Tutorial -5

SOEN-321

Cryptographic hash function

Hash function is a mathematical function that takes an arbitrary size input, and outputs a fixed size value.

Cryptographic hash function must satisfy the following:

1- Pre-image resistance:

Given a hash value y, it is hard to find a message x such that $y = \mathrm{H}(x)$.

2-Weak collision resistant

Given a message x_1, it is hard to find a message $x_2 \neq x_1$ such that $\mathrm{H}(\mathrm{x}_1) = \mathrm{H}(x\_2)$.

3-Strong collision resistant

It is hard to find any different pair x_1, x_2 such that $H(x_1) = H(x\_2)$

Problem 1

Bob is a paranoid cryptographer who does not trust dedicated hash functions such as SHA1 and SHA-2. Bob decided to build his own hash function based on some ideas from number theory. More precisely, Bob decided to use the following hash function:

H(m)= m^2 mod n,   n= p × q, where p and q are two large distinct primes.

Does this hash function satisfy the one-wayness property? What about collision resistance? Explain.

1- Pre-image resistant:

Yes, since p and q are secret, then finding the square root $mod\ n$ is a hard problem

2-Weak collision resistant

No, since for any given input m, the attacker can get the same hash value using input $-m$

3-Strong collision resistant

No, it is easy to choose any pair $(m, -m)$ which yields the same hash

Shamir Secret Sharing

Company ABC needs to secure their vault's passcode. They could use encryption to protect the passcode.

Problem:

What if the holder of the decryption key is unavailable or dies?

What if the decryption key is compromised via a malicious hacker?

What if the holder of the decryption key turns rogue, and uses their power over the vault to their benefit?

Solution:

Utilize secret sharing scheme which has two phases:

1. A dealer distributes shares to n participants, and destroys the secret
2. Any t shares can be used to reconstruct the secret

Properties:

Less than t shares, participants can’t reconstruct the secret

Shares don’t provide any information about the secret

Shamir Secret Sharing

Polynomials Fact:

- 2 points are sufficient to define a line (Linear polynomial)
- 3 points to define a parabola (2^{nd} degree polynomial)
- t points to define t-1 degree polynomial

For (t,n) secret sharing scheme to share a secret s

1. Choose a prime p such that $0 < t < n < p$ and $s < p$
2. Choose $t - 1$ random coefficients $a_1, \ldots, a_{t-1} < p$ and set $a_0 = s$
3. Build a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \, mod \, p$
4. Generate n shares $\left(i, f(i)\right) \, for \, i = 1, \ldots, n$

To reconstruct the secret a_0 from t shares, solve a system of t equations

Problem 2

Consider a (4,3) Shamir secret sharing scheme with p=17. Show how the secret can be recovered from the following shares: (1,10), (2,16), and (3,2).

Polynomial degree: 3 – 1 = 2

$$f(x) = a_0 + a_1 x + a_2 x^2 \ mod\ 17$$

Where a_0 is the secret

From the shares we can form 3 equations:

(x=1, f(1)=10): $10 = a_0 + a_1 + a_2 \ mod\ 17$ (1)

(x=2, f(2)=16): $16 = a_0 + 2a_1 + 4a_2 \ mod\ 17$ (2)

(x=3, f(3)=2): $2 = a_0 + 3a_1 + 9a_2 \ mod\ 17$ (3)

Solve for 3 unknowns:

(1)+(3)-(2)*2: $-20 = 2a_2 \ mod\ 17 = 14$

Substitute $2a_2$ in 2*(1) and (2):

2*(1) $20 = 2a_0 + 2a_1 + 2a_2 \ mod\ 17$

$20 = 2a_0 + 2a_1 + 14 \ mod\ 17$

$6 = 2a_0 + 2a_1 \ mod\ 17$ (a)

(2) $16 = a_0 + 2a_1 + 4a_2 \ mod\ 17$

$16 = a_0 + 2a_1 + 2 \times 14 \ mod\ 17$

$16 = a_0 + 2a_1 + 28 \ mod\ 17$

$16 = a_0 + 2a_1 + 11 \ mod\ 17$

$5 = a_0 + 2a_1 \ mod\ 17$ (b)

(a)-(b): $1 = a_0 \ mod\ 17$