Administrivia

- PSI out today, homework groups
- Term project ideas
  - slashdot ("security")
  - www.iacr.org/eprint

Outline

Hash functions
  - Intro
  - Random Oracle Model
  - Desirable Properties
  - Applications

Introduction

What is a hash fn?
Maps arbitrary strings of data to fixed-length output in deterministic, public, "random" manner.

\[ h : \{0,1\}^* \rightarrow \{0,1\}^d \]

Strings of arbitrary length \( \geq 0 \)
Strings of length \( d \)
Hash Functions

No secret key. All operations public.
Anyone can compute \( h \), poly time computation.

Examples:
- \text{MD4}, \text{MD5}, \text{SHA-1}, \text{SHA-256}, \text{SHA-512}
- \text{d}: 128, 160, 256, 512
- broken (CR): \( 2^6 \), \( 2^{37} \), \( 2^{69} \)

Ideal: Random Oracle

(not achievable in practice)

Oracle:
- on input \( x \in \{0, 1\}^* \)
- if \( x \) not in book
  - flip coin \( d \) times to determine \( h(x) \)
  - record \((x, h(x))\) in book
- else: return \( y \) where \((x, y)\) \in book

Gives random answer every time, except as required for consistency with previous answers. (\( h \) must be deterministic)

In practice, \( \# RO \) so need something "pseudo random"
Desirable Properties

OW 1 "one-way" (pre-image resistance)
Infeasible, given \( y \in \{0, 1\}^d \), to find any \( x \) s.t. \( h(x) = y \)

CR 2 Collision-resistance (strong collision resistance)
Infeasible to find \( x, x' \), s.t. \( x \neq x' \) and \( h(x) = h(x') \) (a "collision")

TCR 3 Weak collision resistance (target CR, and pre-image resistance)
Infeasible, given \( x \), to find \( x' = x \)
s.t. \( h(x) = h(x') \)

PRF 4 Pseudo-randomness
Behavior indistinguishable from RO

NM 5 Non-malleability
Infeasible, given \( h(x) \), to produce \( h(x') \) where \( x \) and \( x' \) are "related"
(e.g., \( x' = x + 1 \))

Informal definitions. Formal requires family of hash functions
Facts

- \( h \uparrow \downarrow CR \Rightarrow h \text{ is TCR} \) (but not reverse)
- \( h \uparrow \downarrow OW \iff h \text{ is CR, TCR} \) (neither impl. holds)
- Collisions can be found in \( O(2^{d/2}) \) - birthday attack
- Inversion can be found in \( O(2^d) \)

Examples

\[ h(x) \text{ is OW, CR} \]

\[ h'(a, b, x_2, \ldots x_n) \text{ is still OW, but not TCR} \]

\[ OW \Rightarrow TCR \]

\[ h'(x) = \begin{cases} 0 & \text{if } |x| \leq n \\ 1 & \text{if } h(x) \text{ otherwise} \end{cases} \]

\[ h \text{ is OW, CR, but } h' \text{ is TCR, not OW} \]

\[ TCR \not\Rightarrow OW \]
Applications

1. **Password storage**
   - Store $h(pw)$, not $pw$, on computer.
   - Use $h(pw)$ to compare against $h(pw')$ where $pw'$ is the typed password.
   - Disclosure of $h(pw)$ should not reveal $pw$.
   - Need OW.

2. **File modification detector**
   - For each file $F$, store $h(F)$ securely (on DVD).
   - Check if $F$ modified by recomputing $h(F)$.
   - Need TCR (adversary wants to change $F$ but not $h(F)$).

3. **Digital signatures**
   - $PK_A$: Alice's Public key
   - $SK_A$: Alice's Private key

   **Signing**: $\sigma = \text{sign}(SK_A, M)$
   **Verify**: $\text{verify}(M, \sigma, PK_A) = \text{true}/false$

   Adversary wants to forge a signature that verifies.

   For large $M$, easier to $\text{sign} h(M)$, $\sigma = \text{sign}(SK_A, h(M))$.

   Need CR, don't need OW. Alice gets Bob to sign $x$, then claims he signed $x'$, if $h(x) = h(x')$. 