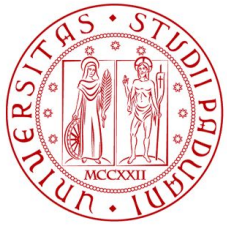
Ethical Hacking

2021-2022

Lesson 5: Cryptographic Tools pt.2

Professors
Luca Pajola
pajola@math.unipd.it.
Pier Paolo Tricomi
pierpaolo.tricomi@phd.unipd.it

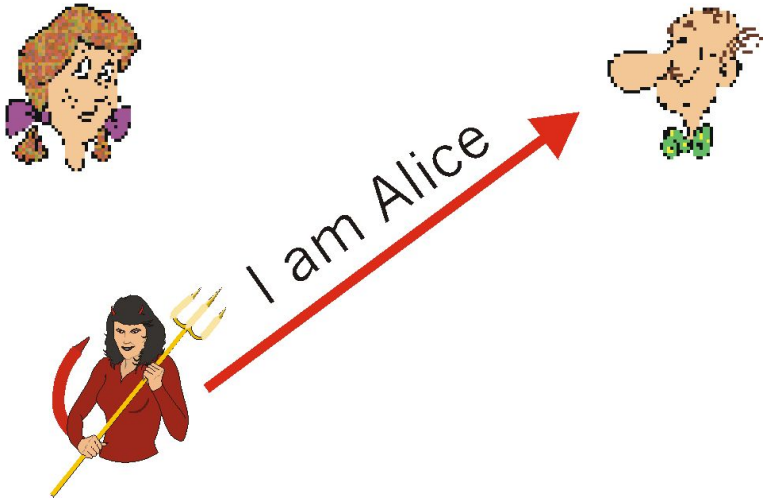


UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

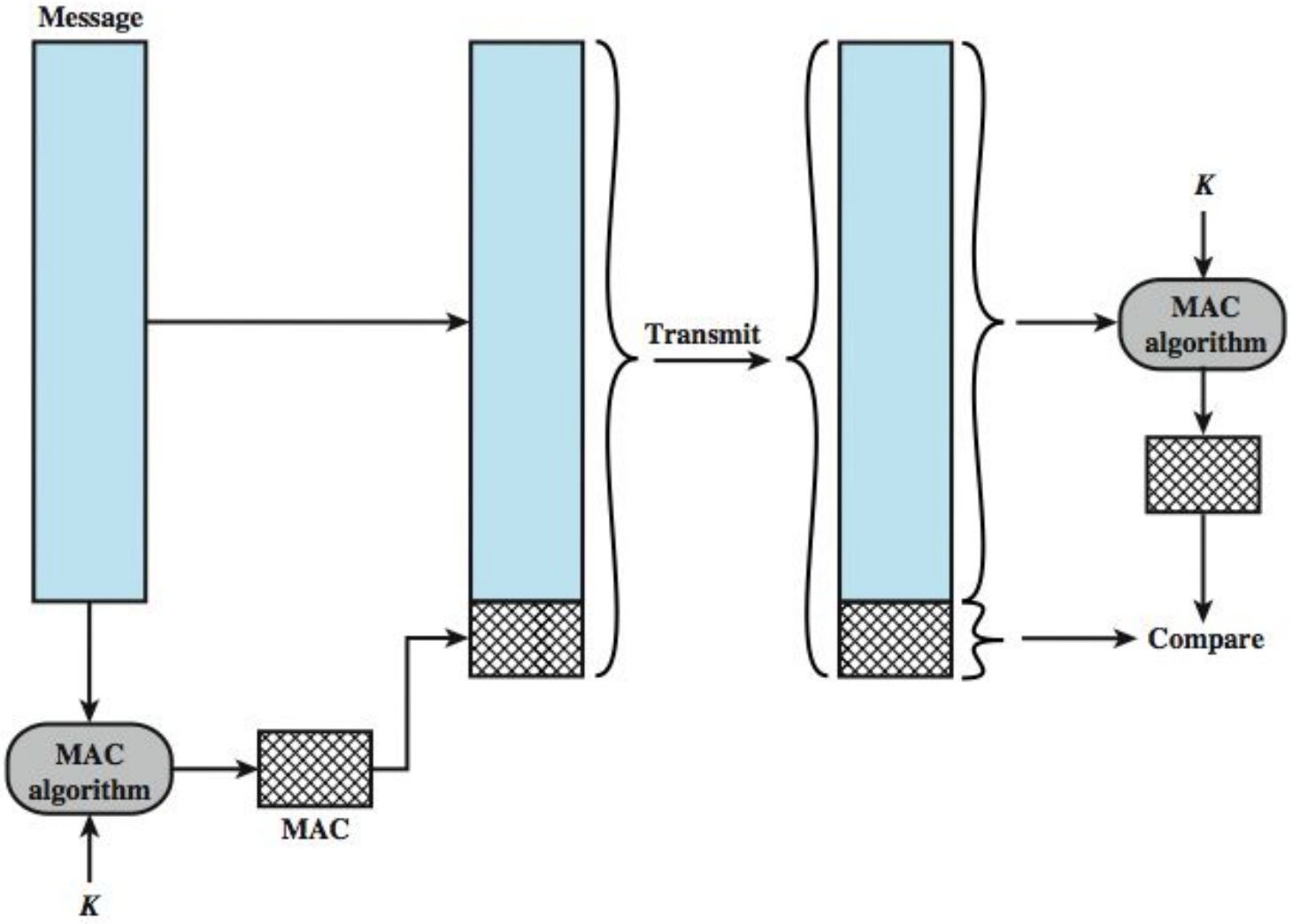
Message Authentication



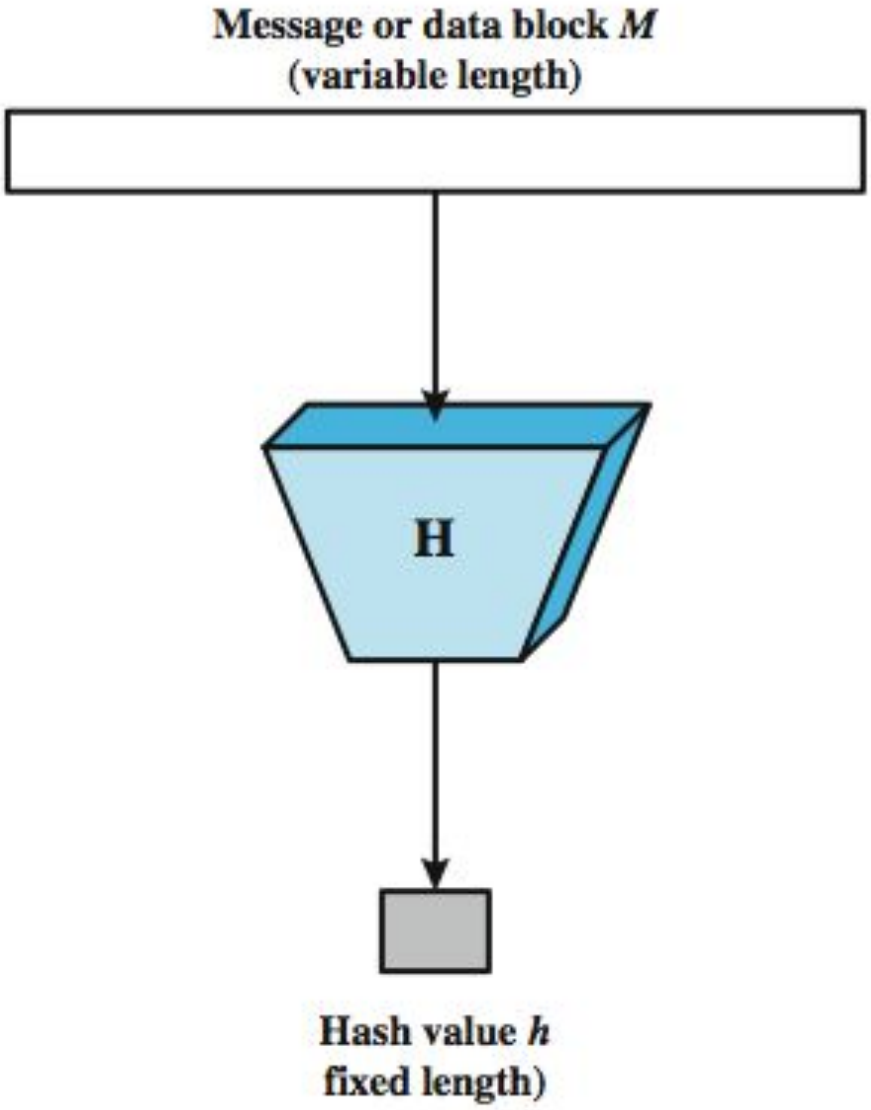
Message Authentication

- 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

- 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

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?