Acc 680 Research Seminar in Accounting (Electronic Commerce
Lecture Notes: Information Security Technologies I

Jagdish S. Gangolly

March 16, 1999

---

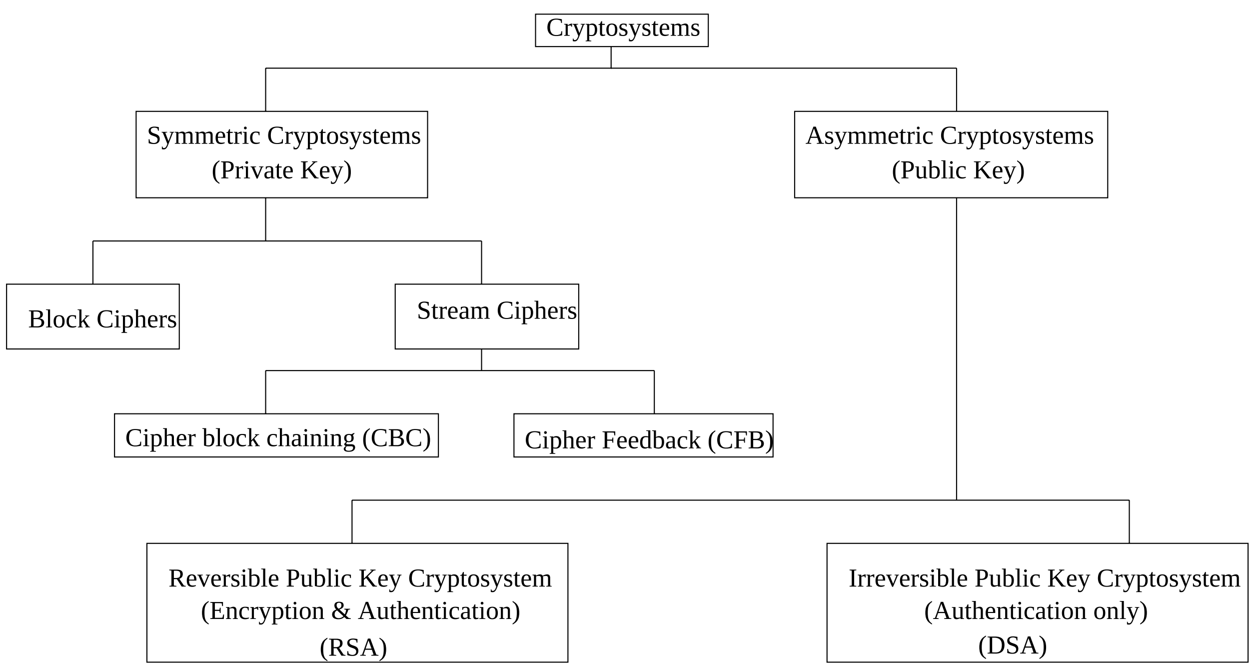
1 Basic Concepts:

- Security Authority
- Security Domain
- Security Policy
- Authorisation
- Accountabiltiy
- Safeguards / Vulnerabilities
- Risk
- Threat
- Attack
  - *Passive attack*
  - *Active attack*

2 Security Services

- Authentication
- Access Control
- Confidentiality
- Integrity
- Non-repudiation

3 Cryptosystems:



CRYPTOSYSTEMS

- **Data Encryption Standard (DES):** Operates on 64 bits of data using a 56-bit key. Exhaustive search to crack the key requires examining

$$2^{56} \simeq 7.10^{16}$$

possible values. Details of DES can be found at:

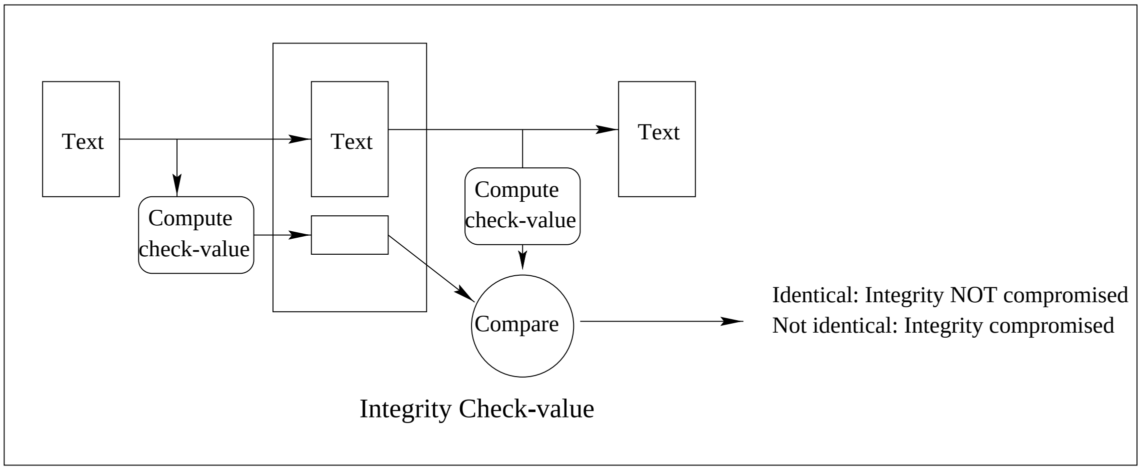
http://csrc.nist.gov/fips/dfips46-3.pdf

In the context of E-Commerce, some alternatives include

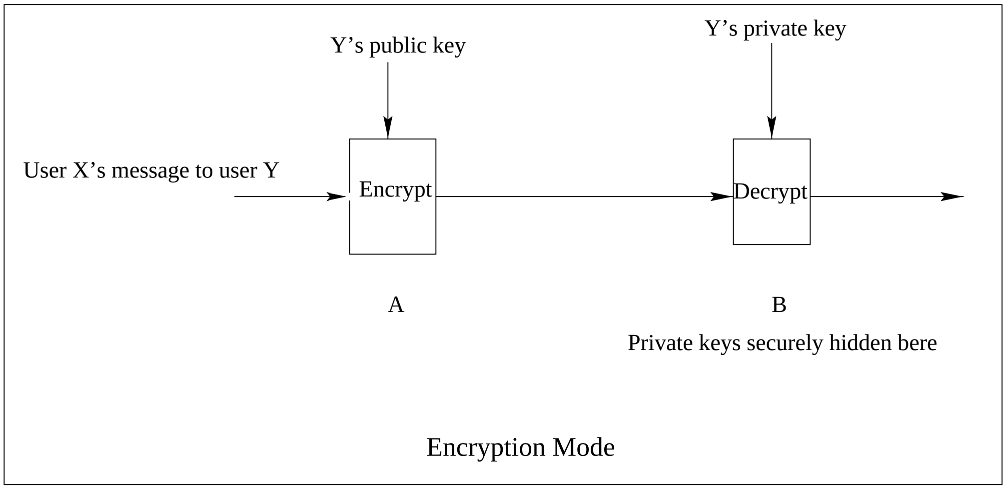
  - *Triple-DES*
  - *SKIPJACK*, a 64-bit block cipher ith 80-bit key.
  - Other proprietary algorithms such as *IDEA, RC2, RC4, RC5, and CAST*.

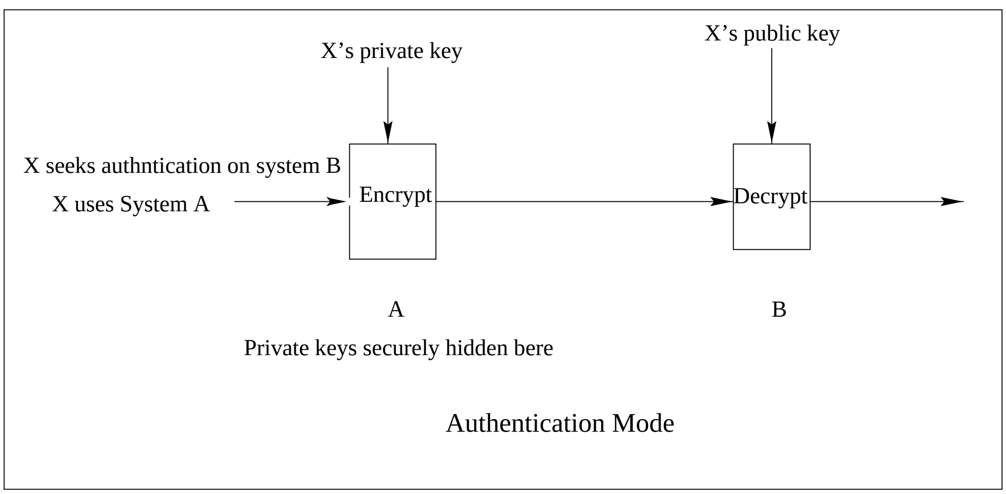
- **Integrity Check-values:** Useful hen confidentiality is not important, but integrity is very important.

  An example is the *Message Authentication Code (MAC)* used in the financial industry. It uses a symmetric block cipher such as DES as a building block.



- **Public-key Cryptosystems:** Uses a pair of related keys: public and private. They can be used for encryption as ell as for authentication.





4 Digital Signatures:

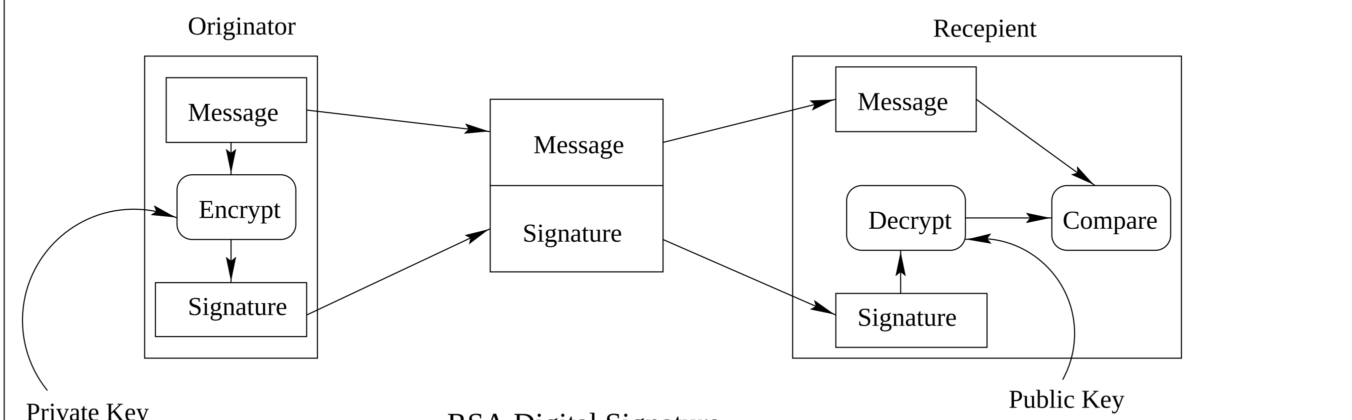
Reversible public-key cryptosystems can be used for encryption as ell as authentication, hereas irreversible public-key cryptosystems can be used for authentication only.

Integrity check-value resembles a digital signature. Ho ever, it can not serve as a digital signature, since it is important that the recepient NOT be able to reproduce the digital signature generated by the originator. Since the recepient kno s the key (key is shared in integrity check-value), this requirement of digital signatures is not met.

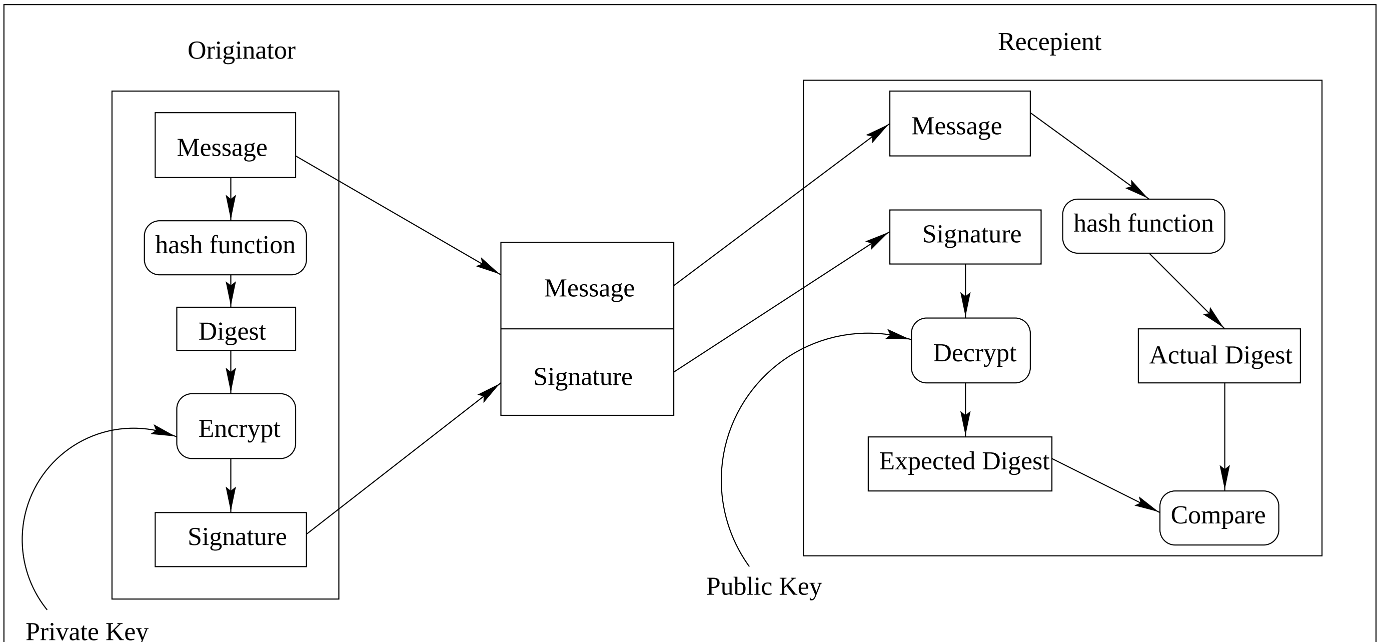
The choice bet een them depends on the relative importance of authentication, non-repudiation, and encryption/integrity services.

T o public-key cryptosystems used in the United States are,

– *Rivest-Shamir-Adelman* (RSA) hich uses the fact that factoring the products of large prime numbers is quite difficult. It is a reversible system, and so can be used for both encryption and authentication. In RSA DS, the digital signature is provided by the encryption of the document using the private key of the sender of the message. To reduce the overheads, a hash function is used in conjunction ith RSA. The hash function creates a *digest* of the message, hich is RSA-encrypted.



RSA Digital Signature



RSA Digital Signature Using Hash Function

– *Digital Signature Standard* (DSS) (hich is based on the difficulty of inverting a mathematical exponentiation operation). It is an irreversible system, and can be used for authentication only.

5 Key management:

- *Key Life cycle:*
  - Key generation/registration
  - Key distribution
  - Key backup/recovery/escro
  - Key replacement/update (*Re-keying*)
  - Key revocation
  - Key termination/destruction/archival.
- *Symmetric Key Distribution:*
  - *Using symmetric keys:*
    - *Types of Keys:*
      - Session or Primary Keys
      - Key-encryption Keys
      - Master Keys
    - *X.9.17 Configurations:*
      - Point-to-Point Configuration
      - Key center Configuration
  - *Using RSA:* Fig 4.9 (p.123)
  - *Diffie-Hellman Key Agreement:*
- *Public Key Distribution:* Certificates

- *Authentication*
  - Pass ords/PINs
  - Authentication Protocols
  - Kerberos (DES-based)/Pretty Good Privacy (PGP) (Public Key-based)
  - Adress-based Authentication
  - Personal Tokens
  - Biometrics

Some Useful Links:

RSA Standard:
http://www.alw.nih.gov/Security/FIRST/papers/crypto/pkcs/pkcs_1.ps

An Overview of the PKCS Standards
http://www.alw.nih.gov/Security/FIRST/papers/crypto/pkcs/overview.ps

Diffie-Hellman Key-Agreement Standard
http://www.alw.nih.gov/Security/FIRST/papers/crypto/pkcs/pkcs_3.ps

Network Security via Private-Key Certificates
http://www.alw.nih.gov/Security/FIRST/papers/crypto/privkey.ps

Answers to Frequently Asked Questions About Today's Cryptography
http://www.alw.nih.gov/Security/FIRST/papers/crypto/rsafaq.ps

Cryptography FAQ
http://www.alw.nih.gov/Security/FIRST/papers/crypto/scfaq.txt

The Architecture and Implementation of Network Layer Security Under Unix
http://www.alw.nih.gov/Security/FIRST/papers/crypto/swipe.ps

Department of Defense Password Management Guideline
http://www.alw.nih.gov/Security/FIRST/papers/password/dodpwman.txt

Foiling the Cracker: A Survey of, and Improvements to, Password Security
http://www.alw.nih.gov/Security/FIRST/papers/password/klein.ps

OPUS: Preventing Weak Password Choices
http://www.alw.nih.gov/Security/FIRST/papers/password/opus.ps

Password Security: A Case History
http://www.alw.nih.gov/Security/FIRST/papers/password/pwstudy.ps

Security Problems in the TCP/IP Protocol Suite
http://www.alw.nih.gov/Security/FIRST/papers/protocol/ipext.ps

A Tour of the Worm
http://www.alw.nih.gov/Security/FIRST/papers/virus/tour.ps

An Introduction to Computer Security: The NIST Handbook
http://csrc.ncsl.nist.gov/nistpubs/800-12/