# Tutorial -7

SOEN-321

# 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 (2nd 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 $a_1, \dots, a_{t-1} < p$ 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 $\big(i, f(i)\big) \, for \, i = 1, \dots, n$

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

# Exercise 4-2

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): $1 = a_0 \; mod \; 17$

# Exercise 5-2

Suppose Bob has an RSA Cryptosystem with a large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (i.e., A<->0, B<->1, etc.), and then encrypting each residue modulo n as a separate plaintext character.

Describe how Eve can easily decrypt a message which is encrypted in this way.

Eve can construct a lookup table for all the valid 26 ciphertexts by encrypting the letters, A to Z using Bob's public key.

Then Eve can use this table (or more precisely the inverse of this table) to decrypt any ciphertext encrypted by Alice

| $m$ | $c = m^e \bmod n$ |
|---|---|
| $A = 0$ | $c = 0$ |
| $B = 1$ | $c = 1$ |
| … | … |
| $Z = 25$ | … |

# Exercise 5-3

Determine the problems in the following protocol in which A wants to establish a shared session key with B using the help of a trusted authority S

A→S: A, B

S→A: $K_{AB}$

A→B: A, $K_{AB}$

The key ($K_{AB}$) is sent in the clear. Therefore, the attacker can also see the key and decrypt the corresponding ciphertexts.

# Exercise 5-4

Consider the following authentication protocol

$A \rightarrow B: TA, Sig_A(TA,B)$

(i) What is the objective of the time stamp TA?

The timestamp ensures the freshness of the signature and prevents replay attacks. If there is no timestamp in the signature, the attacker can use a previously signed message.

# Problem-4 –Ex5

Consider the following authentication protocol

$A \rightarrow B: TA, Sig_A(TA,B)$

(ii)After this protocols is executed

(a) B is authenticated to A

(b) A is authenticated to B

(c) Both A and B are authenticated to each other

The answer is (b)