Password Security

CSCE 499 Technical Presentation

Daniel Case - BA Computer Science/BS Mathematics
Faculty Advisor: Dr. George Hauser

Overview of Project

- Text-Driven Password Security Toolkit
  - Three methods of password encryption
  - Three methods of password cracking

- Today will be talking in detail about *hash functions*
- Implementation of MD5

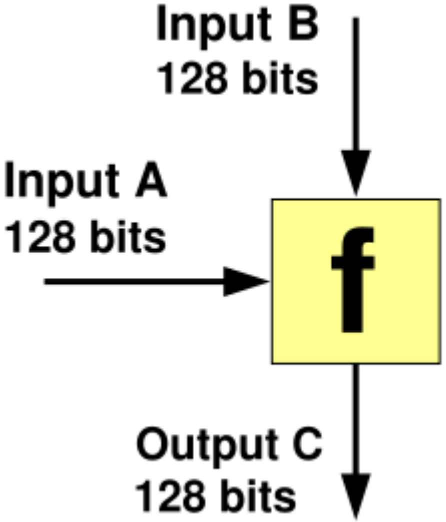
Hash Functions: Definition

- Algorithm that maps strings of *any length* to strings of *fixed length*

- Cryptographic hash function has several properties:
    - Infeasible to generate a message for a given hash
    - Infeasible to find two different messages with the *same* hash
    - Infeasible to modify a message w/out changing the hash

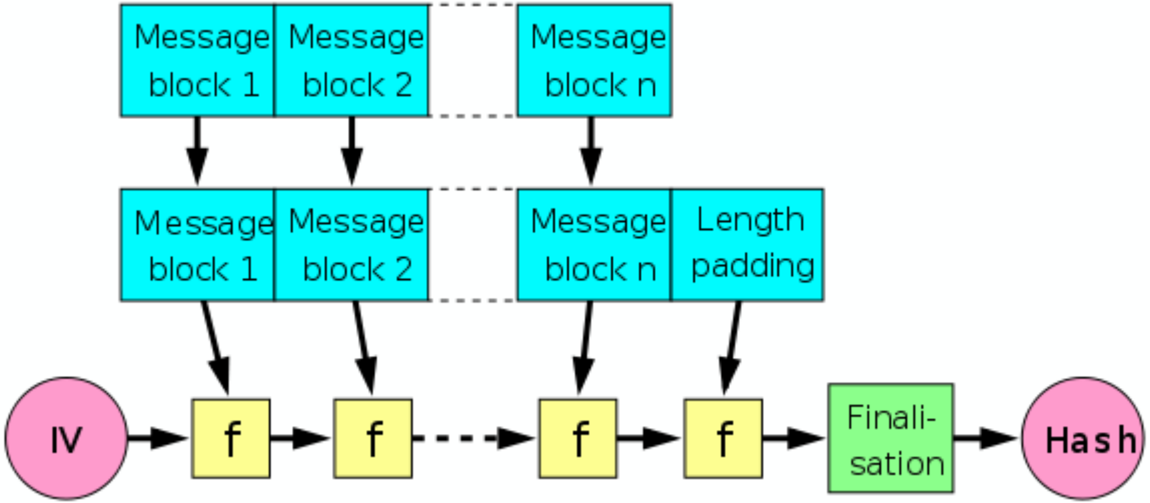
Merkle-Damgard Construction

- Compression function
- Transforms two fixed length inputs into a fixed length output



Merkle-Damgard Construction

- For-loop executes compression function



Code Review

Questions?

Comments?

Images courtesy of wikipedia, hashcat.org, and of course google.com