UNIVERSITY OF AMSTERDAM

Jaap van Ginkel

Security of Systems and Networks

September 12, 2024 Part 4 Modern Crypto Hashing

Recap Question DES

A) Is optimized for software implementation

B) Was established during a public competition

C) Is considered a Feistel Cipher

D) Was Developed in the 1980’s

Recap Question AES

A) Is optimized for hardware implementation

B) Is an SPN cipher

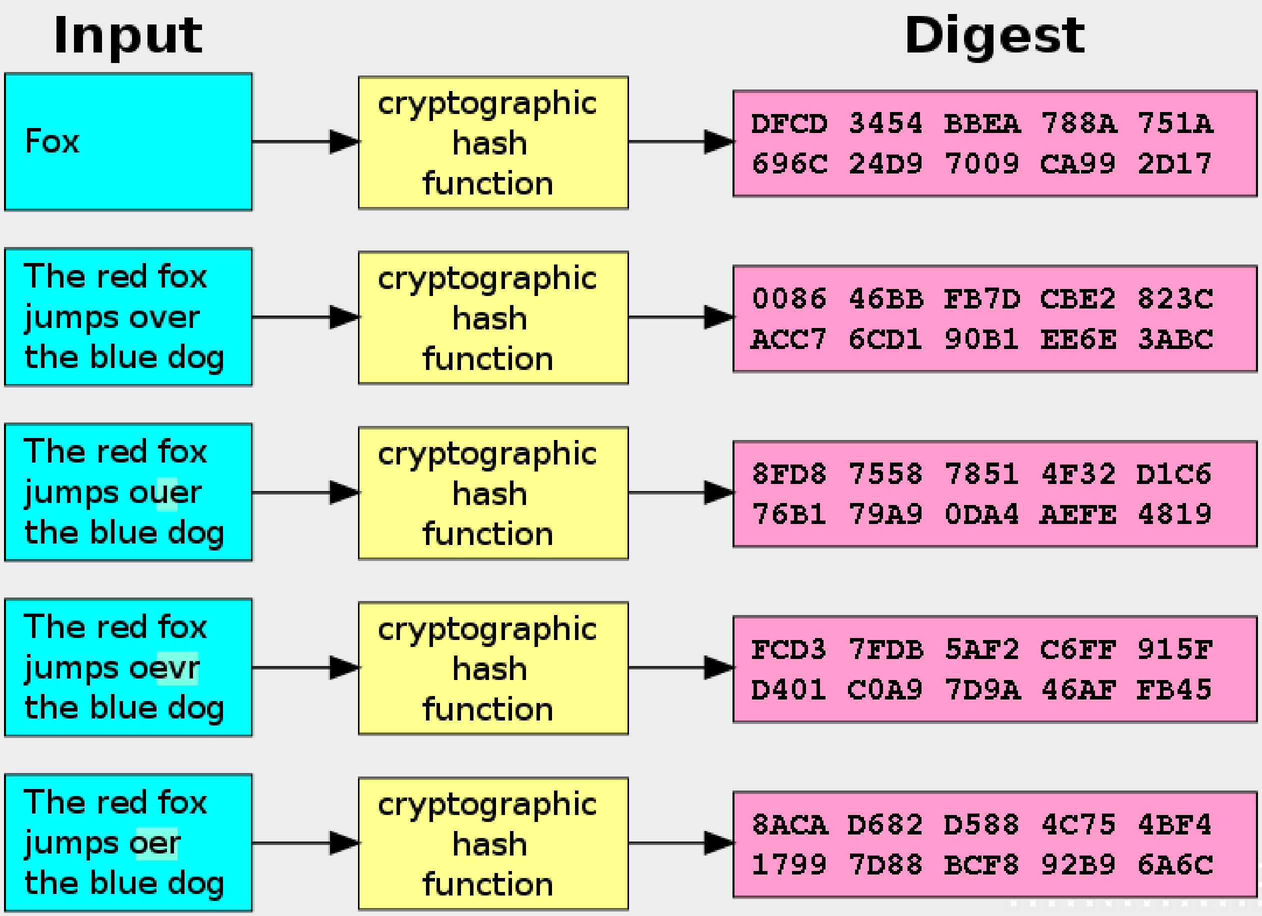
C) Is considered a Feistel Cipher

D) Was Developed in the 1980’s

SSN Modern Cryptography

- Hashes
  - MD5
  - SHA
  - SHA-2
  - SHA-3

HASH or Message Digest



Crypto Hash Function

- Crypto hash function h(x) must provide
  - **Compression** — output length is small
  - **Efficiency** — h(x) easy to compute for any x
  - **One-way** — given a value y it is infeasible to find an x such that h(x) = y
  - **Weak collision resistance** — given x and h(x), infeasible to find y ≠ x such that h(y) = h(x)
  - **Strong collision resistance** — infeasible to find ***any*** x and y, with x ≠ y such that h(x) = h(y)
- Lots of collisions exist, but hard to find ***any***

Pre-Birthday Problem

- Suppose N people in a room
- How large must N be before the probability someone has same birthday as me is $\geq 1/2$?
  - Solve: $1/2 = 1 - (364/365)N$ for N
  - We find $N = 253$

Birthday Problem

- How many people must be in a room before probability is $\geq 1/2$ that any two (or more) have same birthday?
  - $1 - 365/365 \cdot 364/365 \cdots (365-N+1)/365$
  - Set equal to 1/2 and solve: **N = 23**
- Surprising? A paradox?
- Maybe not: "Should be" about sqrt(365) since we compare all **pairs** x and y
  - And there are 365 possible birthdays

Non-crypto Hash (1)

- Data X = (X_0,X_1,X_2,…,Xn-1), each Xi is a byte
- Define h(X) = X0+X1+X2+…+Xn-1
- Is this a secure cryptographic hash?
- Example: X = (10101010, 00001111)
- Hash is h(X) = 10111001
- If Y = (00001111, 10101010) then h(X) = h(Y)
- Easy to find collisions, so **not** secure…

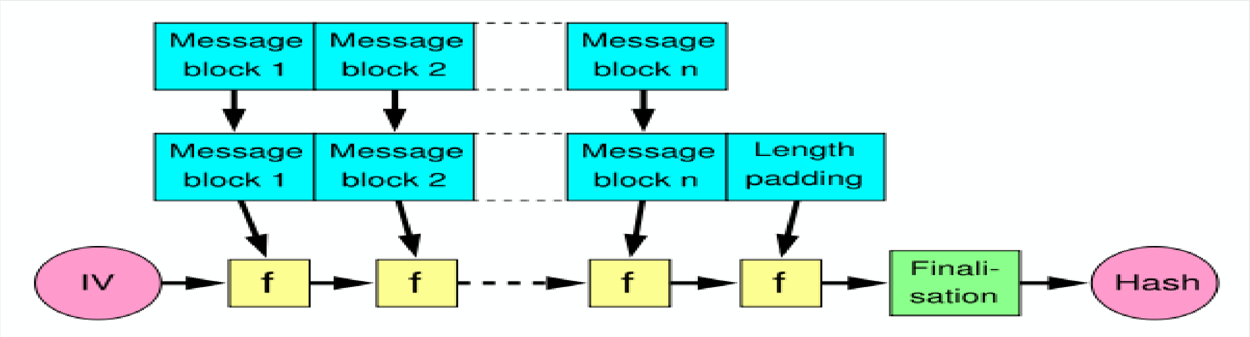
Popular Crypto Hashes

- **MD5** — invented by Rivest
  - 128 bit output
  - Note: MD5 collisions easy to find
- **SHA-1** — A U.S. government standard, inner workings similar to MD5
  - 160 bit output
- SHA-2 – A NIST standard
- Hashes work by hashing message in blocks

Cryptographic Hash

- Different from parity or CRC !
- Also known as Message Digest
- Input always delivers fixed length output
- Hash properties
  - Easy to compute
  - One-way (Can't go back)
  - Collision-resistant (No two inputs result in same hash)
  - Output should be as random as possible (Avalanche)
    - (cryptool demo)

Merkle-Damgård Construction



HASH Algorithms

- MD
- MD2
- MD4
- MD5 (IETF RFC1321),
- SHA
- SHA-1 (NIST)
- SHA-2 (Collection) (SHA-256/224 512/384)
- SHA-3 (Last NIST competition) 2012

Demo fraud exam results

- Birthday Attack

```
Exam Results for the course SSN of the master education SNE
=====================================================

Course:       MSNSSNP6 [Security of Systems and Networks]
Exam date:    Oktober 23 2024
Credits:      06 ECTS
Teacher:      Jaap van Ginkel

Student     First        Last                                Result
=======     =====        ====                                ======
14533812    Josha        van der Heide                       5.4
12774545    Tony         Munzer                              7.3
12326623    Okechukwu    Onwunli                             8.9
12567191    Jannik       Peters                              5.7
14525623    Wouter       Petri                               6.8
12816558    Petr         Pucil                               4.7
```

Hash

- Brute force Attacks
  - Exhaustive search
- Collision Attacks
  - Find *m1* and *m2* where *hash(m1) = hash(m2)*
- Preimage Attacks
  - Find *m* for *hash(m) = h*
- Second Preimage Attacks
  - Find *m2* for given m1 where *hash(m2) = hash(m1)*

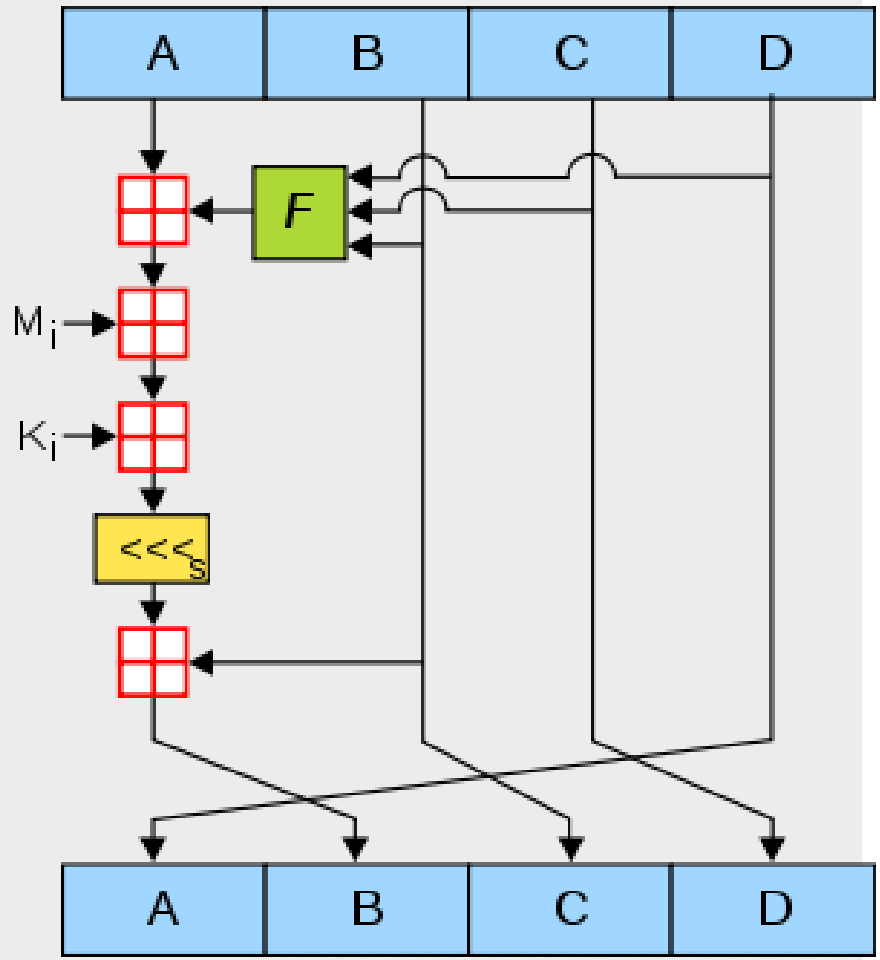
MD5

- 128 bit Hash
- Broken since at least 2005
- Still used a lot :-(

MD5 Algorithm

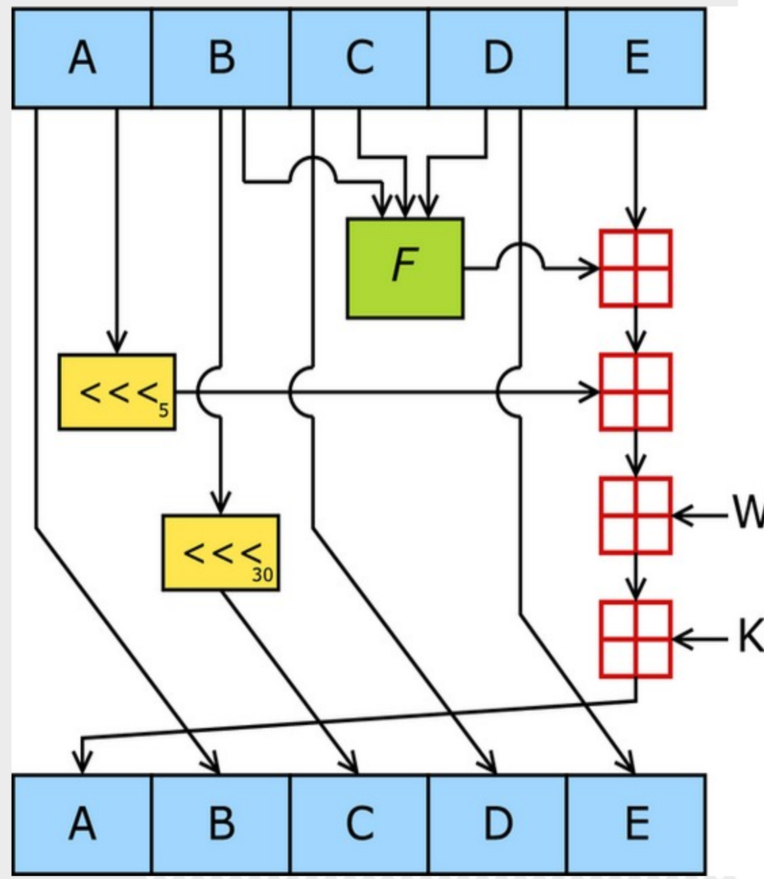
- 128 bit hash
- 512 bit block processing
- Padding with 1 then 0
- 64 Rounds in 4 groups
- Mi is Message block
- Ki is Constant
- F is nonlinear function

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

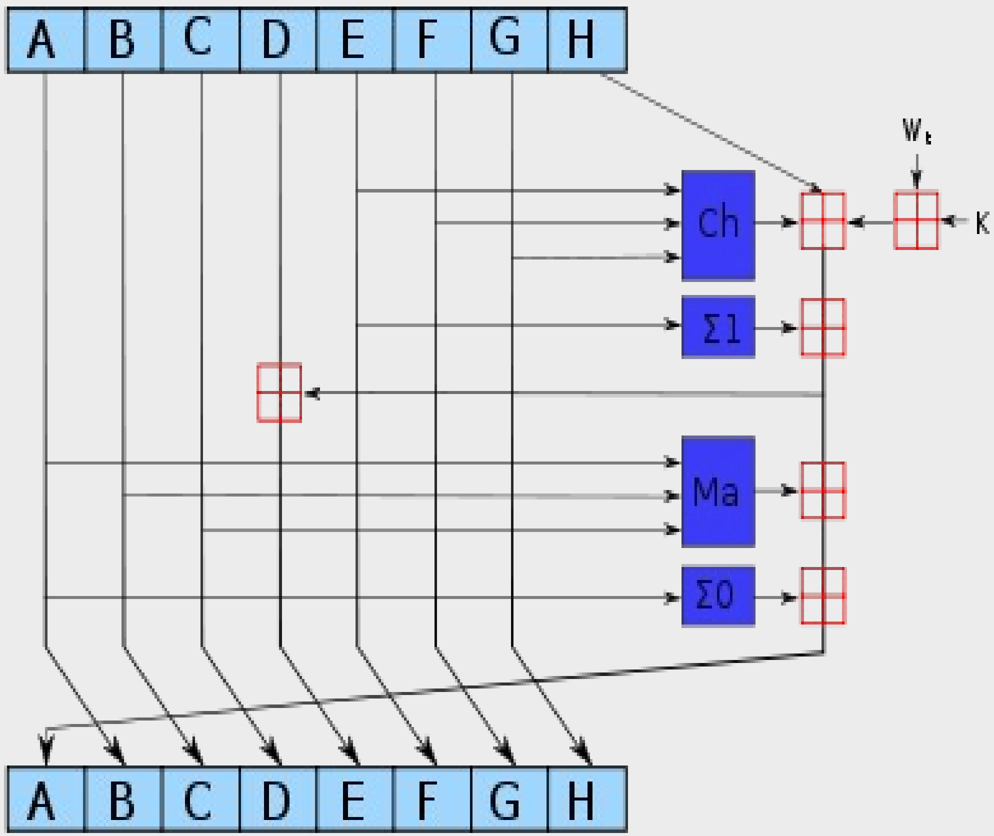


SHA

- Secure Hash Algorithm
- 1993 NIST FIPS
- SHA-0/SHA-1 Similar to MD5
- 160 bit
- Lots of research
- From 2^80 to 2^69
- Move to SHA-2
  - 256 and 512 bit
- SHA-3 challenge



SHA-2



SHA-3

- BLAKE
- Blue Midnight Wish
- CubeHash (Bernstein)
- ECHO (France Telecom)
- Fugue (IBM)
- Grøstl (Knudsen et al.)
- Hamsi
- JH
- Keccak (Keccak team, Daemen et al.)
- Luffa
- Shabal
- SHAvite-3
- SIMD
- Skein (Schneier et al.)

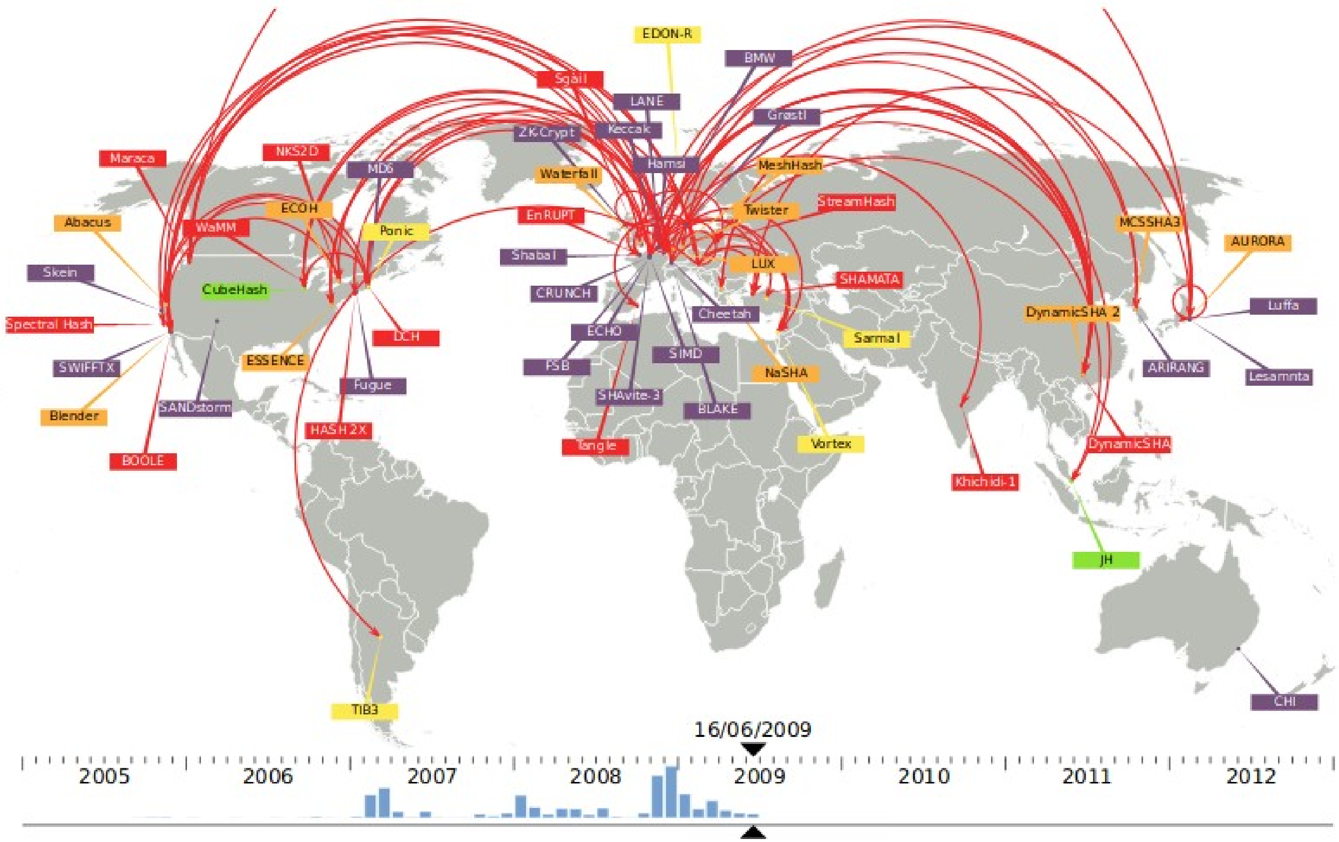
SHA-3 History

- Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche
- Based on RadioGatún, a successor of PANAMA from 1998
- Presented at the NIST Hash Workshop (SHA-3) in 2006
- End of 2008 52 candidates selected
- July 2009, 14 algorithms were selected for the second round. Keccak advanced to the last round in December 2010
- October 2, 2012, Keccak won competition (adapted)
- In 2014, the NIST has published a draft FIPS 202 "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions"
- August 5, 2015 NIST announced that SHA-3 had become a hashing standard.

HMAC

- Keyed-hash message authentication code
- MAC + Encryption
- HMAC-MD5
- HMAC-SHA-1
- Cryptool demo

NIST SHA-3: the battlefield



[courtesy of Christophe De Cannière]

Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) against collision attacks	Capacity against length extension attacks	Performance on Skylake (median cpb)[55]		First published
									long messages	8 bytes	
MD5 (as reference)		128	128 (4 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or	≤18 (collisions found)[56]	0	4.99	55.00	1992
SHA-0		160	160 (5 × 32)	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993
SHA-1							<63 (collisions found[57])		3.47	52.00	1995
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	32 0	7.62 7.63	84.50 85.25	2004 2001
	SHA-384 *SHA-512*	384 512	512 (8 × 64)	1024	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256	128 (≤ 384) 0	5.12 5.06	135.75 135.50	2001
	SHA-512/224 *SHA-512/256*	224 256					112 128	288 256	≈ SHA-384	≈ SHA-384	2012
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	24[58]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024	8.12 8.59 11.06 15.88	154.25 155.50 164.00 164.00	2015
	SHAKE128 *SHAKE256*	*d* (arbitrary) *d* (arbitrary)		1344 1088			min(*d*/2, 128) min(*d*/2, 256)	256 512	7.08 8.59	155.25 155.50	