SHA2

• SHA2 is a **public** algorithm
  – *Security in the mathematics, not in keeping the implementation a secret*

Process the entire message, 64 times.
• Right now, SHA2 is considered a secure hash.
  – *Mathematics have not been broken*
  – *The complexity of reversing a hash would take more computing power than has ever been created*

– SHA2 has several variants based on the length of the output desired: SHA-256 (256-bit output) is most common.
Other Algorithms

• **MD5 (1991):**
  – 2005-2008: MD5 was mathematically simplified and available processing power could fake hashes
  – “should be considered cryptographically broken and unsuitable for further use”

• **SHA-0 (1993):**
  – 1998: Was shown to be easily simplified; some hashes can be reversed in less than an hour!

• **SHA-1 (1995):**
  – Replacement to concerns about SHA-0
  – 2005: Theoretical attack developed showing some weakness in the mathematics (reverse in \( \leq 2^{69} \))
Sharing a Secret

- **Diffie–Hellman Key Exchange**
  - Secure algorithm with large numbers
  - Demonstrates the basics of how SSL works

- **Setup:**
  - Two parties: Alice and Bob
  - Alice and Bob both agree on a prime number $p$ and a primitive root of $p$ called $g$. 
Alice

- $p = 23$
- $g = 5$
Bob

- $p = 23$
- $g = 5$
Secret
Attacker