Math 314: Class Note

19/11/2024

How can we sign messages that have multiple blocks?

Idea1: sing every block separately (like ECB for encryption)

- Computationally intensive or more responsibility to attack
- Selectively delete or reorder the blocks
- Blocks could have different sizes the blocks
- More data (every block has to include a signature too)

Goal: sign an entire message (multiple blocks all the time)

still need the signature to be connected to the entire message.

Hash Functions

A function that takes as input arbitrarily long inputs and produces much shorter outputs called digests.

Optimal properties of cryptographic have functions

1. Quick to compute
2. Produce relatively small digest (but not too small)
3. Preimage resistance (one-way ness)

If someone gives you a digest it should be hard to find an input that produces that digest.

Solving $h(x) = y$ for x given y is hard

4. Second preimage -Resistance (or weakly collision resistance)

   Given $h(x) = y$

   It should be hard to find a different x_2 with $=y$

Any time that $h(x) = h(x_2)$ with $x_1 \neq x_2$

We have a Collison

Collisions are “bad” but impossible to avoid (pigeonhole principle).

Goals make collisions hard to find.

5. Strong collision Resistance

It should be hard to find only two inputs that produce the same digest $h(x_1) = h(x_2)$

One method to create hashes is to use a block cipher (like AES)

$E_k(x)$ <- Block a cipher with input x and key k

Hash an input x_1 , x_2, …. x_n

Fix H_0= call zeros or some fixed values

$H_i = H_{i-1} + E_k(H_{i-1})$, E_k -> blocks of input are the keys

How long should digest be?

Long enough that we never encounter a collision by “accident”

What is the probability that two people have the same birthday?

The probability that two people have different birthdays (1-1/365)

What is the probability that 3 people have di0?

We need person 1 to have different birthday that person two and person 3 to have different birthdays than person 1 and person2.

Multiply

(1-1/365) (1-2/365) -> probability that person 3 birthday is different from 1 and 2.

(1-1/365) -> probability person 1 and person 3 have different birthdays.

The probability that k people have different birthday is (1-1/365) (1- 2/365) ….1-k-1/365)