Homework 2 Posted

- Due Friday, February 17th at the beginning of class.
- Topics
  - Pseudorandom Permutations
  - (Weak) Pseudorandom Functions
  - MACs
  - Hashing

Cryptography
CS 555

Topic 12: Cryptographic Hash Functions

Recap

- Authenticated Encryption
- Encrypt then Authenticate

$$\mathrm{Enc}_K(m) = \left\langle \mathrm{c}, \mathrm{Mac}'_{K_M}(\mathrm{c}) \right\rangle \text{ where } \mathrm{c} = \mathrm{Enc}'_{K_E}(m)$$

Today's Goals:

- Cryptographic Hash Functions
- Merkle-Damgård Transform

Hash Functions

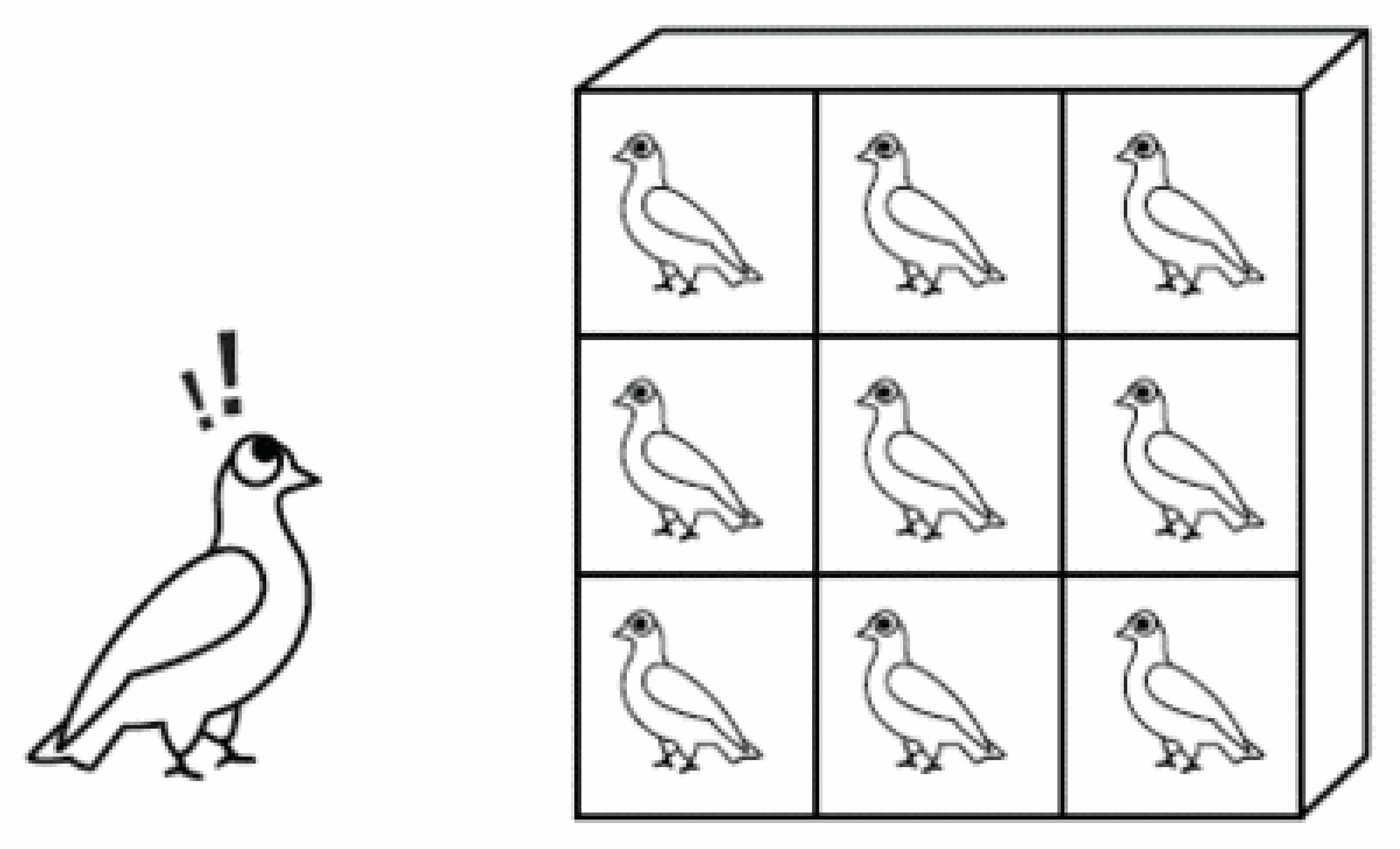
$$H(x)=y$$

Long Input: x

Short Output: y

Pigeonhole Principle

“You cannot fit 10 pigeons into 9 pigeonholes”



Hash Collisions

By Pigeonhole Principle there must exist x and y s.t.

$$H(x) = H(y)$$

Classical Hash Function Applications

- Hash Tables
  - O(1) lookup*
- “Good hash function” should yield “few collisions”

* Certain terms and conditions apply

Collision-Resistant Hash Function

Intuition: Hard for computationally bounded attacker to find x,y s.t. H(x) = H(y)

How to formalize this intuition?

- **Attempt 1:** For all PPT A,

$$\Pr\left[A_{x,y}(1^n) = (x, y)\ s.t\ H(x) = H(y)\right] \leq negl(n)$$

- **The Problem:** Let x,y be given s.t. H(x)=H(y)

$$A_{x,y}(1^n) = (x, y)$$

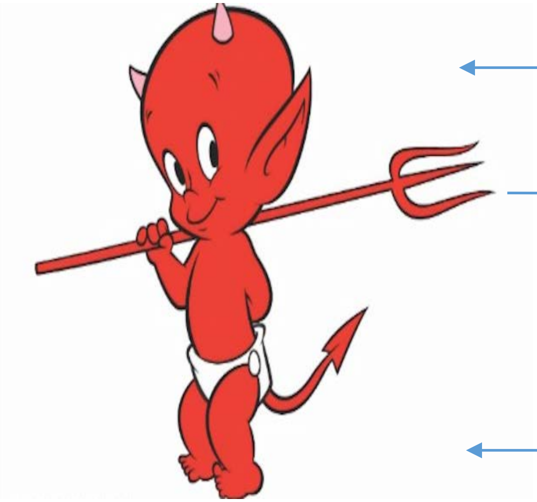
- We are assuming that |x| > |H(x)|. Why?
  - H(x)=x is perfectly collision resistant! (but with no compression)

Keyed Hash Function Syntax

- Two Algorithms
  - $\mathrm{Gen}(1^n; R)$ (Key-generation algorithm)
    - Input: Random Bits R
    - Output: ~~Secret~~ key s
  - $H^s(m)$ (Hashing Algorithm)
    - Input: key s and message $\mathrm{m} \in \{0,1\}^*$ (unbounded length)
    - Output: hash value $H^s(m) \in \{0,1\}^{\ell(n)}$

- Fixed length hash function
  - $m \in \{0,1\}^{\ell'(n)}$ with $\ell'(n) > \ell(n)$

Collision Experiment ($HashColl_{A,\Pi}(n)$)



s

x_1,x_2

$$HashColl_{A,\Pi}(n) = \begin{cases} 1 & if\ H^s(x_1) = H^s(x_2) \\ 0 & otherwise \end{cases}$$

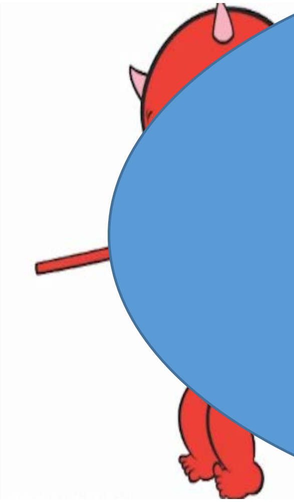
$\mathrm{s} = \mathrm{Gen}(1^n; R)$

Definition: (Gen,H) is a collision resistant hash function if

$$\forall PPT\ A\ \exists \mu\ (\text{negligible})\ \text{s.t}$$

$$\Pr\left[HashColl_{A,\Pi}(n)=1\right] \leq \mu(n)$$

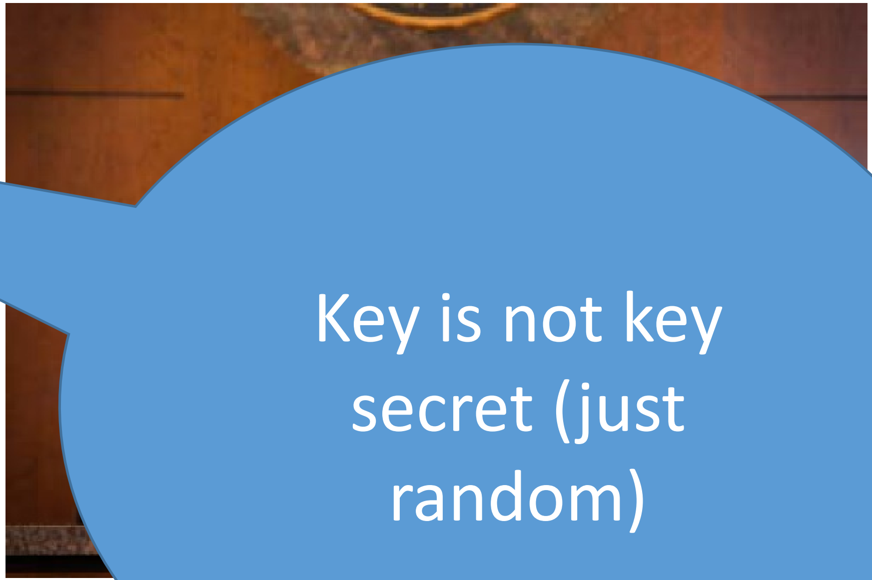
Collision Experiment ($HashColl_{A,\Pi}(n)$)



For simplicity we will sometimes just say that H (or H^s) is a collision resistant hash function

$= H^s(x_2)$

ise



Key is not key secret (just random)

Definition: (Gen,H) is a collision resistant hash function if

$$\forall PPT\ A\ \exists \mu \text{ (negligible) s.t}$$

$$\Pr\left[HashColl_{A,\Pi}(n)=1\right] \le \mu(n)$$

Theory vs Practice

- Most cryptographic hash functions used in practice are un-keyed
  - Examples: MD5, SHA1, SHA2, SHA3
- Tricky to formally define collision resistance for keyless hash function
  - There is a PPT algorithm to find collisions
  - We just usually can't find this algorithm ☺

Formalizing Human Ignorance:
Collision-Resistant Hashing without the Keys

Phillip Rogaway

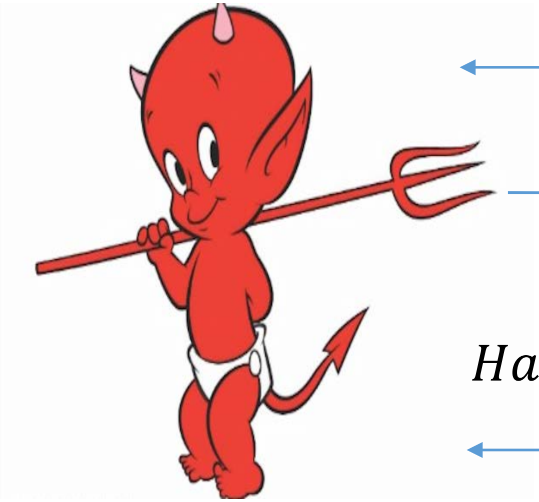
Department of Computer Science, University of California,
Davis, California 95616, USA, and
Department of Computer Science, Faculty of Science,
Chiang Mai University, Chiang Mai 50200, Thailand
rogaway@cs.ucdavis.edu

31 January 2007

Abstract. There is a foundational problem involving collision-resistant hash-functions: com-

Weaker Requirements for Cryptographic Hash

- Target-Collision Resistance



s,x

x'

$$HashTgtColl_{A,\Pi}(n) = \begin{cases} 1 & if\ H^s(x') = H^s(x) \\ 0 & otherwise \end{cases}$$

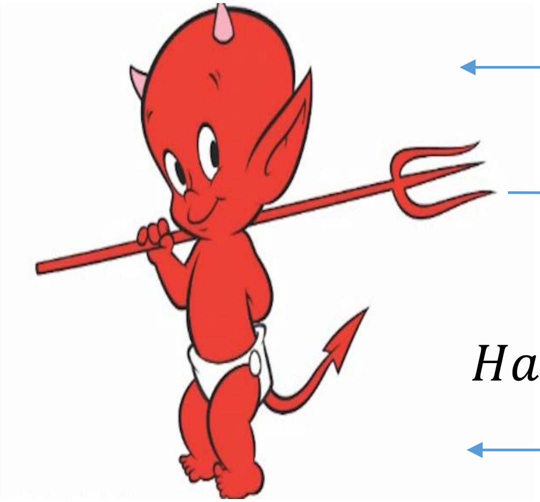
$s = \mathrm{Gen}(1^n; R)$

$x \in \{0,1\}^n$

Question: Why is collision resistance stronger?

Weaker Requirements for Cryptographic Hash

- Preimage Resistance (One-Wayness)



s, y

x

$$HashPreImgRes_{A,\Pi}(n) = \begin{cases} 1 & if\ H^s(x) = y \\ 0 & otherwise \end{cases}$$

$\mathrm{s} = \mathrm{Gen}(1^n; R)$

$y \in \{0,1\}^{\ell(n)}$

Question: Why is collision resistance stronger?

Merkle-Damgård Transform

- Most cryptographic hash functions accept fixed length inputs
- What if we want to hash arbitrary length strings?

Construction: (Gen,h) fixed length hash function from 2n bits to n bits

$$H^s(x_1, \dots, xd) = h^s\left(h^s\left(h^s\left(\dots h^s(0^n \parallel x_1)\right) \parallel x_{d-1}\right) \parallel x_d\right)$$

Merkle-Damgård Transform

Construction: (Gen,h) fixed length hash function from 2n bits to n bits

$H^s(x)$ =

1. Break x into n bit segments $x_1,..,x_d$ (pad last block by zeros if needed)
2. $z_0 = 0^n$ (initialization)
3. For i = 1 to d+1
    1. $z_i = h^s(z_{i-1} \parallel x_\mathrm{i})$
4. Output z_{d+1}

Merkle-Damgård Transform

Theorem: If (Gen,h) is collision resistant then so is (Gen,H)

Proof: Show that any collision in H^s yields a collision in h^s. Thus a PPT attacker for (Gen,H) can be transformed into PPT attacker for (Gen,h).

Suppose that

$$H^s(x) = H^s(x')$$

(note x and x' may have different lengths)

Merkle-Damgård Transform

Theorem: If (Gen,h) is collision resistant then so is (Gen,H)

Proof: Suppose that

$$H^s(x) = H^s(x')$$

Case 1: |x|=|x'| (proof for case two is similar)

$$H^s(x) = z_{d+1} = h^s(z_d \parallel x_d) = H^s(x') = z'_{d+1} = h^s(z'_d \parallel x'_d)$$

$$z_d \parallel x_d =? \, z'_d \parallel x'_d$$

No → Found collision

Yes?

$$h^s(z_{d-1} \parallel x_{d-1}) = h^s(z'_{d-1} \parallel x'_{d-1})$$

Merkle-Damgård Transform

Theorem: If (Gen,h) is collision resistant then so is (Gen,H)

Proof: Suppose that

$$H^s(x) = H^s(x')$$

Case 1: |x|=|x'| (proof for case two is similar)

If for some i we have $z_i \parallel x_i \neq z_i' \parallel x_i'$ then we will find a collision

But x and x' are different!

Next Class

- Read Katz and Lindell 5.3-5.4 + A.4
- Appendix A.4 (“Birthday Problem”)
- HMACs + Generic Attacks on Hash Functions

- Work on Homework 2 ☺