Classes of Cryptographic Hash Functions:

"provable" secure hash functions: ← usually some properties are provably secure...

bad reputation and very time-consuming w.r.t. other hash functions.

→ based on Modular arithmetic (Security based roughly on factoring RSA moduli)

e.g.: VSH, Mash

→ based on block ciphers (security in black box model).
e.g.: MPC-2, MDC-4

(easy to implement since it is based on known block-ciphers.)

Customized Hash Functions:

→ Designed for optimal performance
→ very popular, all based on MD4.

MD-family: MD4 (already broken)
MD5 (CSSL certificates faked)
RIPEMD, HAVAL (collisions found)
Message Digest Algorithm

SHA-family: Current Standard, but weakened security due to various attacks. Collisions can be found much faster than exhaustive search.
Secure Hash Algorithm
e.g. SHA1, SHA-256, SHA-512

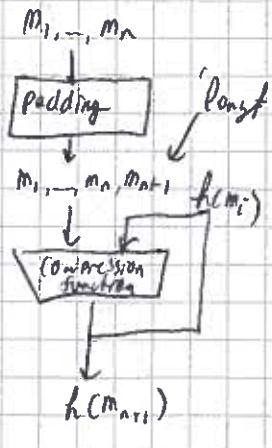
SHA3: Ongoing competition to find next (NIST) standard.
Still 5 proposals left. Final Round.

National Institute of Standards and Technology

Design: (Iterative approach)

Merkle Damgard construction

Merkle Damgard Strengthening
(reduced freedom in finding collisions).



SLIDE