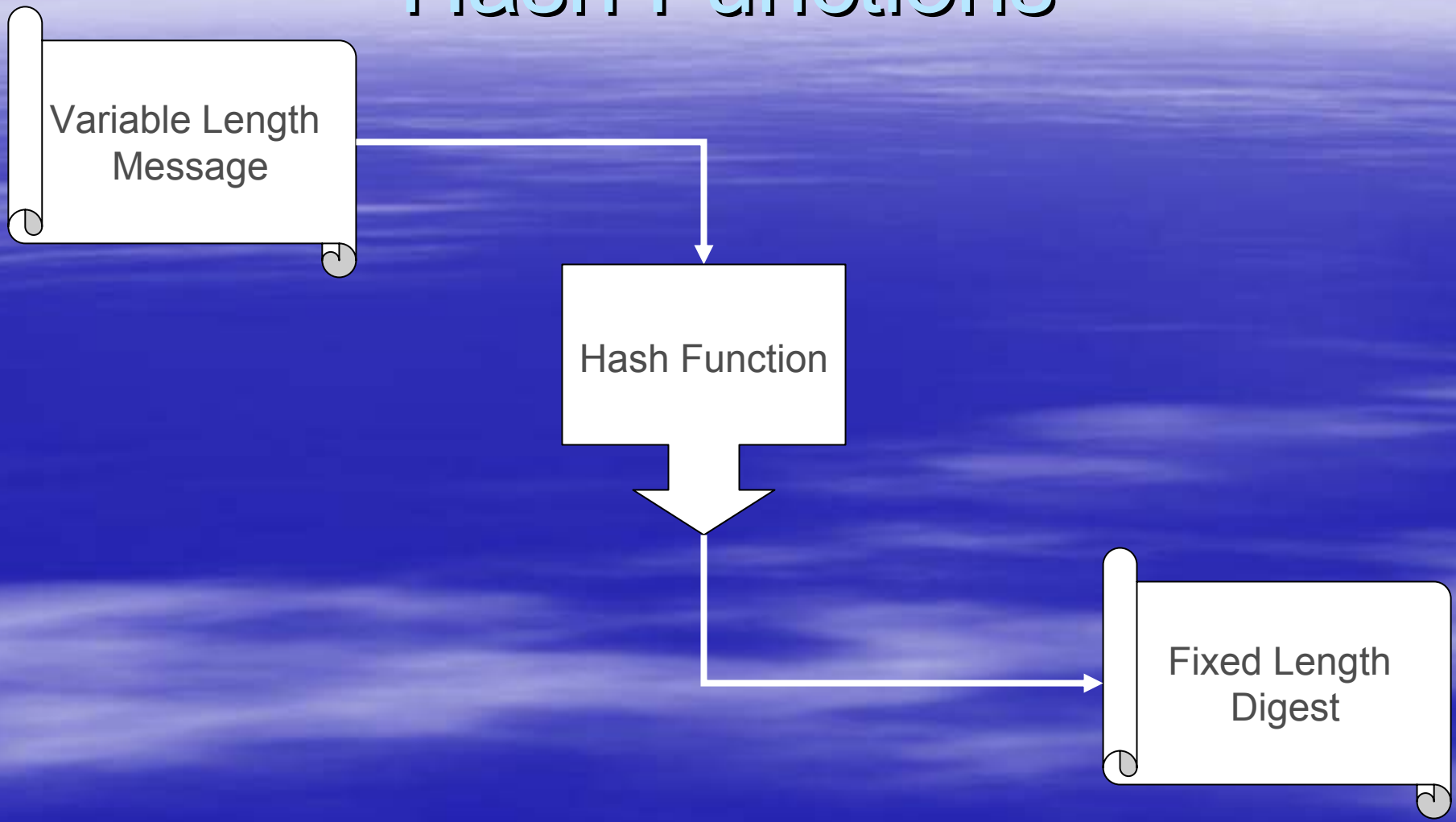
Digital Signatures

- Digital signatures not only prove who sent a message, they are attest that the message was not changed.
- However, they are slow and double the message size.

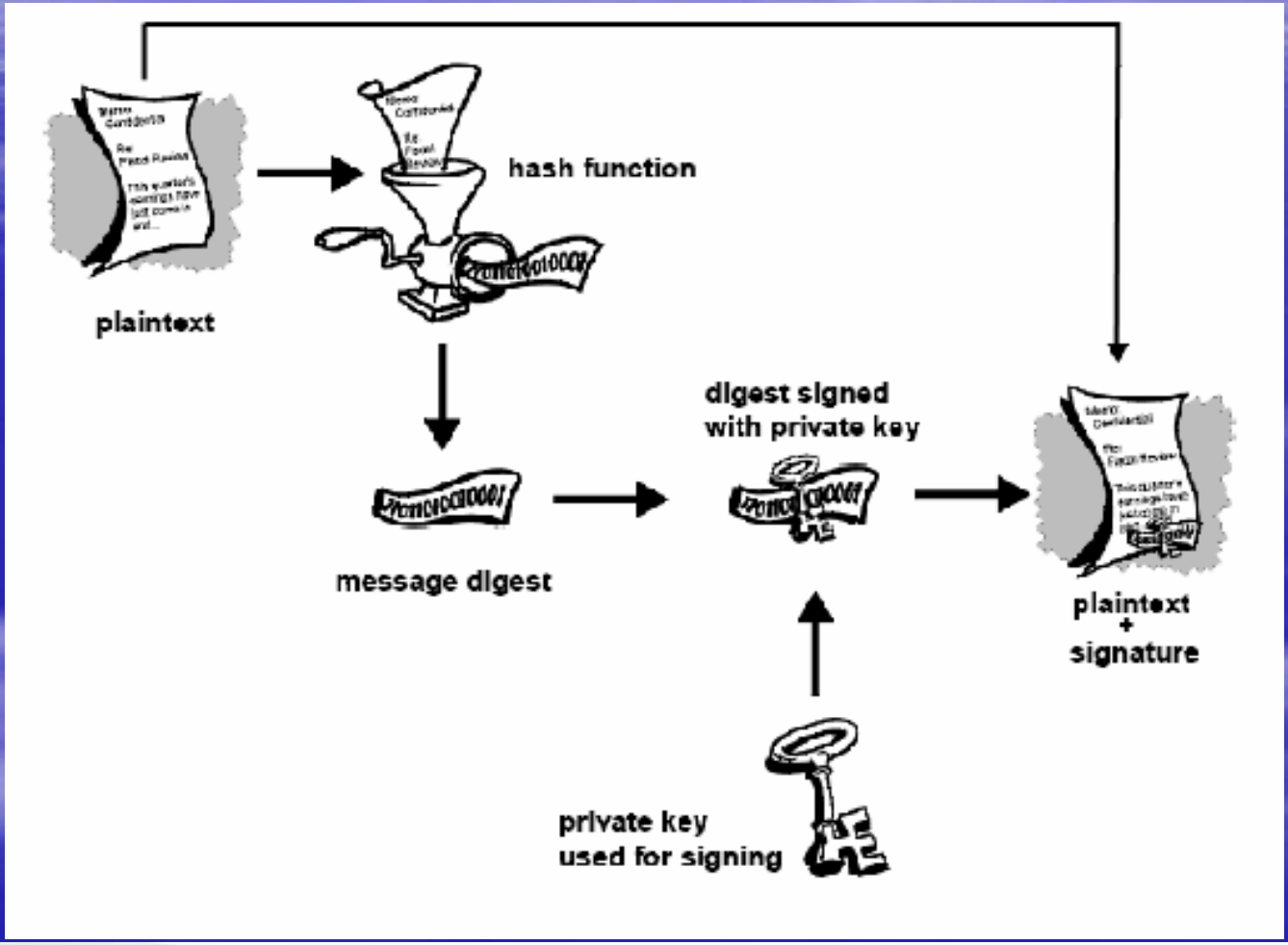
Digital Signatures



Hash Functions



Digital Signatures with Hashes



Digital Certificates

Is Alice's public key really Alice's public key or is it really evil Sarah pretending to be Alice (who is locked up in the closet)?

Digital Certificates have three components:

- A public key
- Certificate information
- One or more digital signatures

X.509 is a common format for digital certificates.

Public Key Infrastructure

- Used to manage digital certificates by issuing, trusting and revoking certificates.

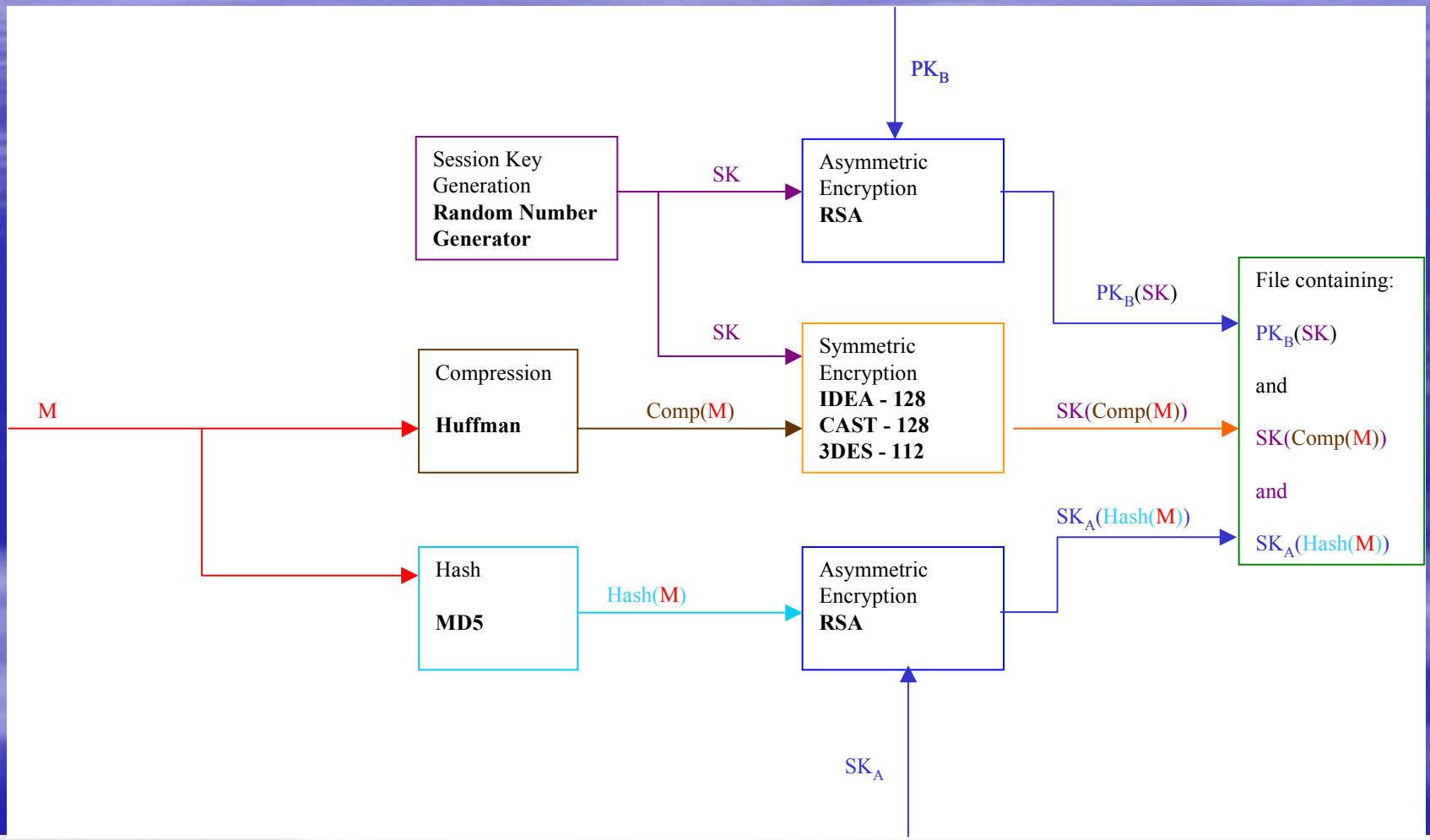
- Two components:
  - Certification Authority: creates certificates and signs them.
  - Registration Authority: the people, processes, and tools used to support registration of users.

Pretty Good Privacy (PGP)

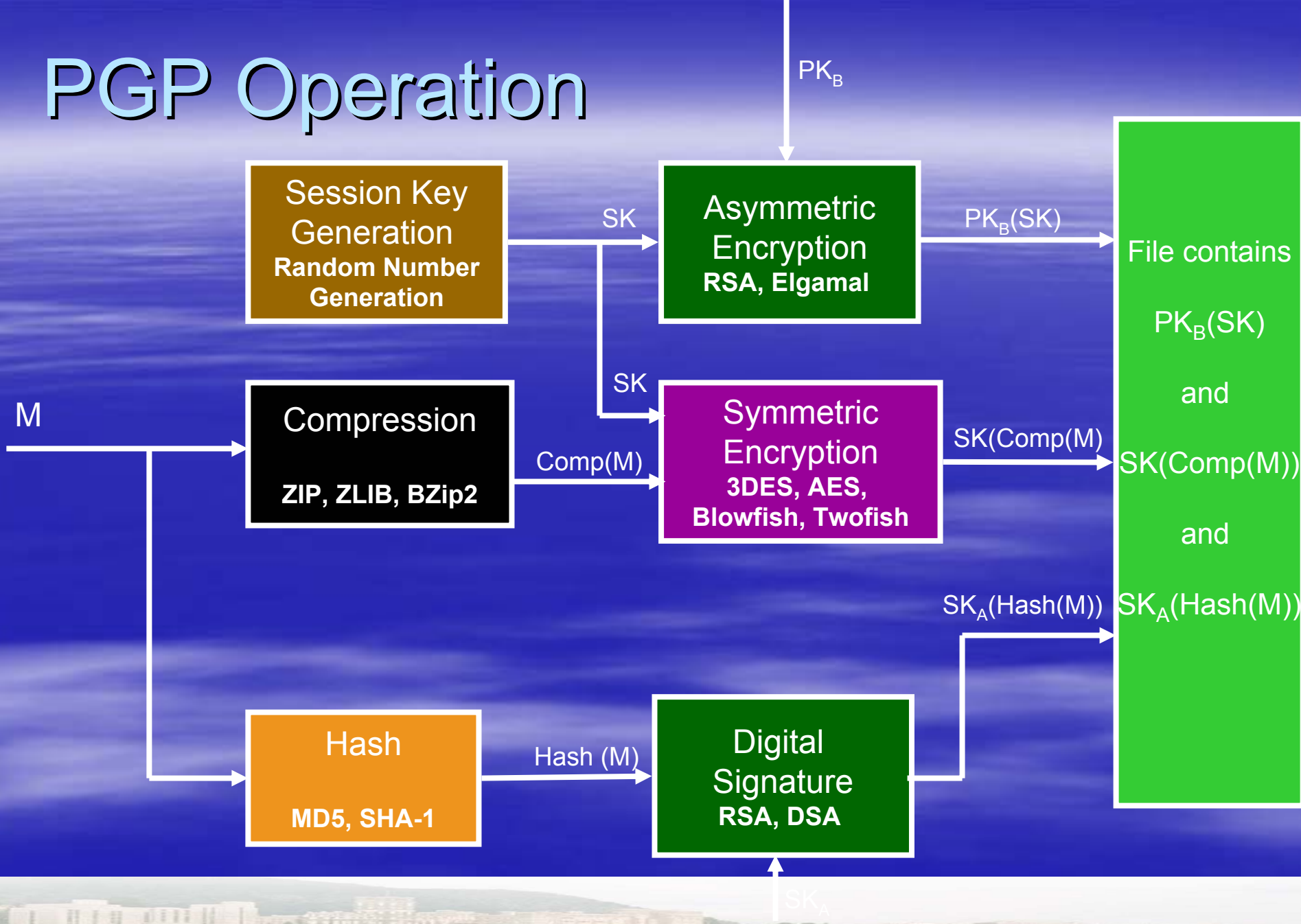
"It's personal. It's private. And it's no one's business but yours."

- Created by Phil Zimmermann in 1991.
- Freeware and commercial products.
- The focal point for a national debate on strong encryption export control during the 1990s.
- The debate ended in 1999 with privacy winning out.

PGP Operation



PGP Operation



How Good is PGP?

"If all the personal computers in the world - 260 million - were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message."

William Crowell,
Deputy Director, NSA,
March 20, 1997.

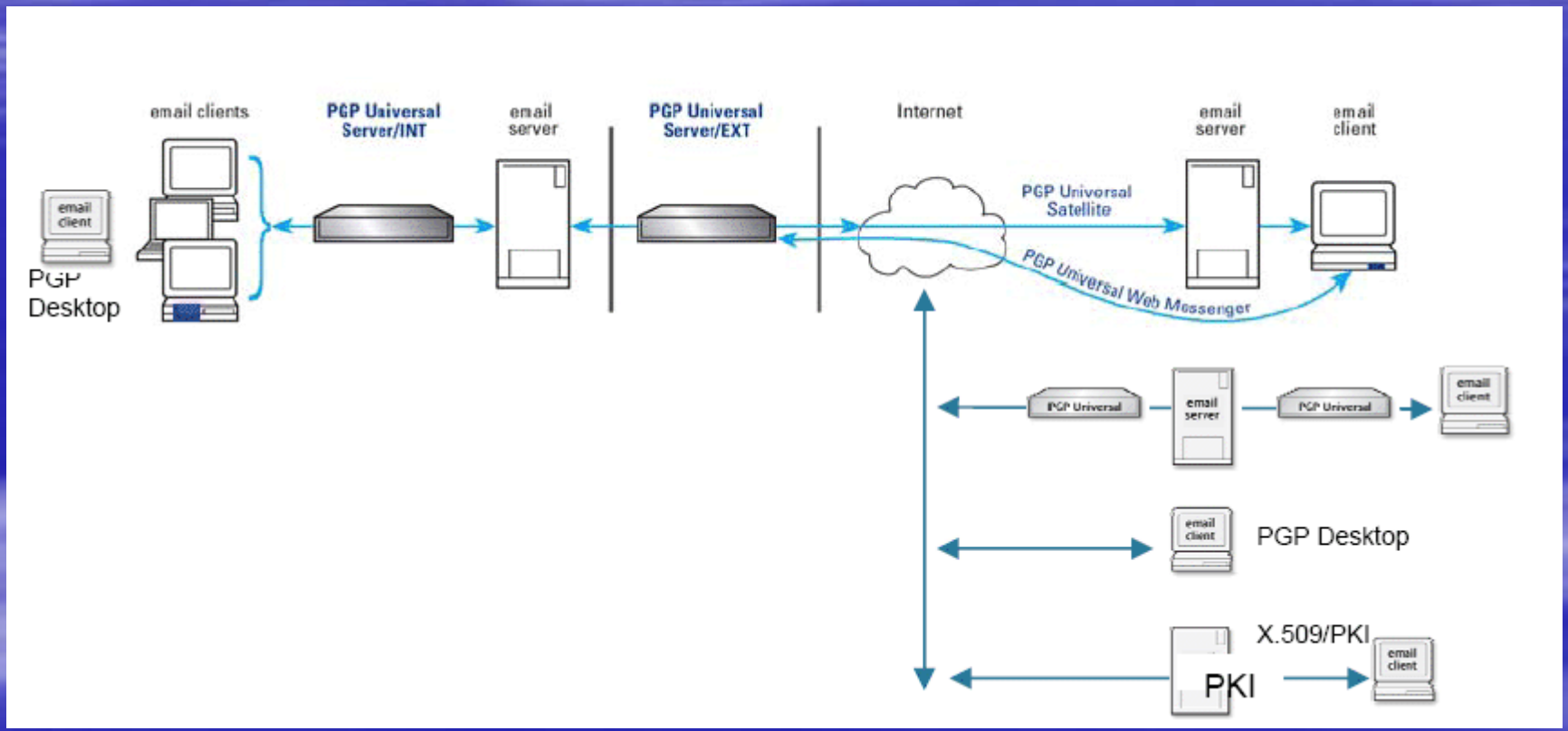
PGP Universal

- Released by PGP Corporation (www.pgp.com)
- Shifts email encryption from the desktop to the network so that it becomes a transparent service.
- Provides mechanisms to handle internal and external traffic as well as recipients without a email security solution.

PGP Universal

- No requirement for user to distribute public keys.
- No requirement for user to decide when to implement security policy.
- Ability to project security policy to secure electronic boundaries.

PGP Universal



Implications

Encryption is no longer too hard or too slow for routine operations.
It will spread everywhere.

Implications

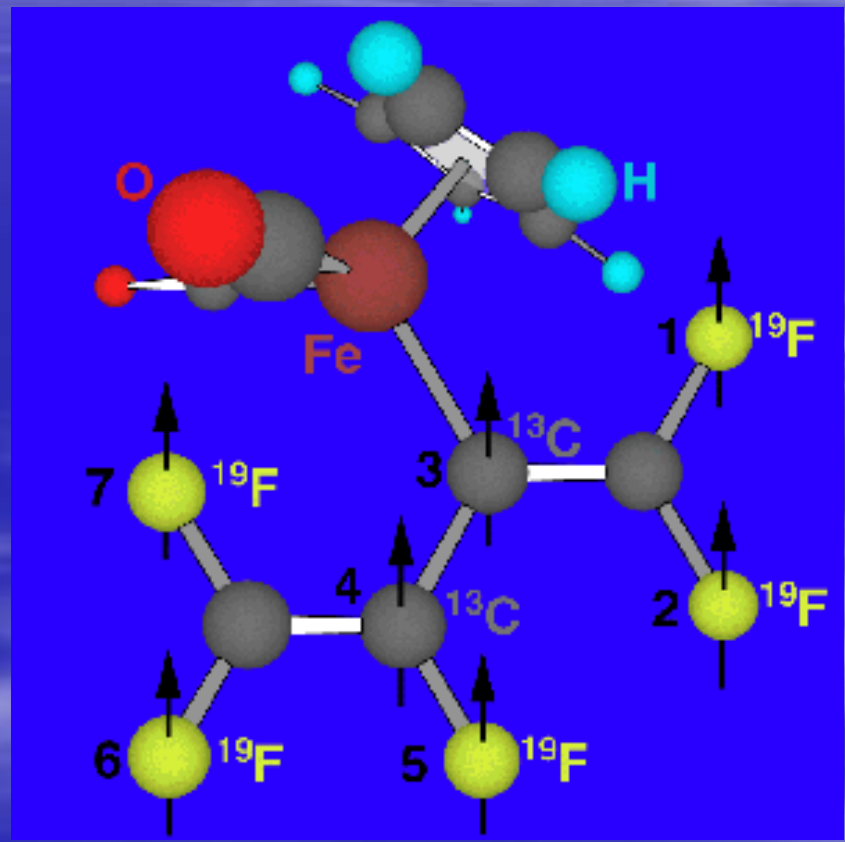
The plethora of computing devices and their interconnectivity pose new risks.

Implications

- Life gets more complicated while we figure how to live with ubiquitous encryption.
  - Bad and good folks get more privacy.
  - Bad and good folks get more authentication.
  - Authorization gets harder to check.
  - We continue to use a variety of techniques to keep bad guys on the run.

Implications
(Information Technology)

- Moore's law remains true but is not a factor.
- Quantum computing may change everything but it is unlikely. There are physical limits that smart folks like Einstein think we cannot surpass and some problems remain difficult to solve.



Implications

Growing social and legislative pressure to protect privacy of personally identifiable or company confidential information while it is in storage, being processed, or in transit.

Implications

- Privacy remains an issue not because everyone can read our mail, but because everyone can identify us.
- Will the demands for authentication (national ID card) destroy privacy, ensure safe computing, both, neither or none of the above?

The Implications of Encryption

Curtis A. Carver Jr. and John M.D. Hill
Department of Electrical Engineering and Computer Science
United States Military Academy