Lecture 4.2: Hash Functions: Design*

CS 436/636/736
Spring 2012

Nitesh Saxena

* some slides borrowed from Gene Tsudik
Course Administration

• HW1 being graded
• HW2 posted
  — Due Tuesday, 11am – Feb 28
Outline of Today’s lecture

• Hash Functions
  – Known Hash Functions
    • SHA-1
Secure Hash Algorithm (SHA)
- SHA was published by NIST as a standard in 1993

- Revised in 1995 as SHA-1
  - Input: Up to 2⁶⁴ bits
  - Output: 160 bit digest
  - 80-bit collision resistance
- Pad with at least 64 bits to resist padding attack
  - 1000...0<message length>

- Processes 512-bit block
  - Initiate 5x32-bit MD registers
  - Apply compression function
    - 4 rounds of 20 steps each
    - each round uses different non-linear fi
    - registers are shifted and switched

Figure 3.x: SHA-1 Processing of a Single 512-bit Block
SHA-1 of a 512-Bit Block

Figure 3.5 SHA-1 Processing of a Single 512-bit Block

Note: addition (+) is mod 2^32
Basic Steps

Step1: Padding
Step2: Appending length as 64 bit unsigned
Step3: Initialize MD buffer 5 32-bit words

A|B|C|D|E
A = 67452301
B = efcdab89
C = 98badcfe
D = 10325476
E = c3d2e1f0
Basic Steps...

Step 4: the 80-step processing of 512-bit blocks: 4 rounds, 20 steps each

Each step $t$ ($0 \leq t \leq 79$):
- Input:
  - $W_t$ - a 32-bit word from the message
  - $K_t$ - a constant
  - ABCDE: current MD
- Output:
  - ABCDE: new MD
Basic Steps...

- Only 4 per-round distinctive additive constants
  - $0 \leq t < 19 \ K_t = 5A827999$
  - $20 \leq t < 39 \ K_t = 6ED9EBA1$
  - $40 \leq t < 59 \ K_t = 8F1BBCDC$
  - $60 \leq t < 79 \ K_t = CA62C1D6$
CLS: Circular Left Shift
Basic Logic Functions

- Only 3 different functions

<table>
<thead>
<tr>
<th>Round</th>
<th>Function $f_r(B,C,D)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 $\leq t &lt; 19$</td>
<td>$(B \land C) \lor (\neg B \land D)$</td>
</tr>
<tr>
<td>20 $\leq t &lt; 39$</td>
<td>$B \oplus C \oplus D$</td>
</tr>
<tr>
<td>40 $\leq t &lt; 59$</td>
<td>$(B \land C) \lor (B \land D) \lor (C \land D)$</td>
</tr>
<tr>
<td>60 $\leq t &lt; 79$</td>
<td>$B \oplus C \oplus D$</td>
</tr>
</tbody>
</table>
Twist With $W_t$’s

- Additional mixing used with input message 512-bit block
  $W_0|W_1|...|W_{15} = m_0|m_1|m_2|...|m_{15}$
  For $15 < t < 80$:
  $W_t = W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}$

- XOR is a very efficient operation, but with multilevel shifting, it should produce very extensive and random mixing!
Other Hash Functions

• Many other hash functions
  – SHA-2 (SHA-256)
    • Output 256 bits
  – MD5 – Message Digest algorithm 5
    • Output 128 bits
    • Very similar to SHA – please study on your own
  – MD4
  – MD6
  – ..
Current Security of MD5 and SHA-1

• SHA-1
  – B’day attack requires $2^{80}$ calls
  – Faster attacks $2^{69}$ calls
  [http://infosec.sdu.edu.cn/uploadfile/papers/Finding%20Collisions%20in%20the%20Full%20SHA-1.pdf](http://infosec.sdu.edu.cn/uploadfile/papers/Finding%20Collisions%20in%20the%20Full%20SHA-1.pdf)

• MD5
  – Output is 128-bits, so B’day attack requires $2^{64}$ calls only
  – Faster attacks to find a collision:

• Better use stronger versions, such as SHA-256
• Although, these attacks are still not practical – they only find two random messages that collide
Further Reading

- Stallings Chapter 11
- HAC Chapter 9