Cryptographic Hash Functions

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

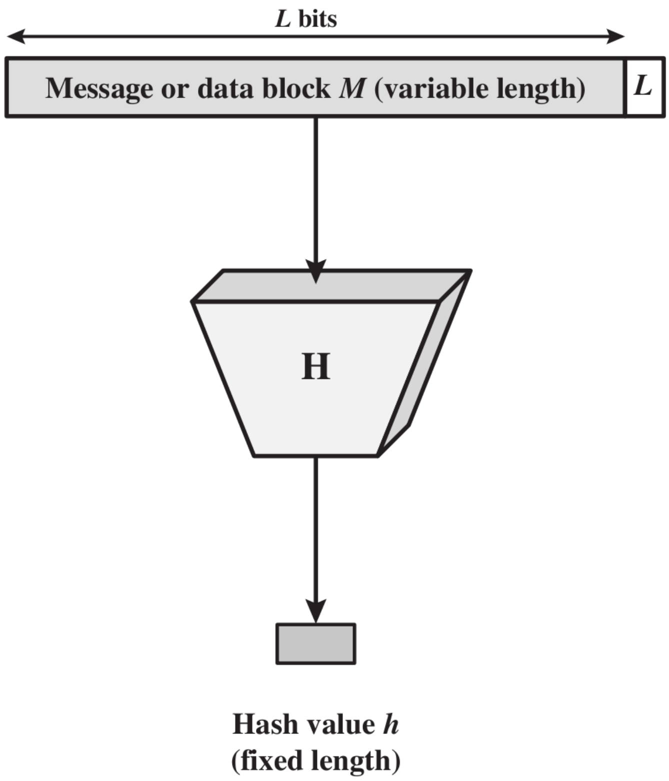
Prepared by Steven Gordon on 28 October 2013
css322y13s2l09, Steve/Courses/2013/s2/css322/lectures/hash.tex, r2963

Contents

Hash Functions

- Hash function H: variable-length block of data M input; fixed-size hash value $h = \mathrm{H}(M)$ output
- Applying H to large set of inputs should produce evenly distributed and random looking outputs
- Cryptographic hash function: computationally infeasible to find:
  1. M that maps to known h (one-way property)
  2. M_1 and M_2 that produce same h (collision-free property)
- Used to determine whether or not data has changed
- Examples: message authentication, digital signatures, one-way password file, intrusion/virus detection, PRNG

Cryptographic Hash Function



Credit: Figure 11.1 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

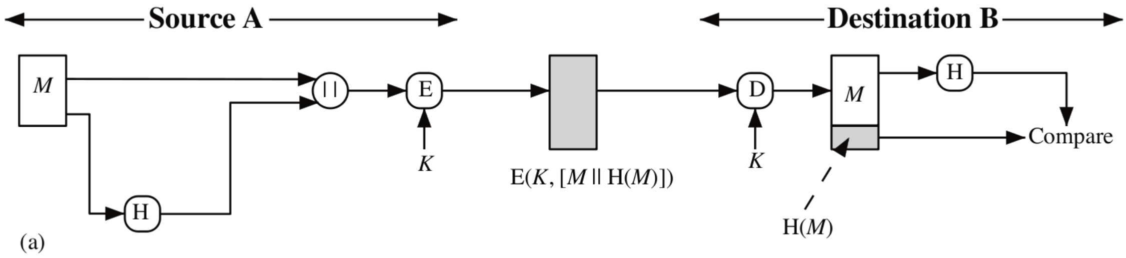
Contents

Message Authentication

- Verify the integrity of a message
  - Ensure data received are exactly as sent
  - Assure identity of the sender is valid
- Hash function used to provide message authentication called message digest

Message Authentication Example (a)

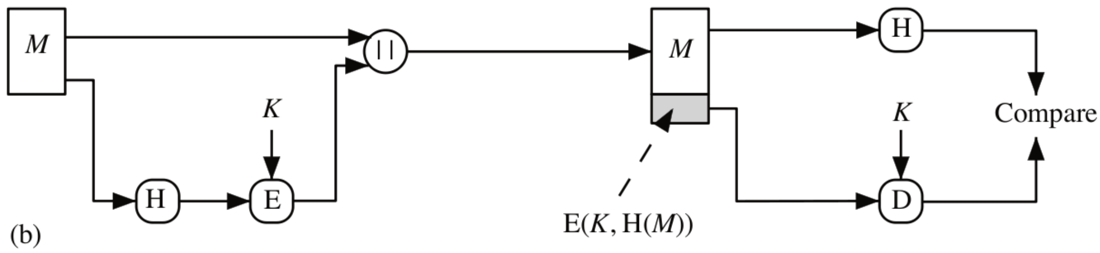
- Encrypt the message and hash code using symmetric encryption



(a)

Message Authentication Example (b)

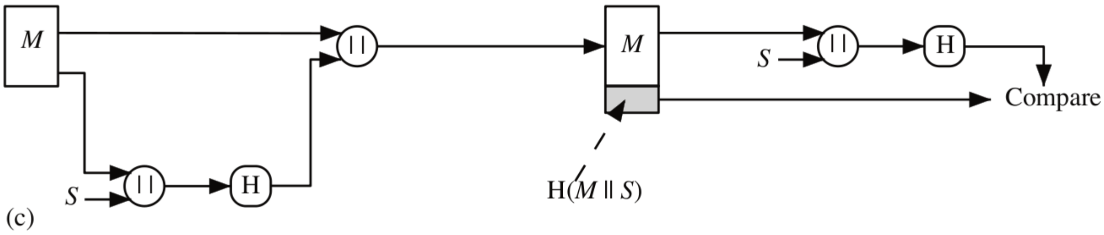
- Encrypt only hash code
- Reduces computation overhead when confidentiality not required



(b)

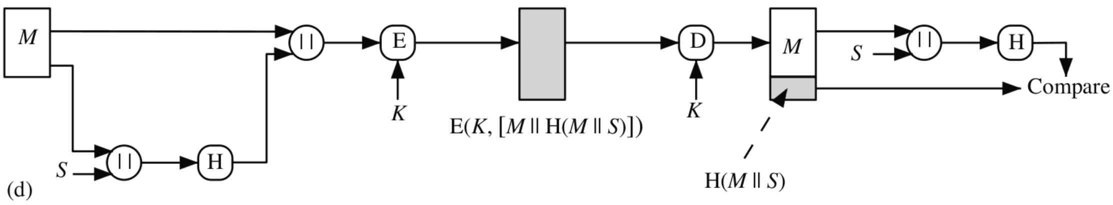
Message Authentication Example (c)

- Shared secret S is hashed
- No encryption needed



Message Authentication Example (d)

- Shared secret combined with confidentiality



Authentication and Encryption

- Sometimes desirable to avoid encryption when performing authentication
  - Encryption in software can be slow
  - Encryption in hardware has financial costs
  - Encryption hardware can be inefficient for small amounts of data
  - Encryption algorithms may be patented, increasing costs to use
- Message Authentication Codes (or keyed hash function)
  - Take secret key K and message M as input; produce hash (or MAC) as output
  - Combining hash function and encryption produces same result as MAC; but MAC algorithms can be more efficient than encryption algorithms
  - MAC covered in next topic

Contents

Digital Signatures

- Aim of a signature: prove to anyone that a message originated at (or is approved by) a particular user
- Symmetric key cryptography
  - Two users, A and B, share a secret key K
  - Receiver of message (user A) can verify that message came from the other user (B)
  - User C *cannot* prove that the message came from B (it may also have came from A)
- Public key cryptography can provide signature: only one user has the private key

Digital Signature Operations (Concept)

Signing

- User signs a message by encrypting with own private key

$$S = E(PR_A, M)$$

- User attaches signature to message

Verification

- User verifies a message by decrypting signature with signer's public key

$$M' = D(PU_A, S)$$

- User then compares received message M with decrypted M'; if identical, signature is verified

Digital Signature Operations (Practice)

No need to encrypt entire message; encrypt hash of message

Signing

- User signs a message by encrypting hash of message with own private key

$$S = E(PR_A, H(M))$$

- User attaches signature to message

Verification

- User verifies a message by decrypting signature with signer's public key

$$h = D(PU_A, S)$$

- User then compares hash of received message, $H(M)$, with decrypted h; if identical, signature is verified

Digital Signature Algorithms

- RSA
- Digital Signature Algorithm (DSA): FIPS-186
- ECDSA: DSA with elliptic curve cryptography
- ElGamal signature scheme: DSA is enhancement of ElGamal
- Bilinear pairing based signatures, e.g. BLS
- Different hash algorithms can be used; e.g. SHA2
  - Pre-image resistant, second pre-image resistant, collision resistant

Contents

Pre-images and Collisions

- For hash value $h = \mathrm{H}(x)$, x is pre-image of h
- H is a many-to-one mapping; h has multiple pre-images
- Collision occurs if $x \neq y$ and $\mathrm{H}(x) = \mathrm{H}(y)$
- Collisions are undesirable
- How many pre-images for given hash value?
  - If H takes b-bit input block, 2^b possible messages
  - For n-bit hash code, where $b > n$, 2^n possible hash codes
  - On average, if uniformly distributed hash values, then each hash value has 2^{b-n} pre-images

Requirements of Cryptographic Hash Function

Variable input size: H can be applied to input block of any size

Fixed output size: H produces fixed length output

Efficiency: $\mathrm{H}(x)$ relatively easy to compute (practical implementations)

Pre-image resistant: For any given h, computationally infeasible to find y such that $\mathrm{H}(y) = h$ (*one-way property*)

Second pre-image resistant: For any given x, computationally infeasible to find $y \neq x$ with $\mathrm{H}(y) = \mathrm{H}(x)$ (*weak collision resistant*)

Collision resistant: Computationally infeasible to find any pair (x, y) such that $\mathrm{H}(x) = \mathrm{H}(y)$ (*strong collision resistant*)

Pseudo-randomness: Output of H meets standard tests for pseudo-randomness

Required Hash Properties for Different Applications

Weak hash function: Satisfies first 5 requirements (but not collision resistant)

Strong hash function: Also collision resistant

	Preimage Resistant	Second Preimage Resistant	Collision Resistant
Hash + digital signature	yes	yes	yes*
Intrusion detection and virus detection		yes	
Hash + symmetric encryption			
One-way password file	yes		
MAC	yes	yes	yes*

* Resistance required if attacker is able to mount a chosen message attack

Credit: Table 11.2 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Brute Attacks on Hash Functions

Pre-image and Second Pre-image Attack

- Find a y that gives specific h; try all possible values of y
- With m-bit hash code, effort required proportional to 2^m

Collision Resistant Brute Attack

- Find any two messages that have same hash values
- Effort required is proportional to $2^{m/2}$
- Due to birthday paradox, easier than pre-image attacks

Practical Effort

- Cryptanalysis attacks possible in theory; complex
- Collision resistance desirable for general hash algorithms
- MD5 uses 128-bits: collision attacks possible (2^{60})
- SHA uses longer codes; collision attacks infeasible

Contents

MD5

- Message Digest algorithm 5, developed by Ron Rivest in 1991
- Standardised by IETF in RFC 1321
- Generates 128-bit hash
- Was commonly used by applications, passwords, file integrity; no longer recommended
- Collision and other attacks possible; tools publicly available to attack MD5

SHA

- Secure Hash Algorithm, developed by NIST
- Standardised by NIST in FIPS 180 in 1993
- Improvements over time: SHA-0, SHA-1, SHA-2, SHA-3
- SHA-1 (and SHA-0) are considered insecure; no longer recommended
- SHA-3 in development, competition run by NIST

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Credit: Table 11.3 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011