Tutorial -5.1

SOEN-321

Shamir Secret Sharing Scheme (Set 5)

Example:

- Share a treasure map between two people who don't quite trust each other. Split the map and make sure both pieces are needed to find the treasure. Give each person half of the map.
- Generalization
  - Given a secret, s, would like n parties to share the secret so that the following properties hold:
    - 1. All n parties can get together and recover s
    - 2. Less than n parties cannot recover s
  - Map example, s is the map and the people are the parties that share the secret.
  - Split the secret into n pieces, s1, s2, ... sn and give a piece to each party
  - Special case of secret sharing called secret splitting

Shamir Secret Sharing Scheme

(m,n) Threshold Scheme

- A secret is divided into “n” pieces (called the shadows), such that combining any “m” of the shadows will reconstruct the original secret.
- Choose a (public) large polynomial “p” bigger than:
  - The possible number of shadows (n)
  - The size of the secret
  - Other requirements for strength
  - All arithmetic will be “mod p”
- Generate an arbitrary polynomial of degree “m-1”
- Evaluate the polynomial at “n” different points to obtain the shadows “ki”
- Distribute the shadows and destroy M and all the polynomial coefficients

Example

(n,3) Threshold scheme:

Form of our arbitrary polynomial m=3 so polynomial is degree 2

$$F(x) = ax^2 + bx + M \ mod \ p$$

We must decide on a size for n - this is the number of shadows. The number of shadows is independent of the size of the polynomial

Example

- Suppose we want a (5,3) scheme - that means we will have 5 shadows - for hiding message “11” (eleven)
- We choose a prime > 5, 11: say 13 Our polynomial must be degree 2.
- We select the coefficients a, b randomly: F(x) = 7x2 + 8x + 11 (mod 13)
- We must now generate five shadows. We decide to evaluate at points 1,2,3,4,5 (normally we’d mix them up!)
  - F(x) = 7x2 + 8x + 11 (mod 13)
    - k1 = F(x1=1) = 7+8+11 = 0
    - k2 = F(x2=2) = … = 3
    - k3 = F(x3=3) = … = 7
    - k4 = F(x4=4) = … = 12
    - k5 = F(x5=5) = … = 5

Exercise 4 - 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

$k = a_0 + a_1 x + a_2 x^2 \ mod\ 17$

Where a0 is the secret

From the shares we can form 3 equations:

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

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

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

Solve for 3 unknowns:

3 * (1) – (3): $28 = 2a_0 - 6a_2 \ mod\ 17$ (a)

2 * (1) – (2): $4 = a_0 - 2a_2 \ mod\ 17$ (b)

3 * (b) – (a): $-16 = a_0 \ mod\ 17$

$a_0 = 1 \ mod\ 17$