Assignment 3

Computer Security - 1

Q1) Explain briefly why we need to involve a secure one-way hash function in generating digital signatures.

Ans) The use of one-way hash function in the digital signature is it allows us to provide authentication, non-repudiation and integrity to a particular document. A fundamental characteristics of hashing algorithms is that 2 different messages will not have the exact same hash values, that means a single change in the message will produce a different hashing output. The message is then digitally signed and transmitted to the recipient. The recipient then creates their own hash of the message and uses the senders public key to decrypt the sender's hash. Then the receiver checks his hash with the sender's one, if match found then the sender is verified.

Q2) Assume that there are 3 users want to establish a secret sharing with the threshold t=2 without the assistance of a mutually trusted party. Briefly explain how to set up to meet the requirement.

Ans) After each user selects a sub secret, the master selects the sub secret chosen by three users. Each user will act as a leader to create shells for other users, using (2,2) Samir's secret sharing key approach.

Keys/Users	A	B	C
Ka		Ka,b	Ka,c
Kb	Kb,a		Kb,c
Kc	Kc,a	Kc,b	

Shares based on a system of thresholds (2,2)

By working together, A and B can know the Ka and Kb. They can also reconstruct the kc from kc,a and kc,b.

Q3) Describe how an intelligent criminal can use Clipper chip to avoid being wiretapped.

Ans) The Clipper Chip is based on the NSA's "Skipjack" encryption algorithm, which was developed in the 1980s. Skipjack was secure enough on its own to be classified as a "Type 1" NSA product, suitable for government and military use in sensitive communications. It was equipped with the CAPSTONE chip, which handled all cryptographic processing. All telecommunications companies in the United States were supposed to use the clipper chip to provide encryption, preventing outside eavesdropping. There was, however, a back door; the government held the decryption key, and anyone legally authorized could gain access to it and decrypt all messages.

Q4) (a) What is the purpose of getting a digital certificate?

Ans) The digital certificates are electronic credentials issued by the trusted third party. The main purpose of the digital certificates are it verifies the identity of the user and also verifies that the owner owns the public key.

Q4 b) List 5 items containing in a X.509 digital certificate.

Ans) The below are some of the fields available in the digital certificate

i) Version - Tells about the version of the certificate.

ii) serial number - Unique serial number given by the certificate authority after generating a certificate for the user.

iii) Algorithm information - Tells about the algorithm used to generate the signature.

iv) Issuer name - Name of the CA issuing the certificate.

v) Validity period - period of validity of the certificate.

Q5) Give 2 reasons that a digital certificate may be revoked before it expires. Ans) If any certificate seems to be unsecure or not trusted then that certificate will be revoked by the Certificate Authority. In addition to it there are some more reasons to revoke a certificate before it expires.

In them 2 of the reasons are

i) The user's secret key is assumed to be compromised.

ii) The user is no longer certified by this Certificate Authority.

Q6) In (3, 5) secret sharing scheme, the dealer selects K=15, h(x)=5x2+6x+15 mod 19. (a) What are the shadows for x=1, 2, 3, 4, 5?

6) In (3,5) Secret sharing scheme the dealer selects

$K = 15$, $h(x) = 5x^2 + 6x + 15 \bmod 19$

a) what are the shadows for $x = 1, 2, 3, 4, 5$

Given $h(x) = 5x^2 + 6x + 15$

$K_1 = h(1) = (5(1)^2 + 6(1) + 15) \bmod 19$

$= 26 \bmod 19 \Rightarrow 7$

$K_2 = h(2) = (5(2)^2 + 6(2) + 15) \bmod 19$

$= 47 \bmod 19 \Rightarrow 9$

$K_3 = h(3) = (5(3)^2 + 6(3) + 15) \bmod 19$

$= 78 \bmod 19 \Rightarrow 2$

$K_4 = h(4) = (5(4)^2 + 6(4) + 15) \bmod 19$

$= 119 \bmod 19 \Rightarrow 5$

$K_5 = h(5) = (5(5)^2 + 6(5) + 15) \bmod 19$

$= 170 \bmod 19 \Rightarrow 18$

$\therefore$ the shadows for $x = 1, 2, 3, 4, 5$ are

$$\boxed{7, 9, 2, 5, 18}$$

Q6) b) Show how 3 shadow holders with x-=1, 3 and 5 can construct the master secret, K.

b) Show how 3 shadows holders with x: 1, 3, 5 Can Construct the master key 'K'

1) we Can reConstruct the h(x) using three shadows

$$h(x) = \left[7\frac{(x-3)(x-5)}{(1-3)(1-5)} + 2\frac{(x-1)(x-5)}{(3-1)(3-5)} + 18\frac{(x-1)(x-3)}{(5-1)(5-3)}\right] \bmod 19$$

$$= \left[7\frac{(x-3)(x-5)}{(-2)(-4)} + 2\frac{(x-1)(x-5)}{2(-2)} + 18\frac{(x-1)(x-3)}{(4)(2)}\right] \bmod 19$$

$$= [7*\text{inv}(8,19)(x-3)(x-5) + 2*\text{inv}(-4,19)(x-1)(x-5) + 18*\text{inv}(8,19)(x-1)(x-3)] \bmod 19$$

$$= [7*12(x-3)(x-5) + 2*15(x-1)(x-5) + 18*12(x-1)(x-3)] \bmod 19$$

$$= 8[8(x-3)(x-5) + 9(x-1)(x-5) + 7(x-1)(x-3)] \bmod 19$$

$$= 8[8x^2 - 64x + 120 + 9x^2 - 54x + 45 + 7x^2 - 28x + 21] \bmod 19$$

$$= (24x^2 - 146x + 186) \bmod 19$$

$$= 5x^2 + 6x + 15$$

$$\therefore \boxed{K = 15}$$

Q7) (a) A dealer is responsible to break a master secret, K, to 5 users according to a (3, 5) threshold scheme. The public modulus is p=23. Suppose 3 users with shadows (1, 4), (3, 13) and (5, 9), want to reconstruct the master secret. Give detail procedure to show how they can reconstruct the master secret K.

7a) There are 2 parties, 'Sender' and Reciever. These two initially agree on a large prime number p and non-zero integer 'g'. p and g Could be known Publicly when they transmitted over a unsecure channel 'a' and 'b' are Secretly Selected by Sender and Reciever

$Ke1 = g^a \pmod p$ Calculated by Sender

$Ke2 = g^b \pmod p$ Calculated by reciever

Firstly, the lagrange basis polynomial needs to be calculated. The formula for it is defined as

$$L_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{x - x_0}{x_j - x_0} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

Then, given n points, the interpolated polynomial is a linear Combination of the above basis Polynomials as shown below.

$$f(x) = \sum_{j=0}^{n-1} y_j L_j(x)$$

$(x_0, y_0) = (1, 4)$

$(x_1, y_1) = (3, 13)$

$(x_2, y_2) = (5, 9)$

For $(x_0, y_0) = (1,4)$

$(x_1, y_1) = (2,13)$

$(x_2, y_2) = (4,9)$ basis polynomial becomes

$$L_0 = \frac{(x-x_1)}{(x_0-x_1)} \cdot \frac{(x-x_2)}{(x_0-x_2)} = \frac{(x-2)(x-4)}{(1-2)(1-4)} = \frac{(x-2)(x-4)}{3}$$

$$L_1 = \frac{(x-x_0)}{(x_1-x_0)} \frac{(x-x_2)}{(x_1-x_2)} = \frac{(x-1)(x-4)}{(2-1)(2-4)} = \frac{(x-1)(x-4)}{(-2)}$$

$$L_2 = \frac{(x-x_0)}{(x_2-x_0)} \frac{(x-x_1)}{(x_2-x_1)} = \frac{(x-4)(x-2)}{(4-1)(4-2)} = \frac{(x-1)(x-2)}{6}$$

For us these values differs so, for $(x_0, y_0) = (1,2)$

$(x_1, y_1) = (3,13)$

$(x_2, y_2) = (5,9)$

$$L_0 = \frac{(x-3)(x-5)}{(1-3)(1-5)} = \frac{(x-3)(x-5)}{8}$$

$$L_1 = \frac{(x-1)(x-5)}{2(-2)} = \frac{(x-1)(x-5)}{-4}$$

$$L_2 = \frac{(x-1)(x-3)}{(4)(2)} = \frac{(x-1)(x-3)}{8}$$

Apply to this

$$f(x) = \sum_{j=0}^{2} y_j L_j(x)$$

$$f(x) = \frac{4}{8}(x-3)(x-5) - \frac{13}{4}(x-1)(x-5) + \frac{9}{8}(x-1)(x-3)$$

$$= \frac{4}{8}(x^2-8x+15) - \frac{13}{4}(x^2-6x+5) + \frac{9}{8}(x^2-4x+3)$$

$$= \frac{1}{8}(4x^2-32x+60-26x^2+156x-130+9x^2-36x+27) \mod 23$$

$$= \frac{1}{8}(-13x^2+88x-43) \mod 23$$

$$= \frac{1}{8}(13x^2-88x+43) \mod 23$$

Suppose our secret message was decimal equivalent to 8

Let our random generated a_1 and a_2 with mod 23 are

$$a_1 = -88/23$$

$$a_2 = 13/23$$

generated polynomial from

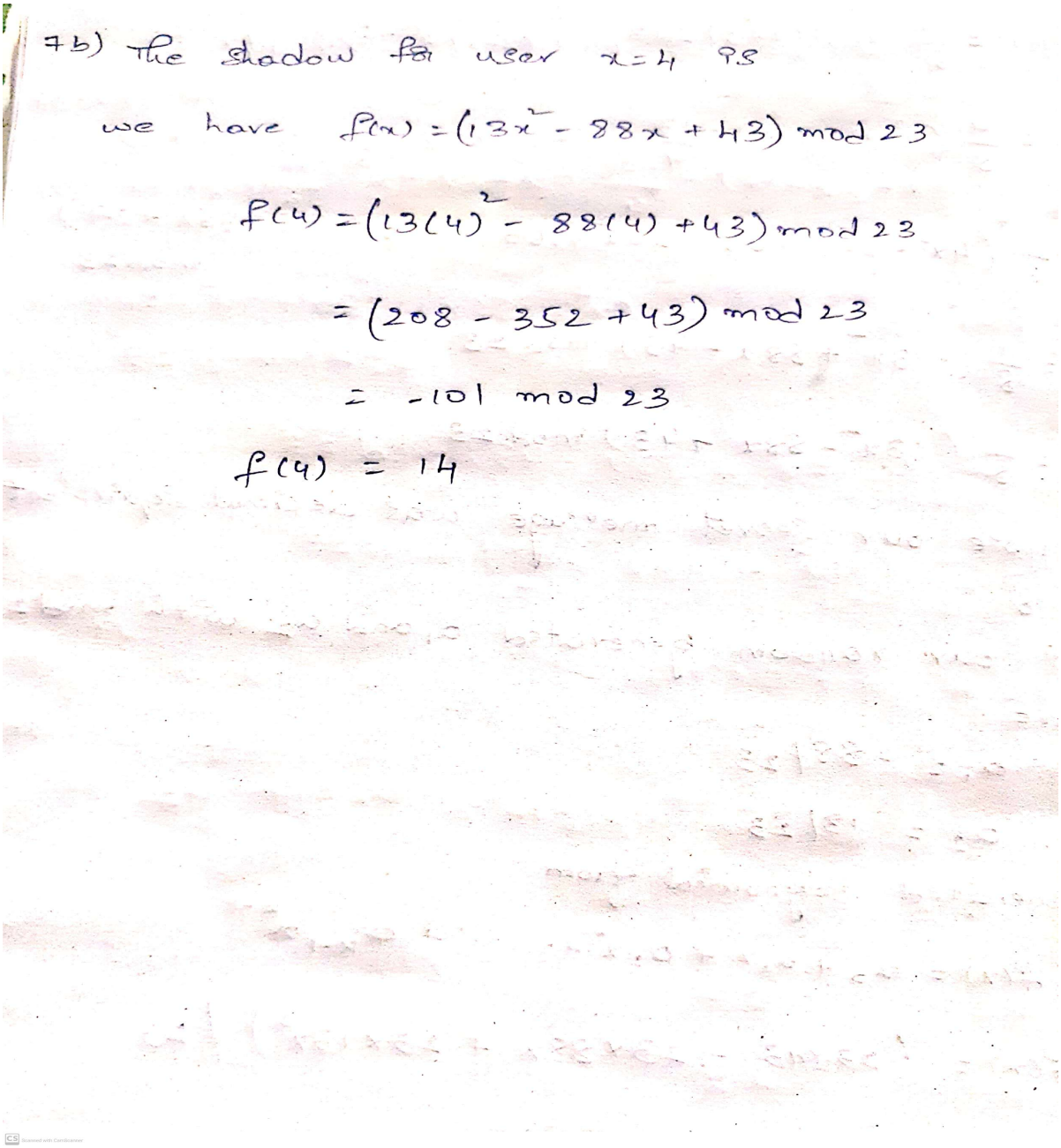
$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$$

$$f(x) = (23\times43 - 23\times88x + 23\times13x^2)/23$$

$$= (13x^2 - 88x + 43) \mod 23$$

$\therefore$ our master secret key is 20 ($\because 43 \mod 23 \Rightarrow 20$)

Q7) (b) What is the shadow of the user with x=4?



7b) The shadow for user $x=4$ is

we have $f(x) = (13x^2 - 88x + 43) \bmod 23$

$f(4) = (13(4)^2 - 88(4) + 43) \bmod 23$

$= (208 - 352 + 43) \bmod 23$

$= -101 \bmod 23$

$f(4) = 14$