1)

A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence. Furthermore, a one-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way.) A good hash function also makes it hard to find two strings that would produce the same hash value. All modern hash algorithms produce hash values of 128 bits and higher. Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect. Since it is computationally infeasible to produce a document that would hash to a given value or find two documents that hash to the same value, a document's hash can serve as a cryptographic equivalent of the document. This makes a one-way hash function a central notion in public-key cryptography. When producing a digital signature for a document, we no longer need to encrypt the entire document with a sender's private key. It is sufficient to encrypt the document's hash value instead. Although a one-way hash function is used mostly for generating digital signatures, it can have other practical applications as well, such as secure password storage, file identification and message authentication code (MAC.)

2)

Each user can select sub secret then the master select the sub secret which is determined by three users
Each user will act as leader to generate shells to other users following (2,2) samir's secret sharing key algorithm

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

Shares based on (2,2) threshold scheme

Later for example, when A, B work together, they know ka, kb . In addition, from kc,a and kc,b, they can reconstruct kc.

3)

The Escrow Encryption Standard is designed to provide users with communications that are secure against decryption by all third parties except authorized agents of the U.S. government. Before a Clipper Chip is installed in a telephone, the government will permanently inscribe it with a unique serial number and a unique encryption key. The government will keep both of these numbers on file. In order to reduce the danger that the file might be stolen or otherwise compromised, the chip's unique encryption key will be split into two pieces, each held by a different "escrow agent." The escrow agents will be required to guard the segments and release them only to persons who can demonstrate they will be used for authorized intercepts. Reuniting the pieces of a chip's unique key gives the government the capability to decrypt any Clipper conversations.

4a)

A digital certificate is like a driving license, passport, or any ID card that authenticates the user or a person from where he came and where he will be. So each organization must have a digital certificate to protect their confidential information about their organization and their employees, so digital certificate encodes the data with SSL 1024, 2048, 4096 RSA key which is super secure to decode the data so any hacker cannot quickly get the information from in between the user and router. The certificate is like a passport, which provides a government agency in which all the countries keep trust. There is the same way certified company providers are a lot more than 20 like Digital Certificate, Verizon, etc. They provide us with a yearly certificate based on each year we have to renew the certificate and install it on an out website where our secured data is stored and where the client comes. The digital certificate provides evidence that the user is genuine and valid, and the certificate they present is digitally signed and acceptable globally to all the sites.

4b)

Many of the certificates that people refer to as Secure Sockets Layer (SSL) certificates are in fact X.509 certificates. The first X.509 certificates were issued in 1988 as part of the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T) and the X.500 Directory Services Standard. In 1993, version 2 added two fields to support directory access control. Version 3 was released in 1996 and defines the formatting used for certificate extensions.

The items containing x509 digital certificates are:

Validity period of the certificate

Subject distinguished name

Subject public key information

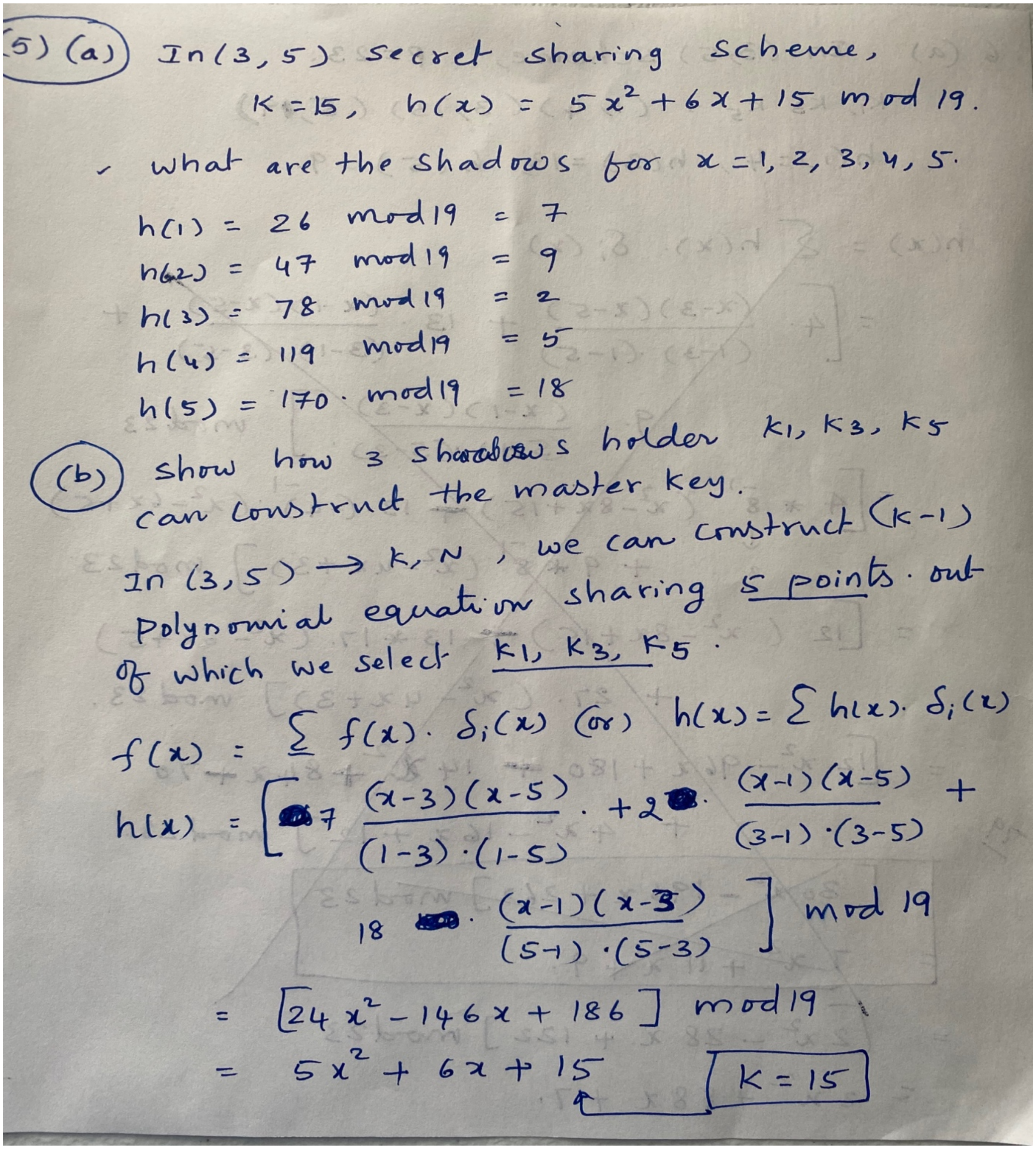
Extensions

The two reasons that a digital certificate may be revoked before it expires are:

Affiliation Changed :- This code is issued if the employee to whom the certificate was issued has left the company.

Superseded :- This code is issued when the information/data of the user changes for example his/her name.

Q 5.



5) (a) In (3, 5) secret sharing scheme,

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

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

$h(1) = 26 \mod 19 = 7$

$h(2) = 47 \mod 19 = 9$

$h(3) = 78 \mod 19 = 2$

$h(4) = 119 \mod 19 = 5$

$h(5) = 170 \cdot \mod 19 = 18$

(b) show how 3 shadows holder K_1, K_3, K_5 can construct the master key.

In $(3, 5) \rightarrow k, N$, we can construct $(k-1)$ Polynomial equation sharing 5 points. out of which we select K_1, K_3, K_5.

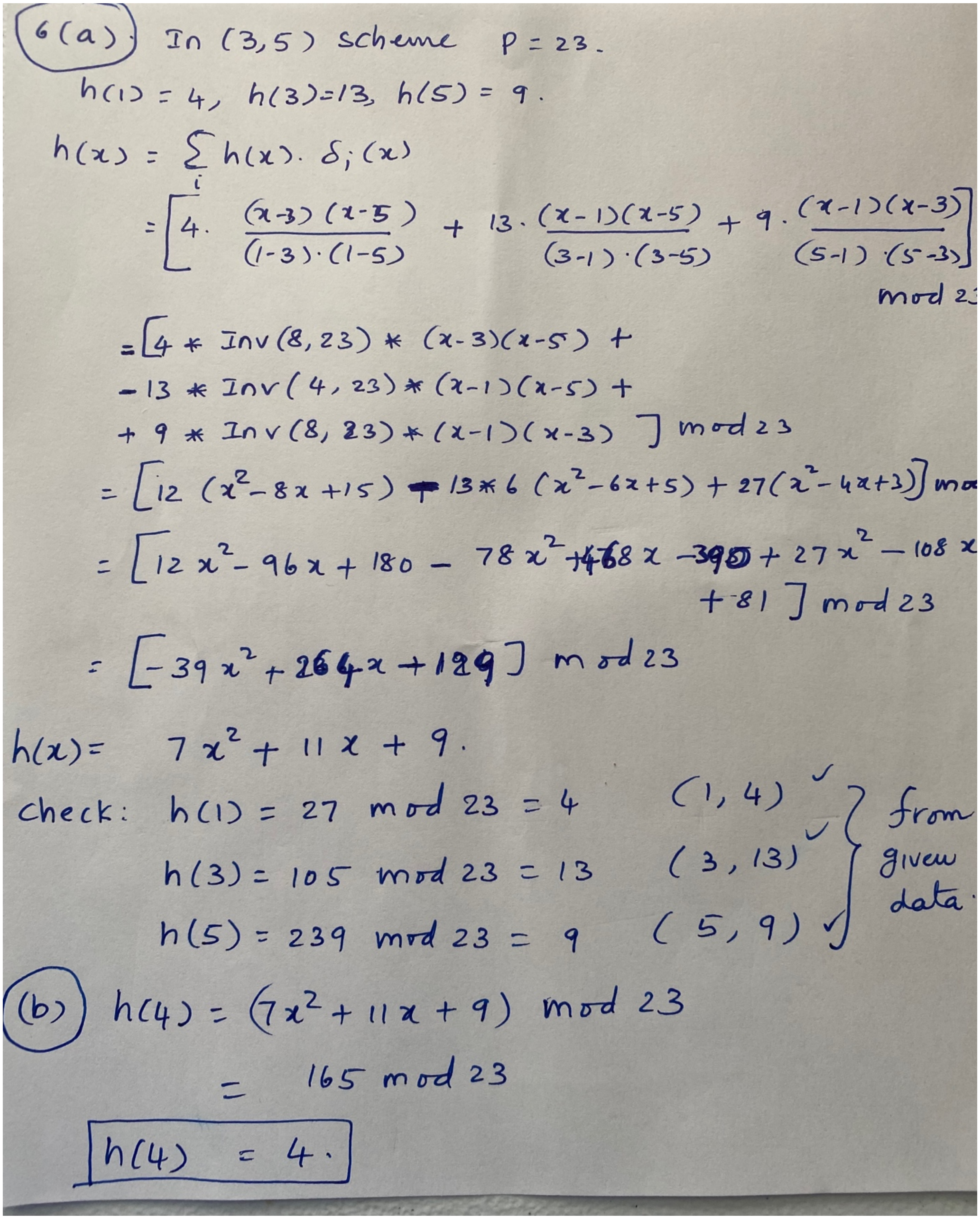
$f(x) = \sum f(x) \cdot \delta_i(x)$ (or) $h(x) = \sum h(x) \cdot \delta_i(x)$

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

$$= [24x^2 - 146x + 186] \mod 19$$

$$= 5x^2 + 6x + 15 \quad \boxed{K = 15}$$

Q 6.



6(a) In (3,5) scheme $p = 23$.

$h(1) = 4$, $h(3) = 13$, $h(5) = 9$.

$$h(x) = \sum_i h(x) \cdot \delta_i(x)$$

$$= \left[4 \cdot \frac{(x-3)(x-5)}{(1-3)\cdot(1-5)} + 13 \cdot \frac{(x-1)(x-5)}{(3-1)\cdot(3-5)} + 9 \cdot \frac{(x-1)(x-3)}{(5-1)\cdot(5-3)} \right] \bmod 2$$

$= [4 * \text{Inv}(8, 23) * (x-3)(x-5) +$

$- 13 * \text{Inv}(4, 23) * (x-1)(x-5) +$

$+ 9 * \text{Inv}(8, 23) * (x-1)(x-3)] \bmod 23$

$= [12(x^2 - 8x + 15) - 13 * 6(x^2 - 6x + 5) + 27(x^2 - 4x + 3)]$ mo

$= [12x^2 - 96x + 180 - 78x^2 + 468x - 390 + 27x^2 - 108x$
$+ 81] \bmod 23$

$= [-39x^2 + 264x + 129] \bmod 23$

$h(x) = 7x^2 + 11x + 9.$

check: $h(1) = 27 \bmod 23 = 4$ (1, 4) ✓

$h(3) = 105 \bmod 23 = 13$ (3, 13) ✓

$h(5) = 239 \bmod 23 = 9$ (5, 9) ✓

from given data.

(b) $h(4) = (7x^2 + 11x + 9) \bmod 23$

$= 165 \bmod 23$

$\boxed{h(4) = 4.}$