CyberSecurity: Principle and Practice

BSc Degree in Computer Science
2023-2024

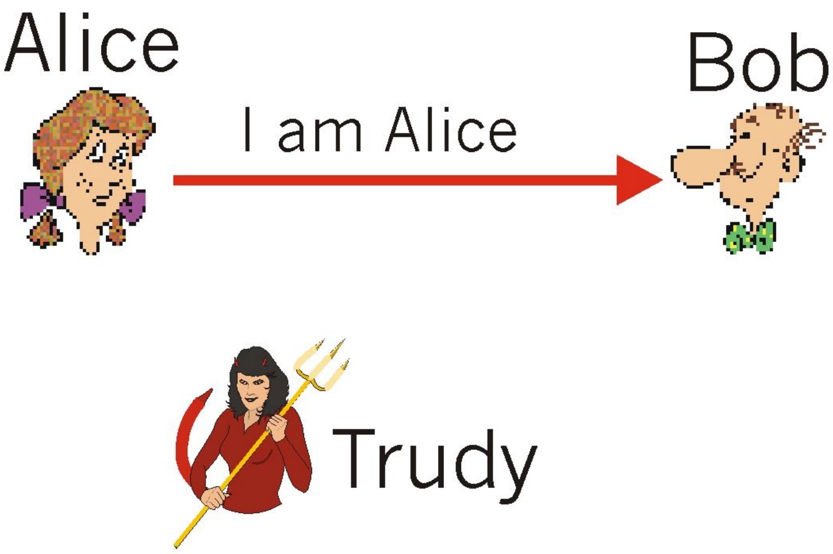
Lesson 5: Cryptographic Tools pt.2

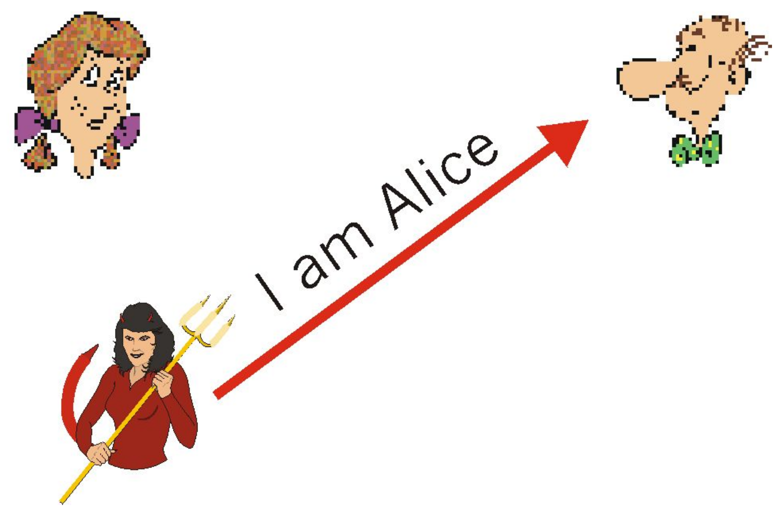
Prof. Mauro Conti
Department of Mathematics
University of Padua
conti@math.unipd.it
http://www.math.unipd.it/~conti/

Teaching Assistants
Tommaso Bianchi
tommaso.bianchi@phd.unipd.it
Riccardo Preatoni
riccardo.preatoni@studenti.unipd.it

Università degli Studi di Padova
SPRITZ Security & Privacy Research Group
Dipartimento Matematica

Message Authentication

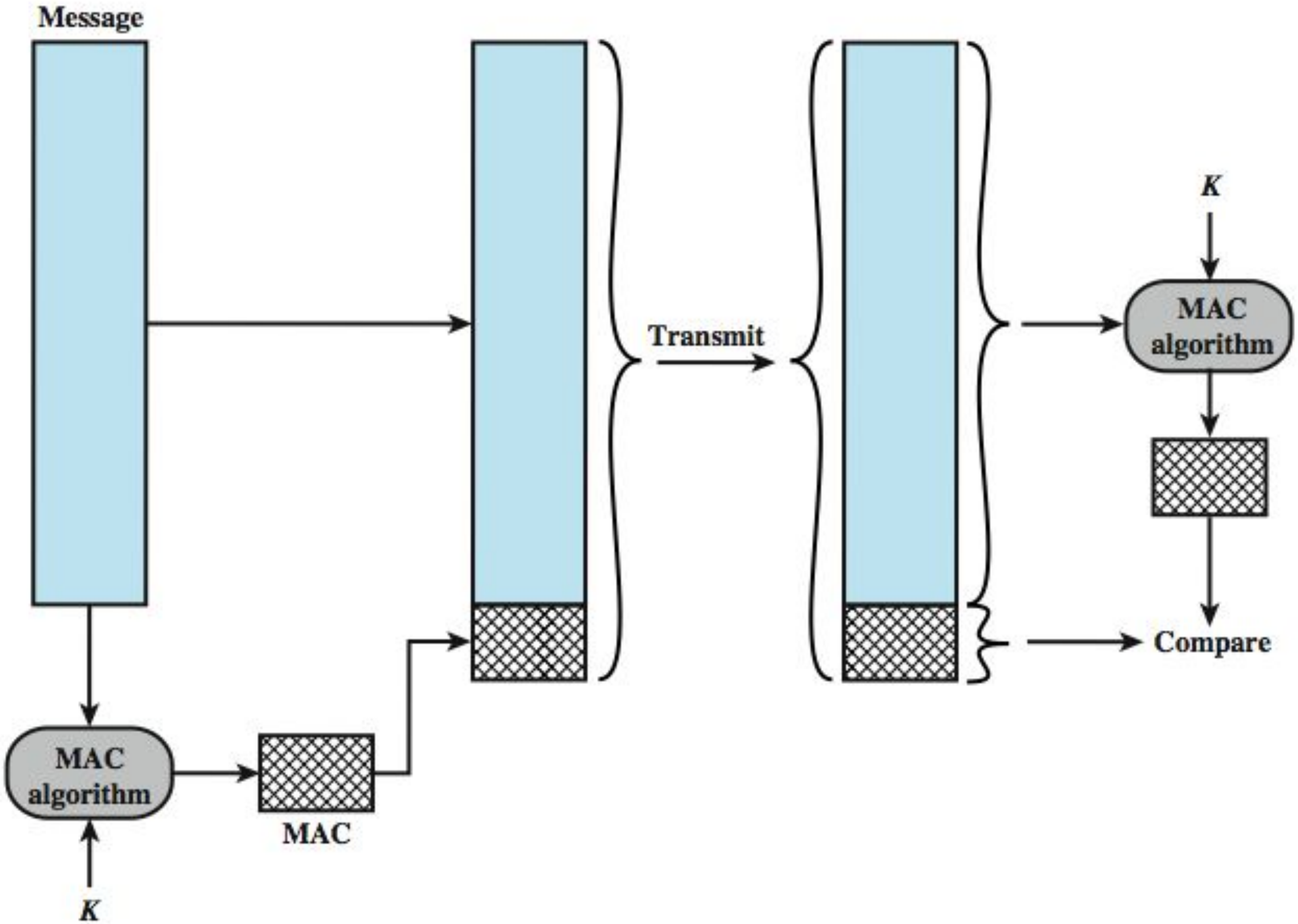




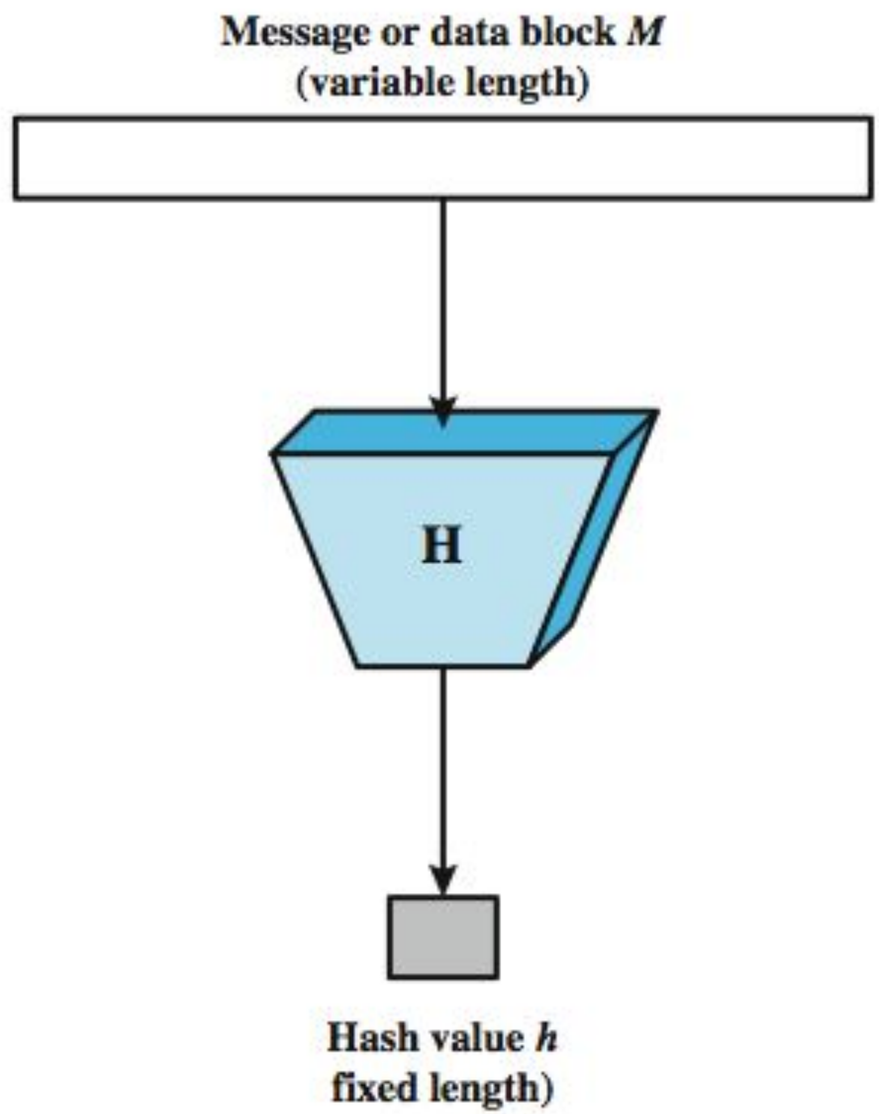
Message Authentication

- Protects against active attacks
- Verifies received message is authentic
    - Contents unaltered
    - From authentic source
    - Timely and in correct sequence
- Can use conventional encryption
    - Only sender & receiver have key needed
- Or a separate authentication mechanisms
    - Append authentication tag to clear text message

Message Authentication Code



Secure Hash Function



Hash Function Properties

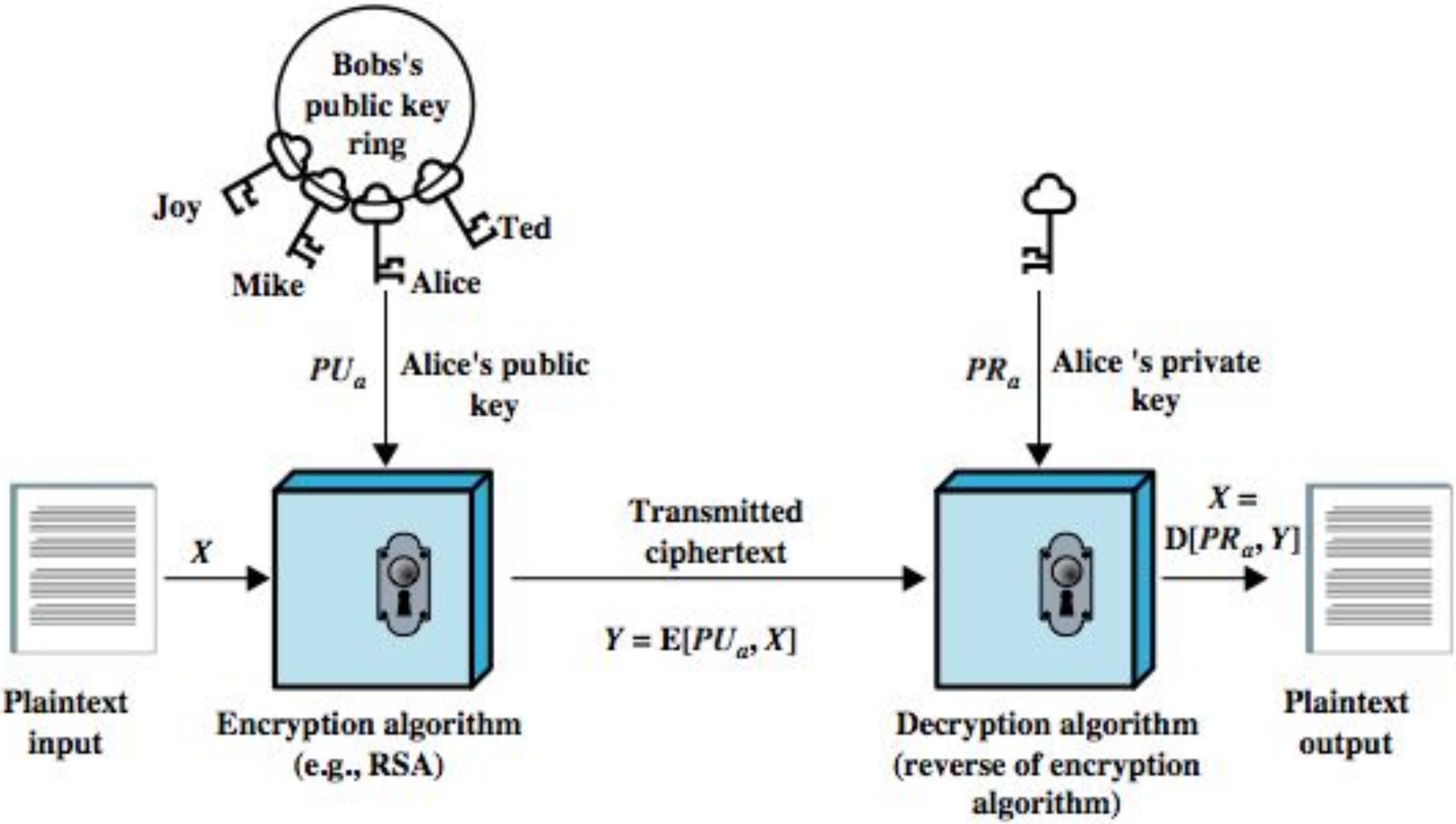
- Applied to any size data
- H produces a fixed-length output.
- $H(x)$ is relatively easy to compute for any given x
- One-way property
  - Computationally infeasible to find x such that $H(x) = h$
- Weak collision resistance
  - (given x) computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- Strong collision resistance
  - Computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$

Hash under attack

UNIVERSITÀ DEGLI STUDI DI PADOVA

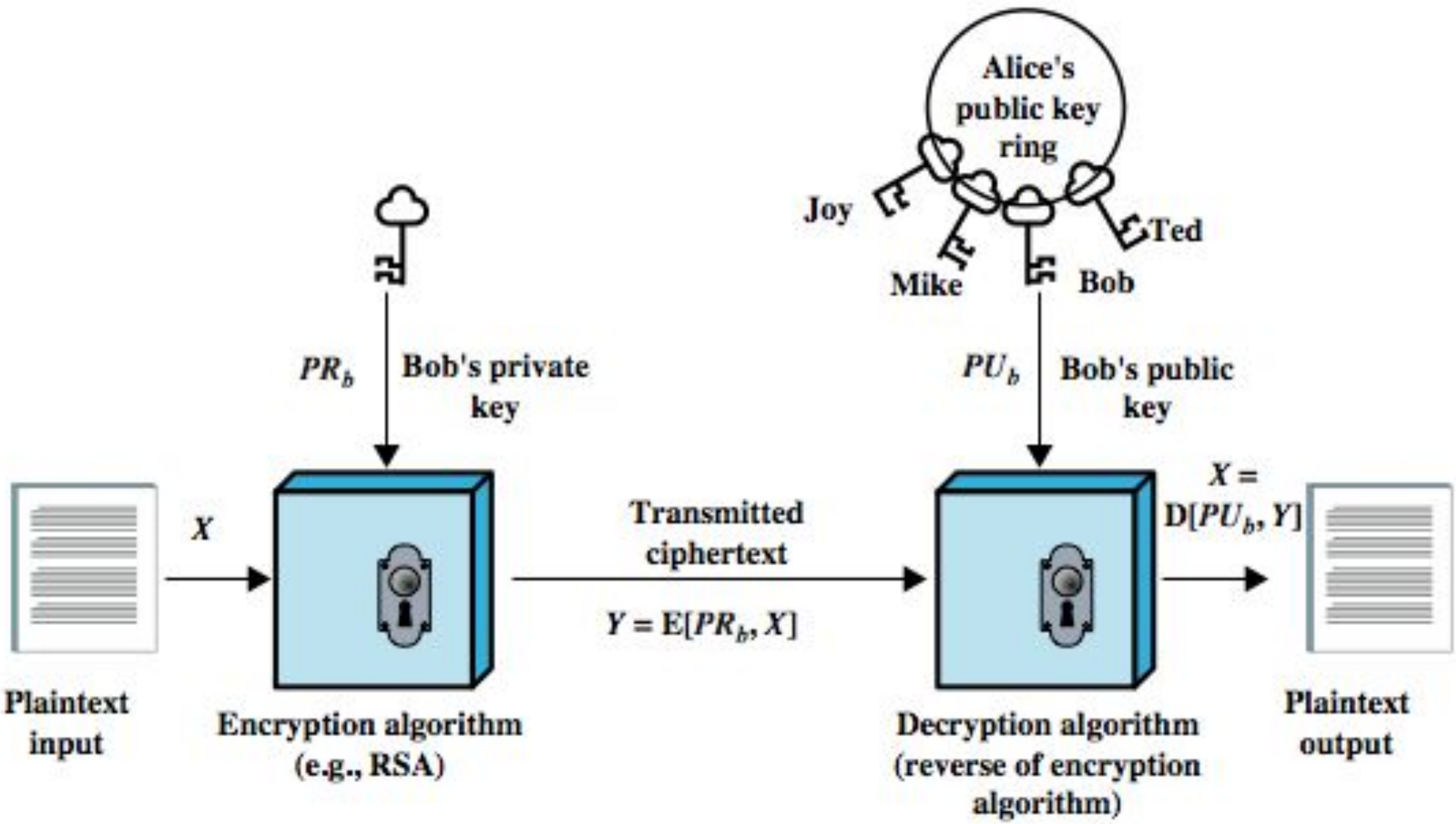
- Two attack approaches
  - Cryptanalysis
    - Exploit logical weakness in algorithms
  - Brute-force attack
    - Trial many inputs
    - Strength proportional to size of hash code
- SHA most widely used hash algorithm
  - SHA-1 gives 160-bit hash
  - More recent SHA-256, SHA-384, SHA-512 provide improved size and security

Public-Key Encryption



(a) Confidentiality

Public-Key Authentication

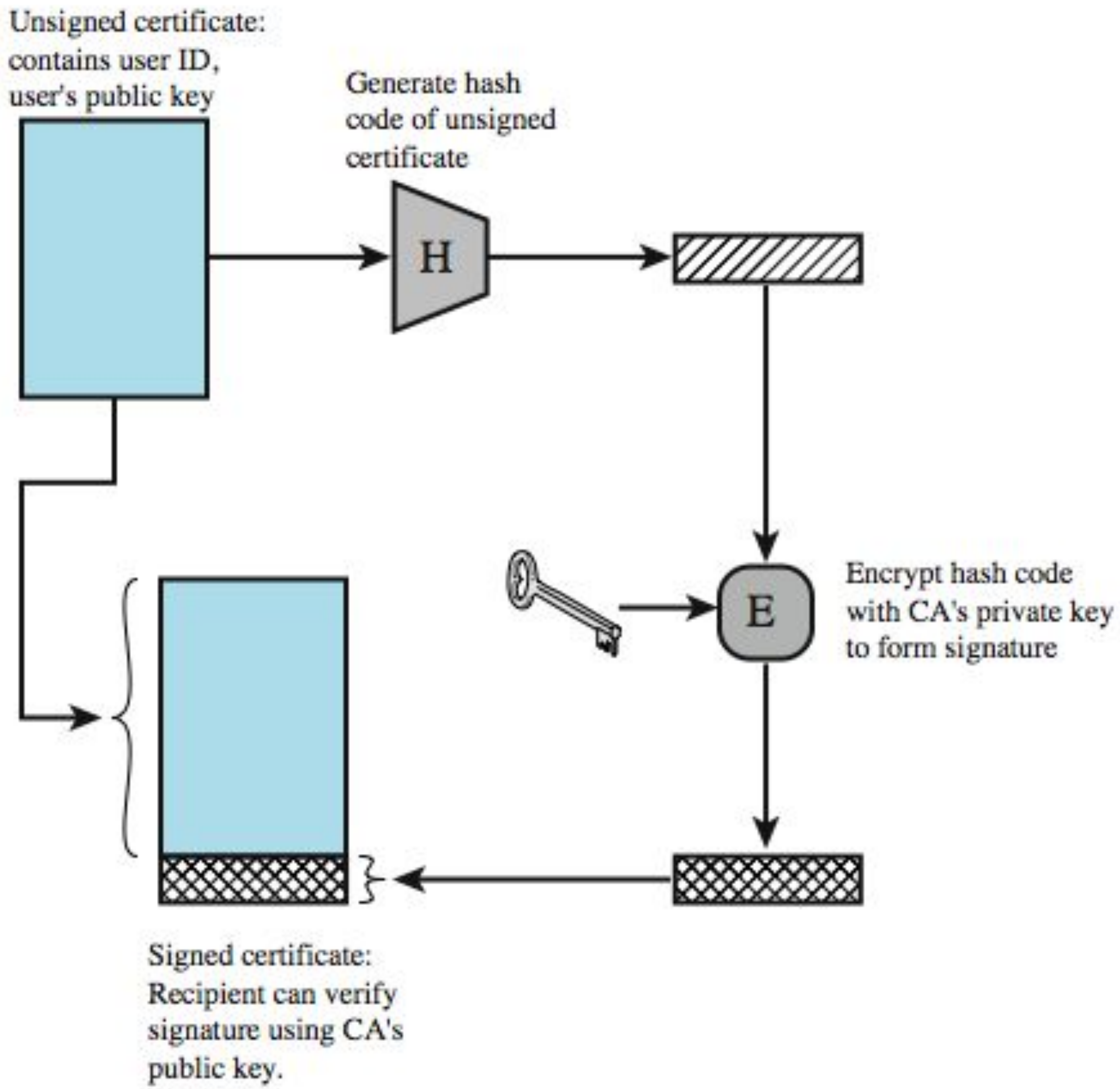


(b) Authentication

Public-Key Requirements

1. Computationally easy to create key pairs
2. Computationally easy for sender knowing public key to encrypt messages
3. Computationally easy for receiver knowing private key to decrypt ciphertext
4. Computationally infeasible for opponent to determine private key from public key
5. Computationally infeasible for opponent to otherwise recover original message
6. Useful if either key can be used for each role

Public-Key Certificates



Random Numbers

- Random numbers have a range of uses
- Requirements:
  - Randomness
    - Based on statistical tests for uniform distribution and independence
  - Unpredictability
    - Successive values not related to previous
    - Clearly true for truly random numbers
    - But more commonly use generator

Random Numbers

- Often use algorithmic technique to create pseudorandom numbers
  - which satisfy statistical randomness tests
  - but likely to be predictable
- True random number generators use a nondeterministic source
  - e.g. radiation, gas discharge, leaky capacitors
  - increasingly provided on modern processors

Questions? Feedback? Suggestions?