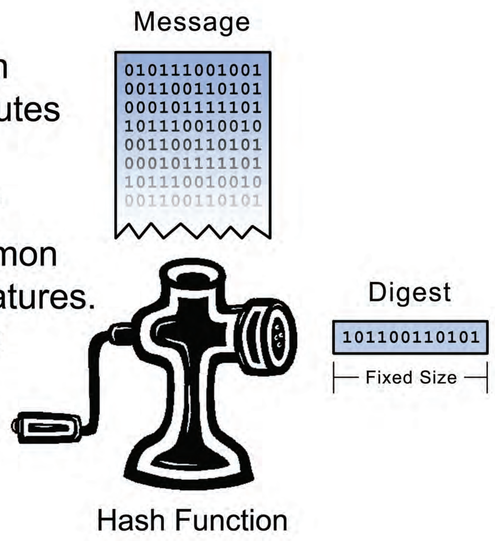
A New Foundation in Cryptographic Hashing

By William R. Speirs II

Traditional Cryptographic Hash Functions

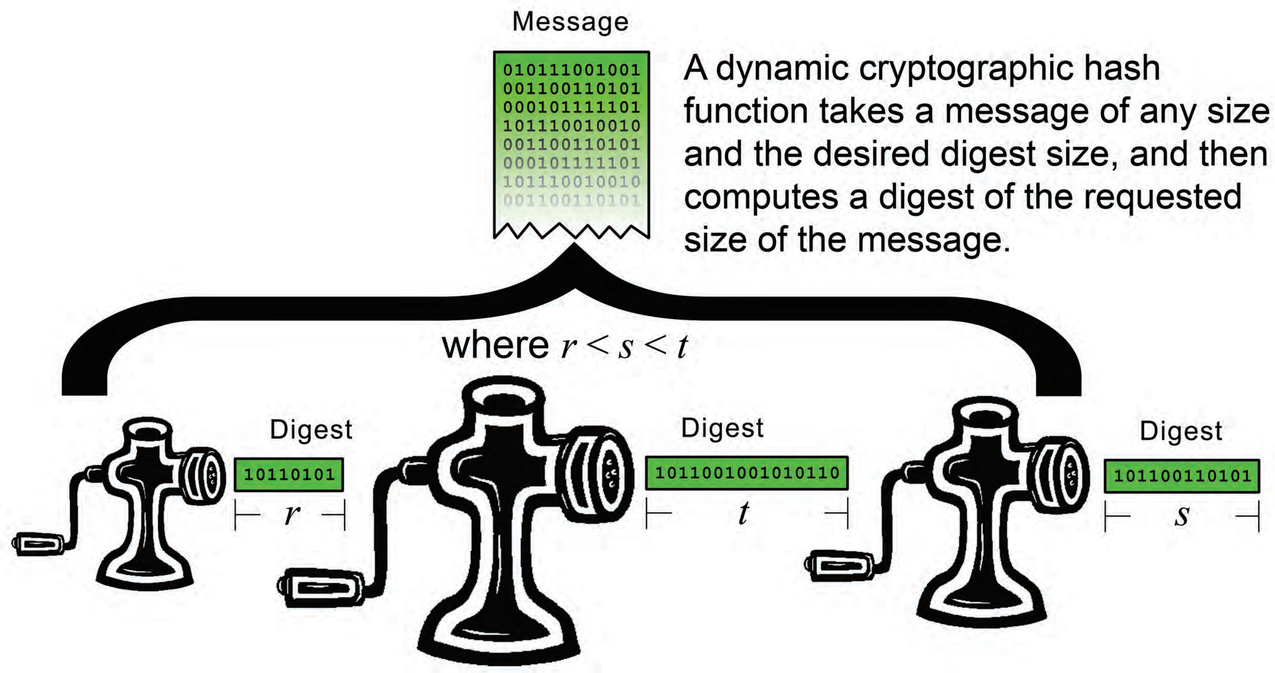
A traditional cryptographic hash function takes a message of any size and computes a fixed size digest of the message.

Hash functions are used in a number of cryptographic protocols. The most common use for a hash function is in digital signatures. Integrity of a message is the other most common use for a hash function. The digest of a message can be considered a unique identifier for the message.



Dynamic Cryptographic Hash Functions

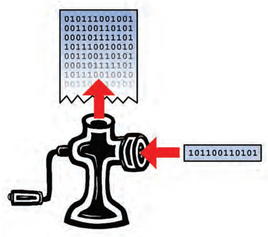
A dynamic cryptographic hash function takes a message of any size and the desired digest size, and then computes a digest of the requested size of the message.



Requirements For Security

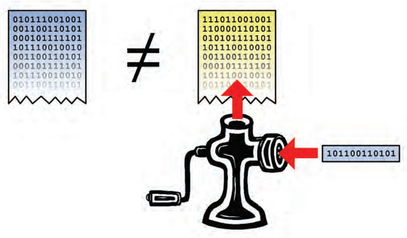
1) Preimage Resistance

For essentially all pre-specified outpus, it is computationally infeasible to find any input which hashes to that output, i.e., to find any preimage x' such that $h(x') = y$ when given any y for which a corresponding input is not known.



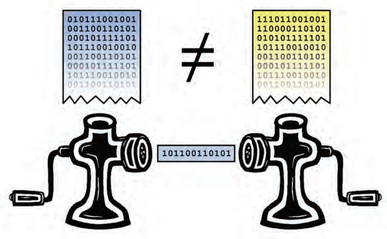
2) Second Preimage Resistance

It is computationally infeasible to find any second input which has the same output as any specified input, i.e., given x, to find a 2nd-preimage $x' \neq x$ such that $h(x) = h(x')$.



3) Collision Resistance

It is computationally infeasible to find any two distinct inputs x, x' which hash to the same output, i.e., such that $h(x) = h(x')$. (Note that here there is a free choice of both inputs.)



Requirements For Security

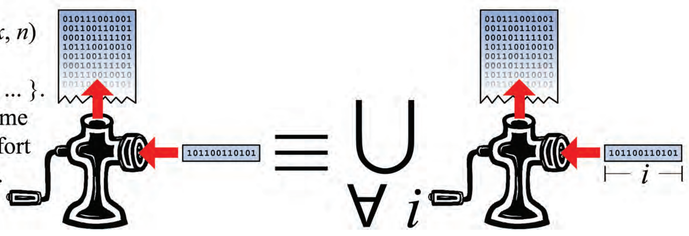
1) Preimage Resistance

2) Second Preimage Resistance

3) Collision Resistance

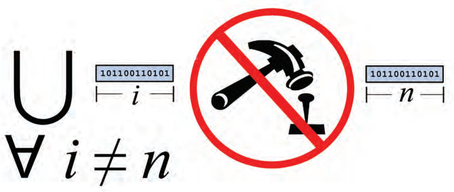
4) Digest-Size Preimage Resistance

Producing the preimage of $h(x, n)$ given only $h(x, n)$ is computationally equivalent to producing the preimage of $h(x, n)$ when given $\{h(x, 1), h(x, 2), \ldots\}$. Essentially, given different size digests of the same message does not decrease the computational effort to invert a dynamic cryptographic hash function.



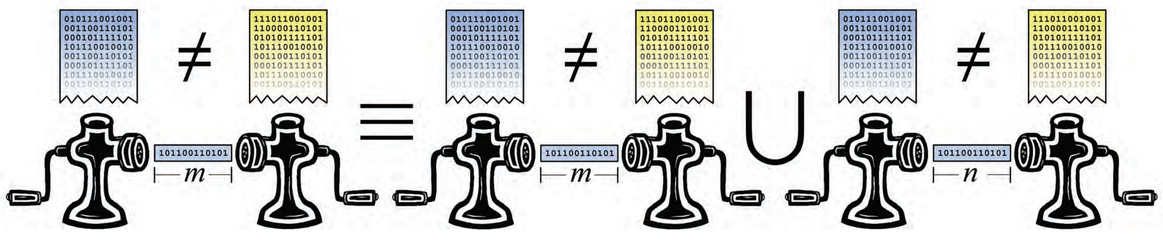
5) Digest-Size Resistance

Given $\{h(x, 1), \ldots, h(x, n - 1), h(x, n + 1), \ldots\}$ only, does not allow one to create $h(x, n)$. Essentially, one cannot construct the n-bit digest of a message from other size digests.



6) Digest-Size Collision Resistance

Given two messages x and x', where $x \neq x'$ and $h(x, n) = h(x', n)$; knowing this collision does not reduce the computational complexity of creating two messages y and y', where $y \neq y'$ and $h(y, m) = h(y', m)$ where $m \neq n$.



Current Attacks*

Practical	Theoretical	No Known
HAVAL	HAVAL	RIPEMD-160
MD2	PANAMA	SHA-2 Family
MD4	SHA-1	Tiger
MD5	StepRightUp	WHIRLPOOL
N-Hash		
RIPEMD		
SHA-0		
SMASH		
Snefru		

*Attack information taken from: http://paginas.terra.com.br/informatica/paulobarreto/hflounge.html

Art contributions by: Ian Molloy & Barry Wittman

PURDUE UNIVERSITY
PURDUE HOMELAND SECURITY INSTITUTE
CERIAS
REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING
Discovery Park e-Enterprise Center