
Update from RSA 2005: More Hash Function Collisions

Cryptography Research, Inc.

www.cryptography.com

575 Market St., 21st Floor, San Francisco, CA 94105

© 1998-2004 Cryptography Research, Inc. Protected under issued and/or pending US and/or international patents. All trademarks are the property of their respective owners. The information contained in this presentation is provided for illustrative purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of CRI or its partners. Unauthorized copying, use or redistribution is prohibited.

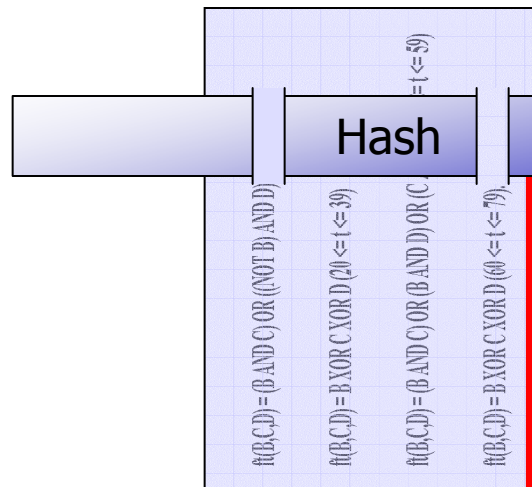
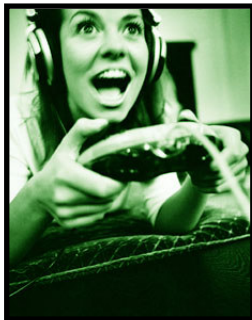


Background: cryptographic hash functions

Compress a large amount of data down to a constant size

- └ Different from compression functions: hash cannot be “uncompressed”
- └ Used for message authentication (digital signatures), commitment schemes, etc.

Pre-image



Hash

7073cc8f46d53b38013d
30c229be49dd17ecd876

7073cc8f46d53b38013d
30c229be49dd17ecd876

Cannot find pre-image



Background: cryptographic hash functions

Compress a large amount of data down to a constant size

- └ Different from compression functions: hash cannot be “uncompressed”
- └ Used for message authentication (digital signatures), commitment schemes, etc.

Security requirements include:

- └ Infeasible to find two messages that hash to the same value
 - Attacks that violate this property are called collision attacks
- └ Infeasible to find an input message that hashes to a particular value
 - Attacks that violate this property are called pre-image attacks

Commonly used cryptographic hash functions

- └ MD4, MD5 (e.g. VeriSign certificates, “md5sum” program)
- └ SHA-1 (e.g. DSS, PGP)



Developments announced at RSA 2005

Collisions announced in SHA-1

- ┌ Xiaoyun Wang, Shandong University, China
- ┌ Yiqun Lisa Yin, Princeton
- ┌ Hongbo Yu, Shandong University, China
- ┌ Based on previous attacks against MD4, MD5 and SHA-0
- ┌ Paper not yet available

Complexity: $< 2^{69}$ hash operations (~ 590 billion billion)

Barely possible with today's technology

- ┌ Example: 3743 custom chips capable of 10 billion hashes/second running for 6 months



What does this mean?

Attack presented is a collision attack (not pre-image attack)

- └ No need to panic (yet). New standards should be developed
- └ Attack does not apply to all systems that use the SHA-1 algorithm (it depends on how the algorithm is used)
 - Systems that sign data from untrusted sources need examination
- └ Still extremely computationally difficult to attack

“It's time to walk, but not run, to the fire exits. You don't see smoke, but the fire alarms have gone off.”

-Jon Callas, CTO PGP Corporation



More information

Details available at:

www.cryptography.com/cnews

