Introductory Cryptography

Message Digests

Kc Udonsi

Message digests

Message digests are meant for creating fingerprints of messages

- Un-keyed message digest : hashes, checksum
- Keyed message digests : MACs