CT255
Introduction to Cyber-Security

Lecture 9
Message Authentication

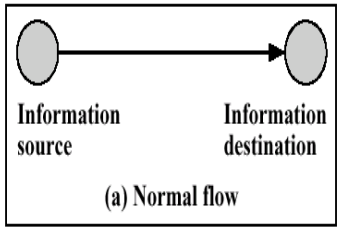
Dr. Michael Schukat, 2019-2022

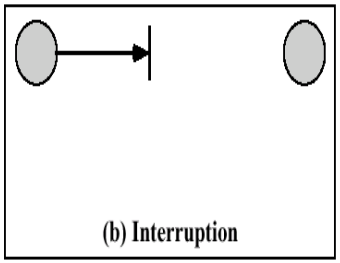
Outline

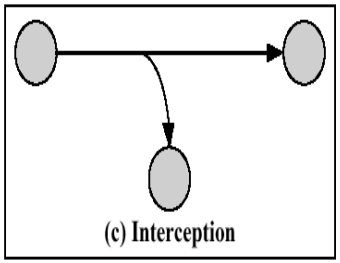
- Types of security attacks
- Message Authentication
- Hash functions revisited

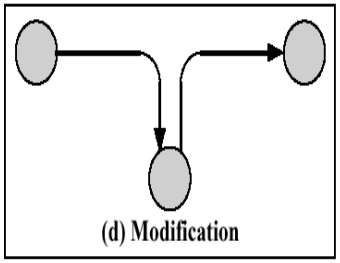
Types of Security Attacks

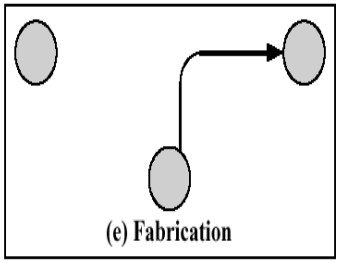
- Interception - of info-traffic flow, attacks confidentiality
- Interruption - of service, attacks availability
- Modification - of info, attacks integrity
- Fabrication - of info, attacks authentication











Passive Attacks

- Are in the nature of eavesdropping or monitoring of transmissions:
  - Release of message content
  - Traffic analysis
    - Analyse pattern of messages (sender, receiver, timing) rather than content
  - Tools like Wireshark allow eavesdropping on network traffic

Active Attacks

- Involved modification or creation of data stream:
  - Masquerade
    - Pretend to be a different entity
  - Replay
    - Retransmission of captured data
  - Modification of message
  - Denial of service (DoS)
    - Inhibits the normal use of communication services

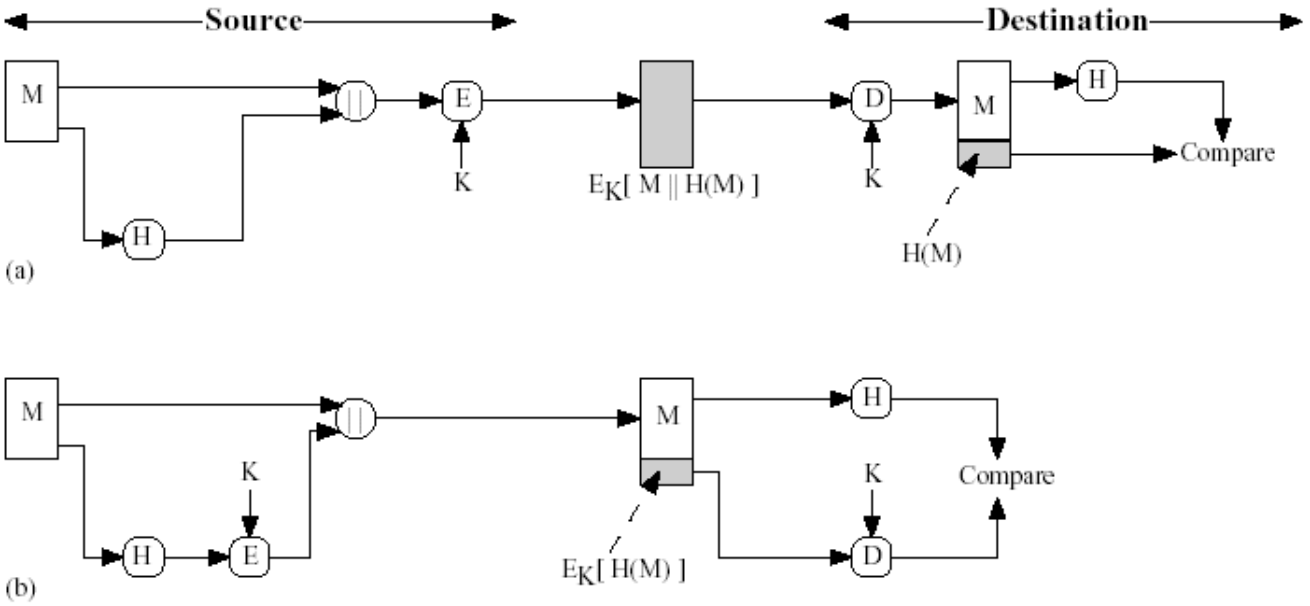
Message Authentication

- There are four types of attacks in the context of communication across a network, which are addressed by message authentication:
  - **Masquerad**e: insertion of messages into the network from a fraudulent source
  - **Content modification**
  - **Sequence modification**
  - **Timing modification**: delete or repeat messages
- Message authentication is concerned with:
  - Protecting the integrity of a message
  - Validating identity of originator
  - Validating sequencing and timeliness
  - Non-repudiation of origin (dispute resolution)

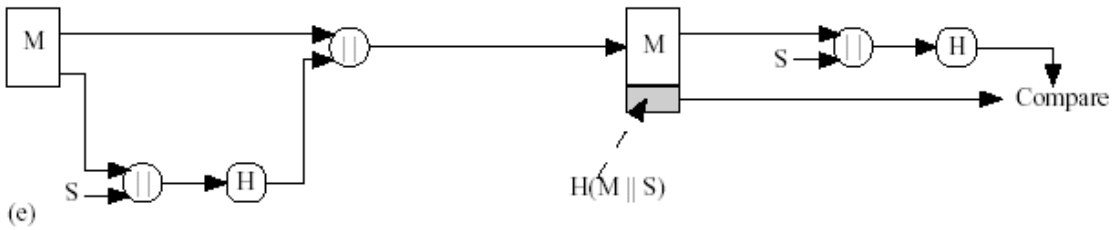
Hash Functions

- A hash function is a variation of a MAC, which produces a fixed size hash code ("**fingerprint**") based on a variable size input message
- A hash function is public and is not keyed, therefore the hash value must be encrypted
- Traditional CRCs are to weak and cannot be used (see requirements for hash functions)
- 128-512 bits hash values are regarded as suitable

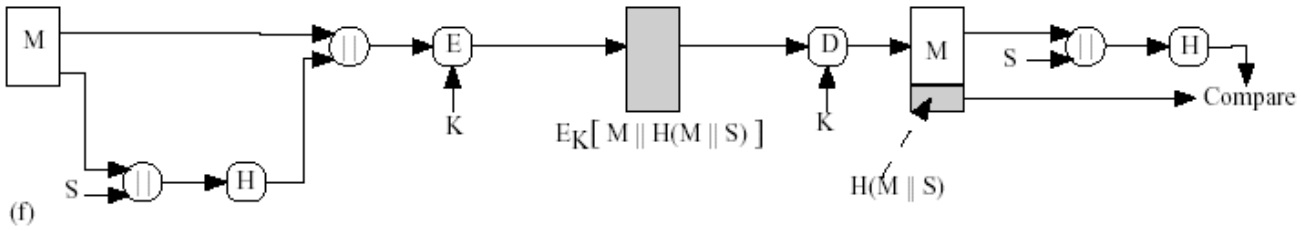
Basic Uses of Hash Functions



Basic Uses of Hash Functions



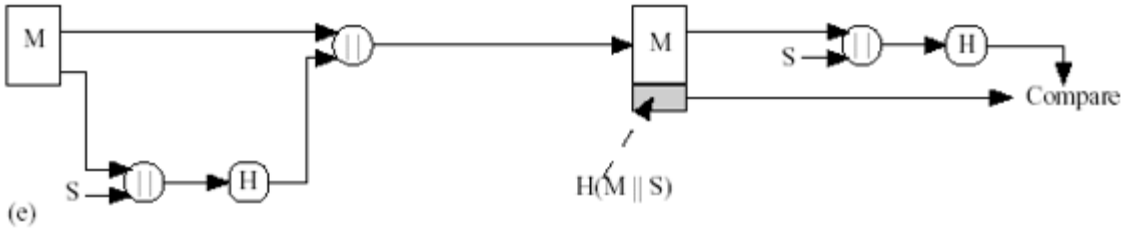
(e)



(f)

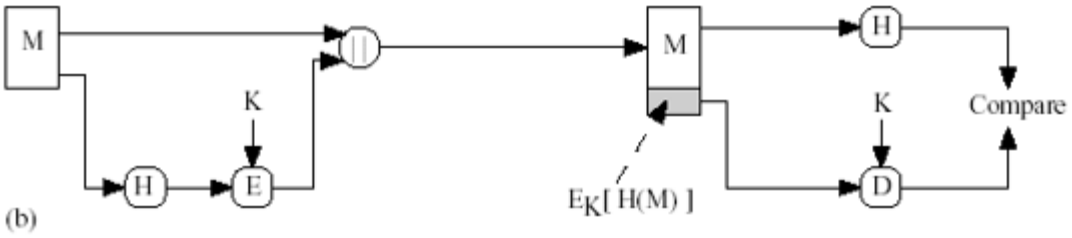
Recall: Requirements for Hash Functions H(x)

- **One way property**:
  For a given hash code h it is infeasible to find x that H(x) = h
- Reason:
  See Figure (e): An opponent could reveal secret key s otherwise



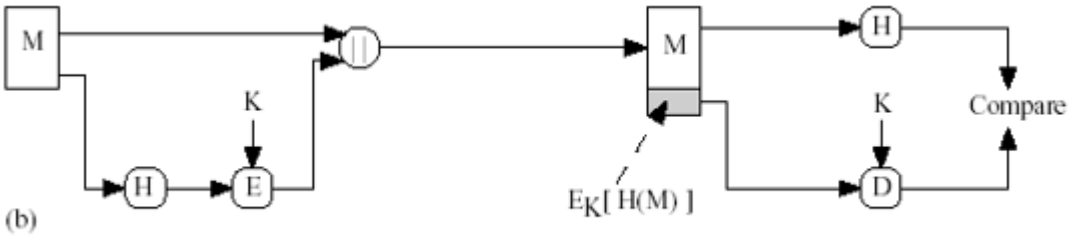
Recall: Requirements for Hash Functions H(x)

- **Weak collision resistance**:
  For a given block (or text) x it it is infeasible to find another block (or text) y with
  y != x with H(x) = H(y)
- Reason:
  See Figure (b): An opponent can calculate the hash code for M, find an alternate message with the same hash code, and send it together with the encrypted (original) hash code to the receiver



Recall: Requirements for Hash Functions H(x)

- **Strong collision resistance**:
  It is computational infeasible to find a pair of blocks (or texts) (x, y) with $H(x) = H(y)$
- Reason:
  See Figure (b), where the message is not encoded and no additional secret key for the hash function is used.
  Attack is based on (counterintuitive) **Birthday Paradox**



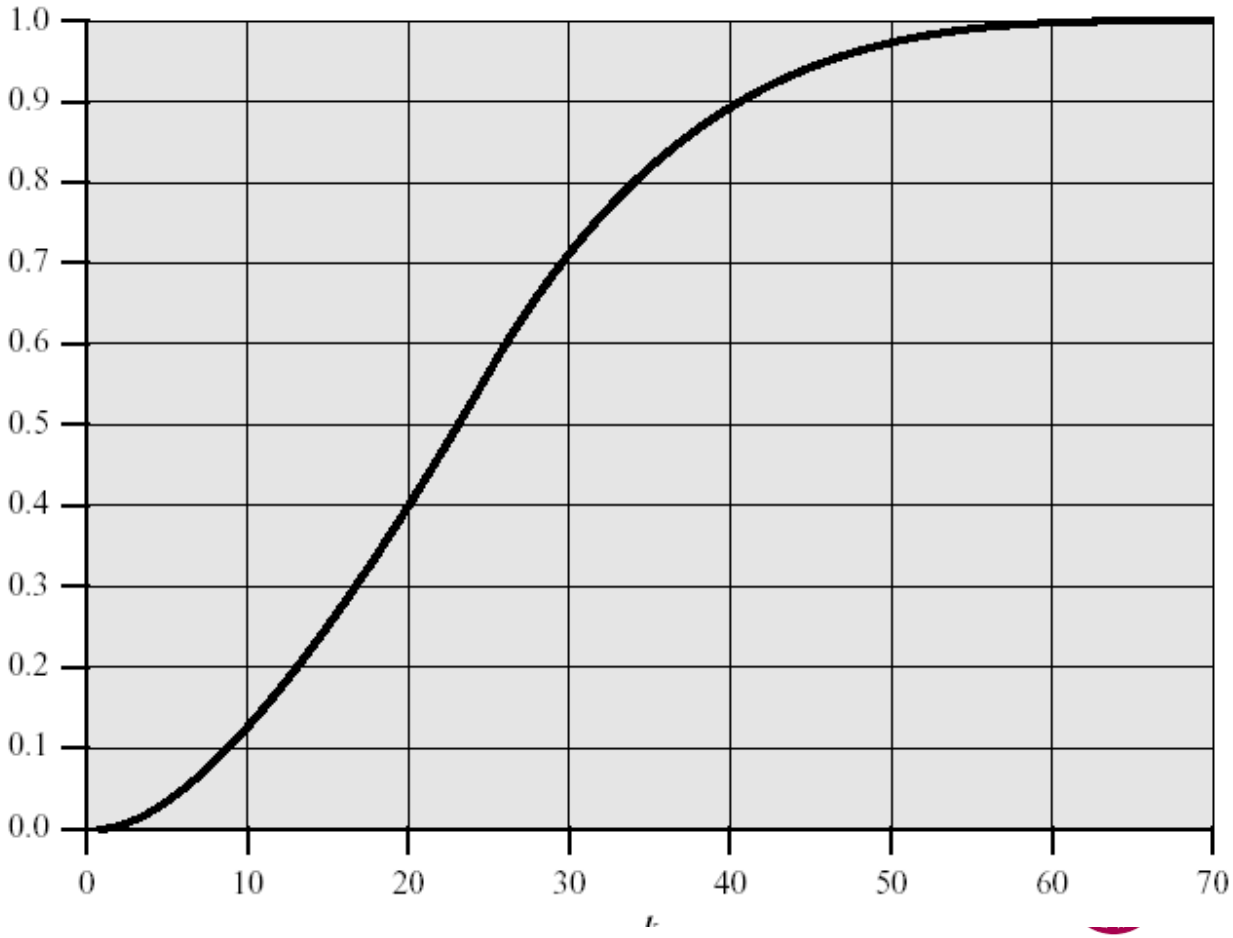
Recall: Birthday Paradox

- What is the minimum value k such that the probability is greater than 50% that at least 2 people in a group of k people have the same birthday, assuming that a year has 365 days?

- Intuitively someone would assume that
  $k = 365 / 2 = 183$

- Probability theory shows, that $k = 23$ is sufficient!

Birthday Paradox



CT255 (S1) Summary

- We covered:
  - GDPR
  - Basic Cryptographic concepts including
    - Classic cryptography
    - Block ciphers, stream ciphers
    - Hash functions and rainbow tables
  - User passwords social engineering

Week 12 MCQ

- Open book, worth 5% (out of 50%)
- 20 random questions covering all CT255 topics
- 20 minutes time to complete
- One question at a time is shown
- Backtracking is not allowed
- Monday 21/11, 13:30 – 13:50 sharp
  - i.e. quiz has to be submitted by 13:50