Public Key Cryptography

Introduction to Computer Security

Naercio Magaia and Imran Khan

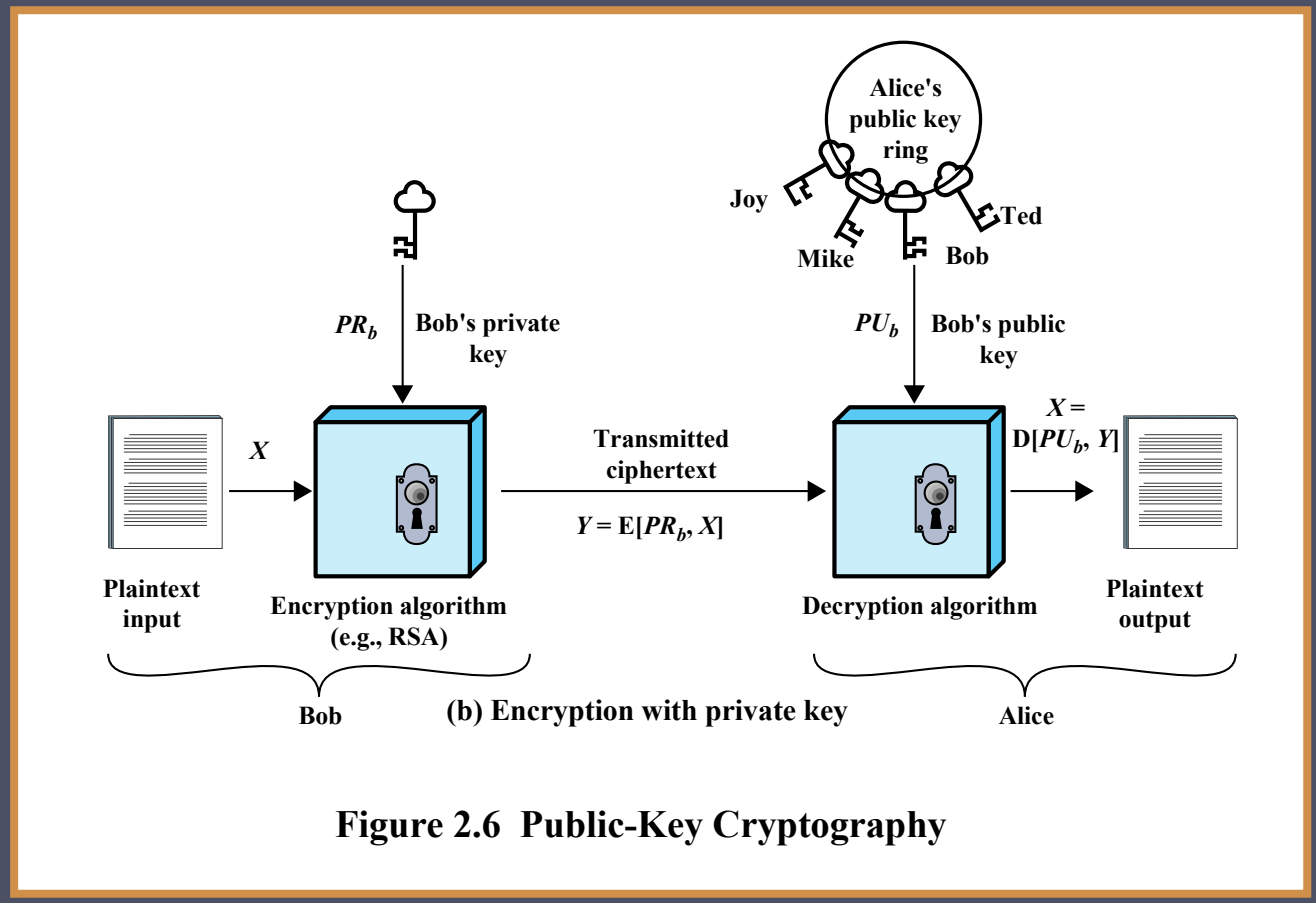


Figure 2.6 Public-Key Cryptography

Provides Authentication & Data Integrity

Why?

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

Requirements for Public-Key Cryptosystems

Computationally easy to create key pairs

Computationally easy for sender knowing public key to encrypt messages

Computationally easy for receiver knowing private key to decrypt ciphertext

Computationally infeasible for opponent to determine private key from public key

Computationally infeasible for opponent to otherwise recover original message

Useful if either key can be used for each role

Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977	Most widely accepted and implemented approach to public-key encryption	Block cipher in which the plaintext and ciphertext are integers between 0 and *n*-1 for some *n*.
Diffie-Hellman key exchange algorithm	Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages	Limited to the exchange of the keys	
Digital Signature Standard (DSS)	Provides only a digital signature function with SHA-1	Cannot be used for encryption or key exchange	
Elliptic curve cryptography (ECC)	Security like RSA, but with much smaller keys		

Digital Signatures

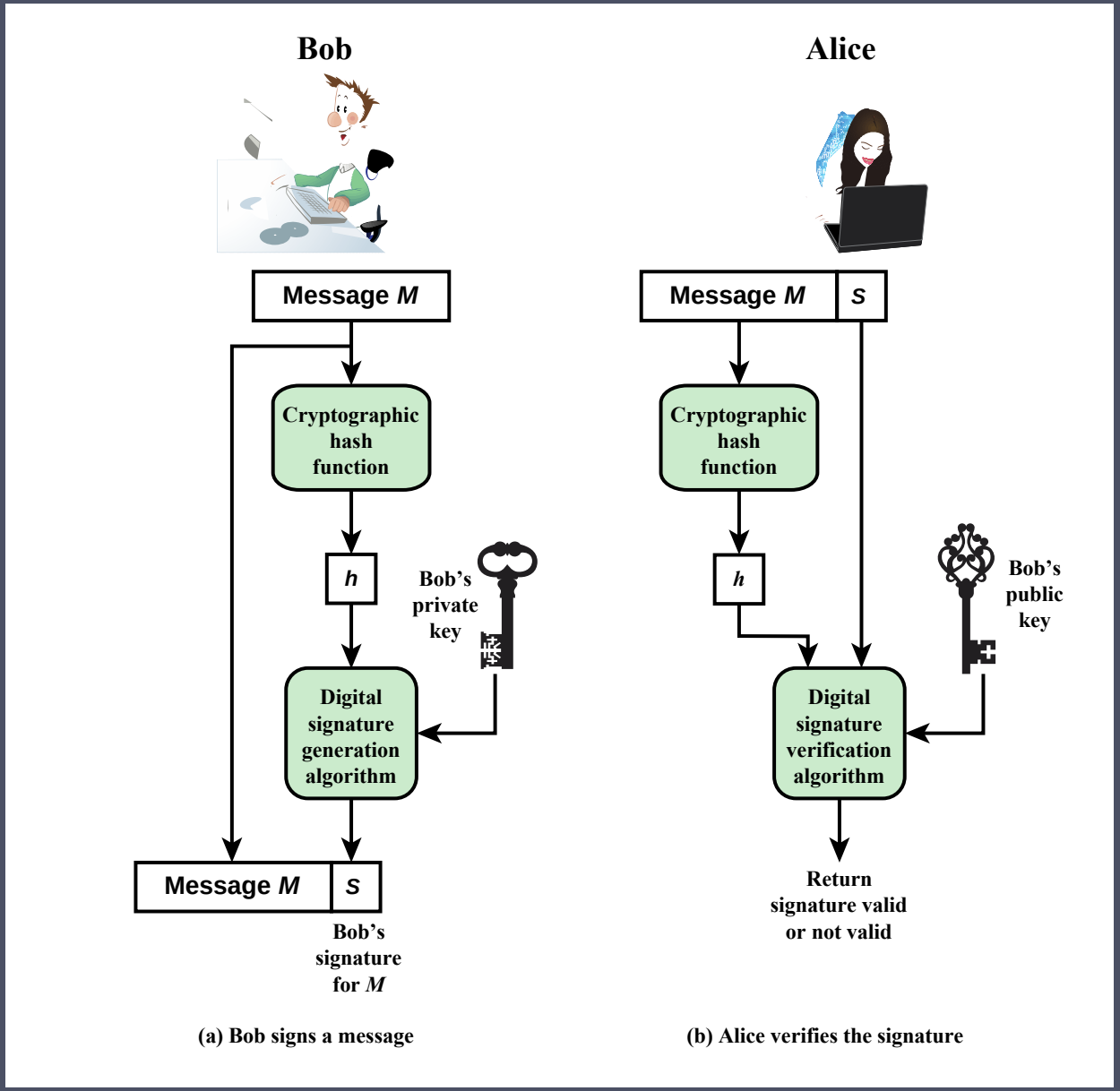
- NIST FIPS PUB 186-4 defines a digital signature as:

  "The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."

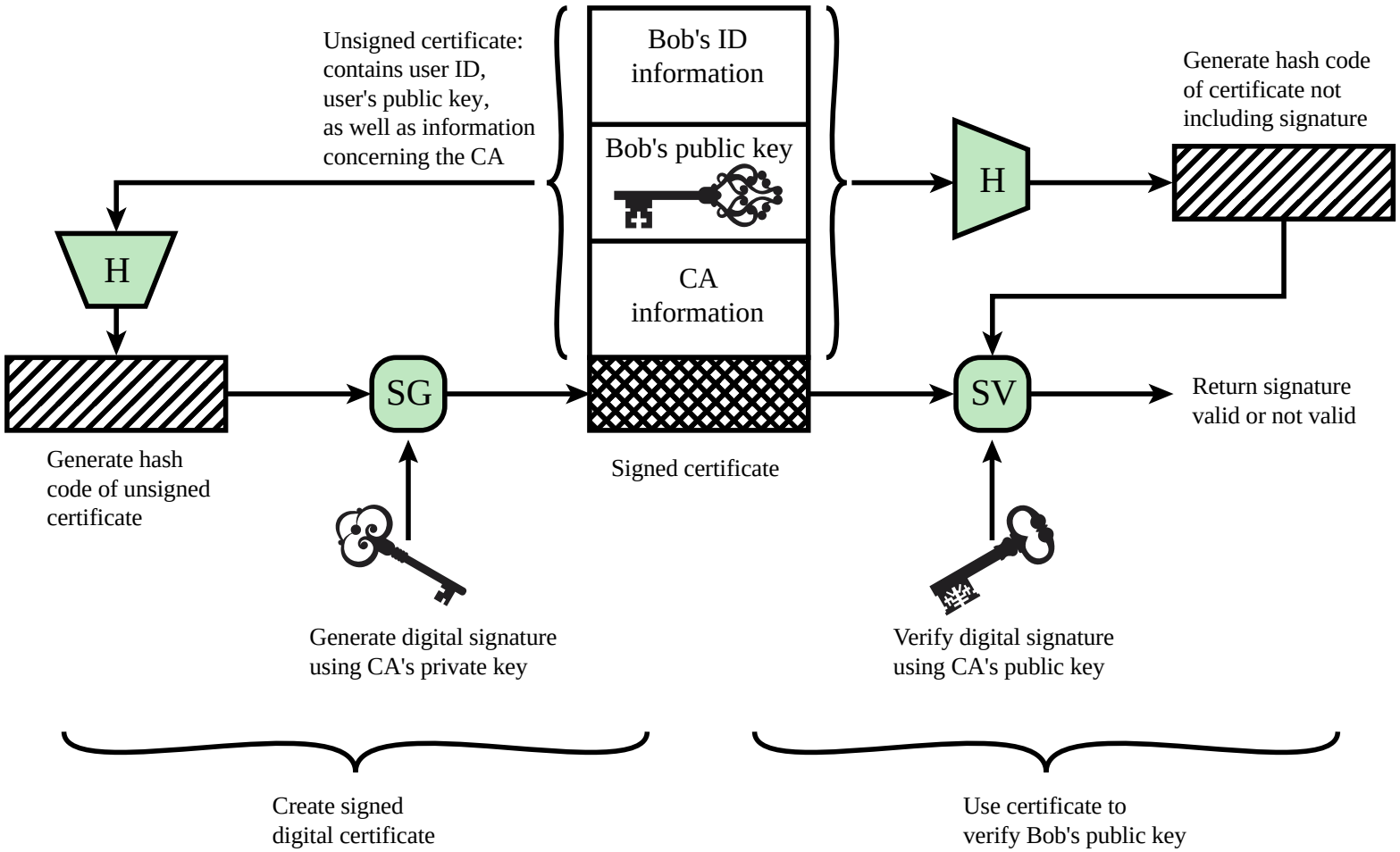
- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block

- FIPS 186-4 specifies the use of one of three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

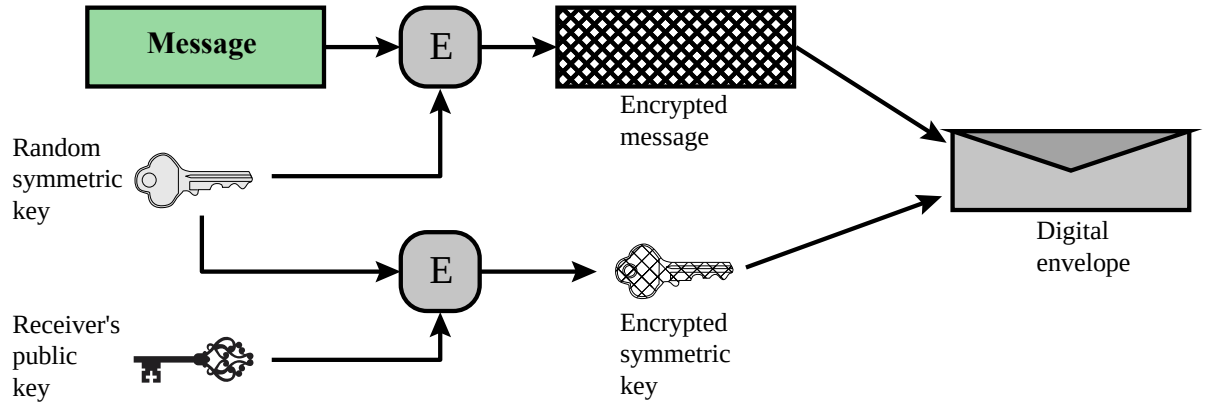
Digital Signatures Process



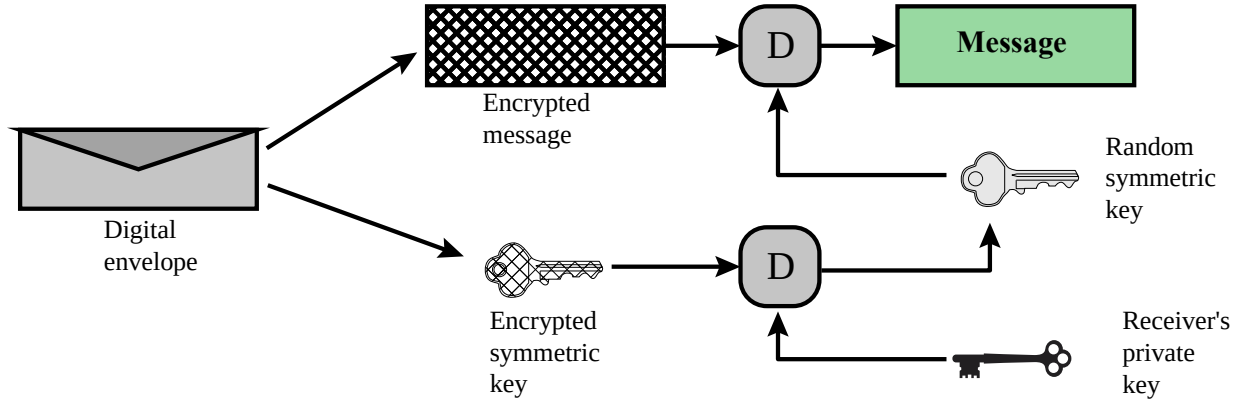
Public-Key Certificate



Digital Envelopes



(a) Creation of a digital envelope



(b) Opening a digital envelope

Applications for Public-Key Cryptosystems

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Random Numbers

- **Uses include generation of:**
  - Keys for public-key algorithms
  - Stream key for symmetric stream cipher
  - Symmetric key for use as a temporary session key or in creating a digital envelope
  - Handshaking to prevent replay attacks (e.g., Kerberos)
  - Session key

Random Number Requirements

Randomness

- Criteria:
  - Uniform distribution
    - Frequency of occurrence of each of the numbers **should be approximately the same**
  - Independence
    - No one value in the sequence **can be inferred** from the others

Unpredictability

- Each number **is statistically independent** of other numbers in the sequence
- Opponent **should not be able to predict** future elements of the sequence on the basis of earlier elements

Random versus Pseudorandom

Cryptographic applications typically make use of algorithmic techniques for random number generation

- Algorithms are deterministic and therefore produce sequences of numbers that are not statistically random

Pseudorandom numbers are:

- Sequences produced that satisfy statistical randomness tests
- Likely to be predictable

True random number generator (TRNG):

- Uses a nondeterministic source to produce randomness
- Most operate by measuring unpredictable natural processes
  - e.g., radiation, gas discharge, leaky capacitors
- Increasingly provided on modern processors

Practical Application: Encryption of Stored Data

Common to encrypt transmitted data

Increasingly common for stored data (*data at rest*)

- There is often little protection beyond domain authentication and operating system access controls
- Data are archived for indefinite periods
- Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt stored data:

- Use a commercially available encryption package (e.g., PGP)
- Back-end appliance
- Library-based tape encryption
- Background laptop/PC data encryption

Summary

- Public-key encryption
  - Structure
  - Requirements for public-key cryptography
  - Asymmetric encryption algorithms
  - Applications for public-key cryptosystems
- Digital signatures and key management
  - Digital signature
  - Public-key certificates
  - Symmetric key exchange using public-key encryption
  - Digital envelopes
- Random and pseudorandom numbers
  - The use of random numbers
  - Random versus pseudorandom
- Practical Application: Encryption of Stored Data