Classes of Cryptographic Hash Functions:

"Flexible" secure hash functions:
- Based on modular arithmetic
  - E.g.: VSH, Mask

- Based on block ciphers
  - Security in black box model
  - E.g.: MDC-2, MDC-4

Customized Hash Functions:
- Designed for optimal performance
- Very popular, all based on MD4
  - MD4 family: MD4 (cracked, broken)
  - MD5 (CSSL certificates fixed)
  - SHA family: Current standard, but weakened recently, due to differential attacks
    - SHA-1: one out of many attacks
    - SHA-256, SHA-512


Design: (Structured approach)
- Merkle-Damgard construction

M = M_1, ..., M_n

\[ h(M) \]

\[ h(M_1, ..., M_n) \]

Markle-Damgard Strengthening
- Reduced freedom in first block

\[ \text{pad}(M_1, ..., M_n) \]