1.) Mention the families of SHA-2 ? Describe how 160-bit of hash value is generated by taking an input message of variable size using SHA-1 ?

→ The families of SHA-2 are

i) SHA-224
ii) SHA-256
iii) SHA-384
iv) SHA-512
v) SHA-512/224
vi) SHA-512/256

Generation of 160 bit of Hash value using SHA-1

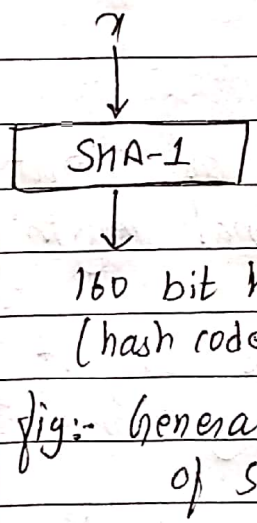

fig:- General Architecture of SHA-1

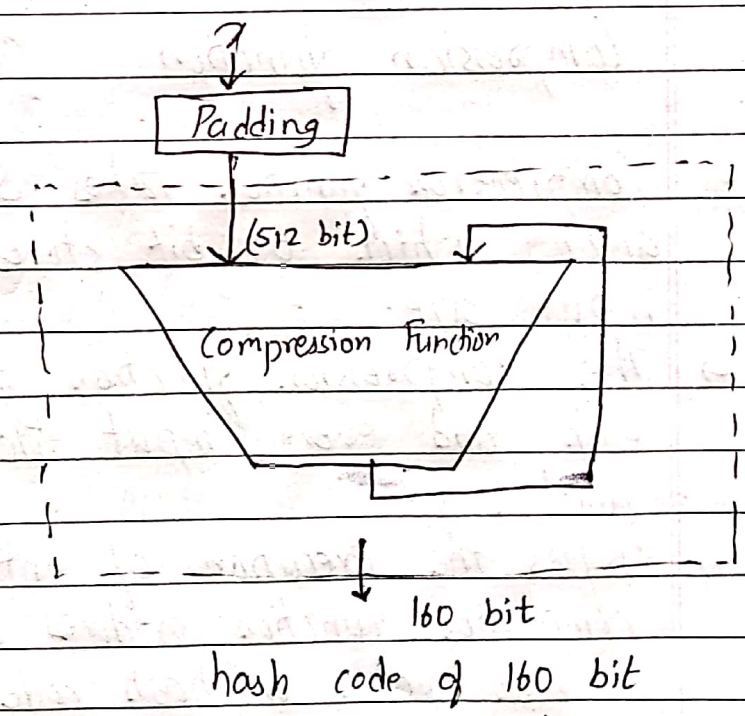

fig:- Detailed Structure of SHA-1 for generating 160 bit of hash value

SHA-1 consist of two major operation in order to generate 160 bit of hash value

- Padding
- Compression function

Padding

→ SHA-1 takes an input of arbitary length x
→ Now the arbitary length x is divided / fragmented into 448 bits.
→ Also the padding seperates 64 bit into binary format in order to store the original length of input

ie; 448 bit + 64 bit = 512 bit

→ Now, the 512 bit is made input to the compression function for futher processing

Compression function

→ Compression function takes 512 bit as an input among which 64 bit stores the original length of input size.
→ The compression function generates the output for each and every input iteratively using same function f.
→ After the execution of entire input, finally the compression function produces an output of 160 bit of hash value or hash code or message digest.

2.) Discuss how encryption and decryption is done using RSA? In a RSA system, a uses named Ram has chosen the primes 5 and 7 to create a key pair. The public key is (e_{Ram}, n) and the privale key is (d_{Ram}, n). Compute the privale and public key pairs. Suppose another uses Sita knows public key of Ram and want to send the plaintext "hi" to Ram using RSA scheme. Show how Sita has encrypted the plaintext and Ram has decrypted the ciphertext.

Encryption using RSA

→ Suppose the sender wish to send some text message to someone whose public key is (n, e).

→ The sender then represents the plaintext as a series of numbers less than n.

→ To encrypt the first plaintext P, which is a numbers modulo n. The encryption process is simple mathematical step as $C = P^e \bmod n$.

→ In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a numbe less than n.

→ Returning to our key generation example with plaintext $P = 10$, we get ciphertext

$$C = 10^5 \bmod 91$$

Decryption using RSA

→ The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.

→ Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n$$

→ Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29

$$\text{Plaintext} = 82^{29} \bmod 91 = 10$$

Here, $P = 5$, $q = 7$

$N = pq = 5 \times 7 = 35$

$\phi = (p-1)(q-1) = 4 \times 6 = 24$

Choose e. Lets look among the primes

$$\gcd(e, \phi) = 1$$

When $e = 2$, $\gcd(2, 24) = 2$ not possible

When $e = 3$, $\gcd(3, 24) = 3$ not possible

When $e = 5$, $\gcd(5, 24) = 1$ possible

$\therefore e = 5$

$1 < 5 < 24$ ie $(1 < e < \phi)$

$ed \equiv 1 \bmod \phi$

$5 \times d \equiv 1 \bmod 24$

$5 \times 5 \equiv 1 \bmod 24$

$25 \equiv 1 \bmod 24$

$\therefore d = 5$

Public key is $(e_{Ram}, n) = (e, n) = (5, 35)$
Private key is $(d_{Ram}, n) = (d, n) = (5, 35)$

Encryption (For Sita)

Message = hi = 2 = P

$C = P^e \bmod n$

$= 2^5 \bmod 35$

$= 32$

Decryption : (For Ram)

$P = C^d \bmod n$

$= 32^5 \bmod 35$

$= 2$

4.) Define authentication system. How challenge response systems can be used as authentication ~~protocol~~ approach?

→ Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be.

Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are.

Challenge Response System

→ Challenge-response, as a password authentication process, is a handshake authentication process in which the authenticator issues a challenge to the uses seeking authentication.

→ The uses must provide a correct response in orders to be authenticated.

→ Nowadays, responses are by a one-way function using a password token, commonly referred to as asynchronous tokens. ~~When~~

→ When the server receives the uses response, it checks to be sure the password is correct.

→ If so, the user is authenticated, and if not or for any reason the network does not want to accept the password, the request is denied.

5.) Define SSL. How SSL Record Protocol provides security in Secure Socket layer Protocol?

→ SSL stands for "Secure Sockets layer" which is a secure protocol developed for sending information securely over the internet. It encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted.

SSL Record Protocol provides security in Secure Socket Layer Protocol as

i) Confidentiality :-
The handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

ii) Message Integrity :-
The handshake protocol also defines a shared secret key that is used to form a message authentication code (MAC).

The SSL Record Protocol takes a application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmit the resulting unit in a TCP segment. Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users.

Decrypt "CMAL" using Hill cipher with key $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$

So

Here encrypted message is "CMAL"

$$k = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

Now, 2×1 matrix of ciphertext

CM AL

Now

Inverse of k $(k^{-1}) = \frac{1}{\det k} \text{ adj } k$

$$= \frac{1}{|ad-bc|} \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

$$= \frac{1}{|77-88|} \begin{bmatrix} 11 & -8+26 \\ -11+26 & 7 \end{bmatrix}$$

$$= \frac{1}{|-11+26|} \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix}$$

$$= \frac{1}{15} \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} \quad [\because (15 \times 7) \bmod 26 = 1]$$

$$= 7 \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} = \begin{bmatrix} 77 & 129 \\ 105 & 49 \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

Then

For CM

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \begin{pmatrix} 2 \\ 12 \end{pmatrix}$$

$$= \begin{pmatrix} 314 \\ 278 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 2 \\ 18 \end{pmatrix} = \begin{pmatrix} C \\ S \end{pmatrix}$$

For AL

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 11 \end{pmatrix}$$

$$= \begin{pmatrix} 242 \\ 253 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 8 \\ 19 \end{pmatrix} = \begin{pmatrix} I \\ T \end{pmatrix}$$

$\therefore$ CMAL is decrypted as CSIT

7.) Divide $5x^2 + 4x + 6$ by $2x + 1$ over GF(7).

Sol:

Here, $f(x) = 5x^2 + 4x + 6$

$g(x) = 2x + 1$

~~$f(x) / g(x) =$~~

Step 1 :-

Divide 5 by 2 using multiplicative inverse

i.e. $\frac{5}{2} = 5 \times 2^{-1} = 5 \times 4 \quad (2^{-1} = 4)$

$= 20 \mod 7 \quad [\because GF(7)]$

$= 6$

So, first term of quotient is $6x$

$$2x+1 \overline{)\ 5x^2 + 4x + 6\ (\ 6x}$$

$$\underline{-12x^2 + 6x}$$

$$-7x^2 - 2x + 6$$

For, GF(7), above term will be $5x + 6$

$[\because (7-7)x^2 + (7-2)x + 6]$

Again

$$2x+1 \overline{)\ 5x + 6\ (\ 6}$$

$$\underline{12x + 6}$$

$$-7x + 0 \quad [\because (7-7)x = 0]$$

For GF(7) above term will be 0

So, quotient is $(6x + 6)$

So,

$5x^2 + 4x + 6 = (2x+1)(6x+6)$

5.) Differentiate between virus, worm and trojan horse.

Virus :-

→ It is hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e. inserting a copy of itself into and becoming part of another program.
→ It cannot run by itself
→ It requires that its host program be run to make the active virus
→ Once a virus is executing it can perform any function, such as erasing files

Worm

→ It is a program that copies itself from one computer to another with the goal of overtaking the entire network of computers.
→ Most worms are designed to infiltrate systems by exploiting their security failures.
→ It is very dangerous as they take up a lot of bandwidth and other valuable resources.
→ It is often design to carry out the attack

Trojan Horse

→ It is a program with an overt effect and a covert effect (known & unexpected effect)
→ It is a useful, or apparently useful program a command procedure containing hidden code that, when invoked, performs some unwanted or harmful actions.
→ It contains malicious code that when triggered cause loss or even theft of data.

2.) Describe the purpose of PKI trust model ? list any four types of firewall.

→ Public-key infrastructure (PKI) defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute and revoke digital certificate based on asymmetric cryptography.

The purpose of PKI trust model is to enable secure, convenient, and efficient acquisition of public keys. It is used to provide trusted and efficient key and certificate management. It works best when there is a large mass of users.

The any four types of firewall are

i) Packet Filtering Firewalls
ii) Circuit level Gateway Firewalls
iii) Application level Gateway Firewall
iv) Stateful Multilayer Inspection Firewalls

17.) What is digital signature? How DSS approach is used to generate digital signature?

→ A digital signature is an electronic signature that can be used to authenticate the identity of the senders of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. It is easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. It can be used with any kind of message, whether it is encrypted or plaintext.

DSS approach

The DSS uses an algorithm that is designed to provide only the digital signature function. The DSS approach also makes use of a hash function. The hash code is provided as input to a signature function along a random number generated for this particular signature.

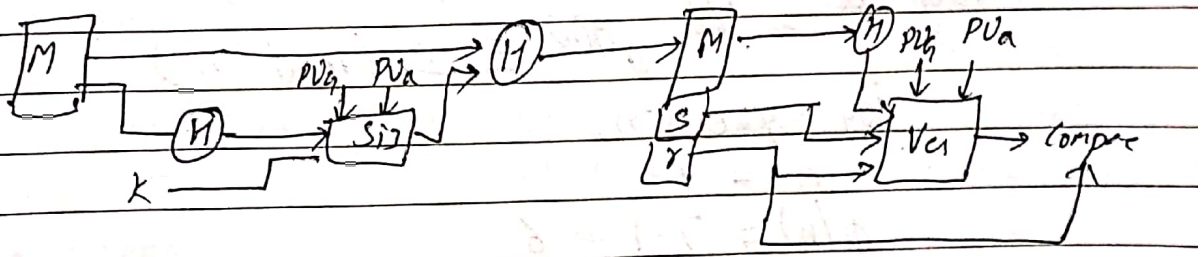

fig:- DSS approach

The signature function also depends on the sender's private key and a set of parameters known to a group of communicating principals. The result is a signature consisting of two components, labeled s & r.

11) Define Eulers totient Function. Find out whether 3 is primitive root of 7?

→ The number of positive integers less than n and relatively prime to n is known as Euler totient function. It is denoted by $\phi(n)$.
By convention, $\phi(1) = 1$

n	$\phi(n)$
1	1
3	2
13	12
14	6
15	8
19	18
20	8

If n is prime number then $\phi(n) = n-1$

3 is primitive root of 7 ?
If an integer 'a' has order $\phi(n)$ mod n (a +ve integer) and $(a,n) = 1$, then a is primitive root of n. Thus n has a primitive root a, iff

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

By question,
$n = 7$
$\phi(n) = 7-1 = 6$
According to def^n;
$a^6 \equiv 1 \pmod 7$
Since, 2, 3, 4, 5, 6 may be the primitive roots
To check for 3

$$3^6 = 729 \mod 7$$
$$\equiv 1 \pmod 7$$

Hence, 3 is a primitive root of 7

12.) Write Short Notes On

a) Vernam Ciphes

This system choose a keyword that is as long as the plaintext and has no stastical relationship to it. It was introduced by an AT&T engineer named Gilbert Vernam in 1918. This system works on binary data (bits) rather than letters. The system can be expressed succinctly as

$$c_i = p_i \text{ xor } k_i$$

where

p_i = i^{th} binary digit of plaintext
k_i = i^{th} binary digit of key
c_i = i^{th} binary digit of ciphertext

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.

b) Kerberos Protocol

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It is currently the default authorization technology used by Microsoft Windows, and implementation of Kerberos exist in Apple OS, Free BSD, UNIX and Linux. Main entities involved in Kerberos operation are

- Client
- Server
- Authentication Server (AS)
- Key Distribution Center (KDC)
- Ticket Granting Server (TGS)