Noakhali Science & Technology University

Noakhali-3814

Assignment On

Chapter – 12,13

Course Title : Information Security

Course Code : CSE 2205

Institute of Information Technology(IIT)

Submitted by:

Mir Mohammod Tahasin

Roll No : MUH2025007M

Year-2,Term-2

Institute of Information Technology

NSTU.

Submitted To:

Dr. Mohammad Nuruzzaman Bhuiyan

Assistant Professor

Institute of Information Technology

NSTU

Date of Submission:

20-01-2023

1. Write a routine (in pseudocode) to calculate the eighty constants in SHA-512 from the following table:

I	w_i
0..... 15	0,1,2,3,4,5,6,7,8,9,10,11,12, 13,14,15
16..... 31	0,4,8,12,1,5,9,13,2,6,10,14,3, 7,11,15

Question-01:

Solution:

(Routine in Pseudocode):

```
for i=0 to 79
      if i<=15
         wi = i

      else
         s0 = (wi-15) right rotate 17
         s1 = (wi-2)  right rorate 19
         s2 = (wi-7)  right rotate 10
         wi = s0 xor s1 xor x2 xor (wi-16)
      end if
   end for
```

Explanation:

SHA-512 is a hashing algorithm that performs a hashing function on some data given to it. Hashing functions take some data as input and produce an output (called hash digest) of fixed length for that input data. This output should, however, satisfy some conditions to be useful. So, SHA-512 does its work in a few stages. These stages go as follows:

1. Input formatting
2. Hash buffer initialization
3. Message Processing
4. Output

Here,the standard purposes a for circle to repeat through the numbers from 0 to 79.For every cycle,it first checks in the event that the ongoing worth of I is not exactly or equivalent to 15.Assuming it is,the consistent Wi is set to the worth of I.On the off chance that I is more prominent than 15,the standard purposes bitwise activities to compute Wi as the elite or(xor) of the aftereffects of turning the past upsides of Wi by specific sums,and afterward xor with Wi-16.The "right pivot"administrator turns the pieces of a number to the right by a predetermined number of positions,disposing of pieces that are moved off tyhe end and bringing the pieces that were on the passed on finish to the right end .

Question-02:

Solution:

Signature:

This process works as follows

1. The sender selects a random number r

2. The sender computes the first signature s1 using s1-erimodp

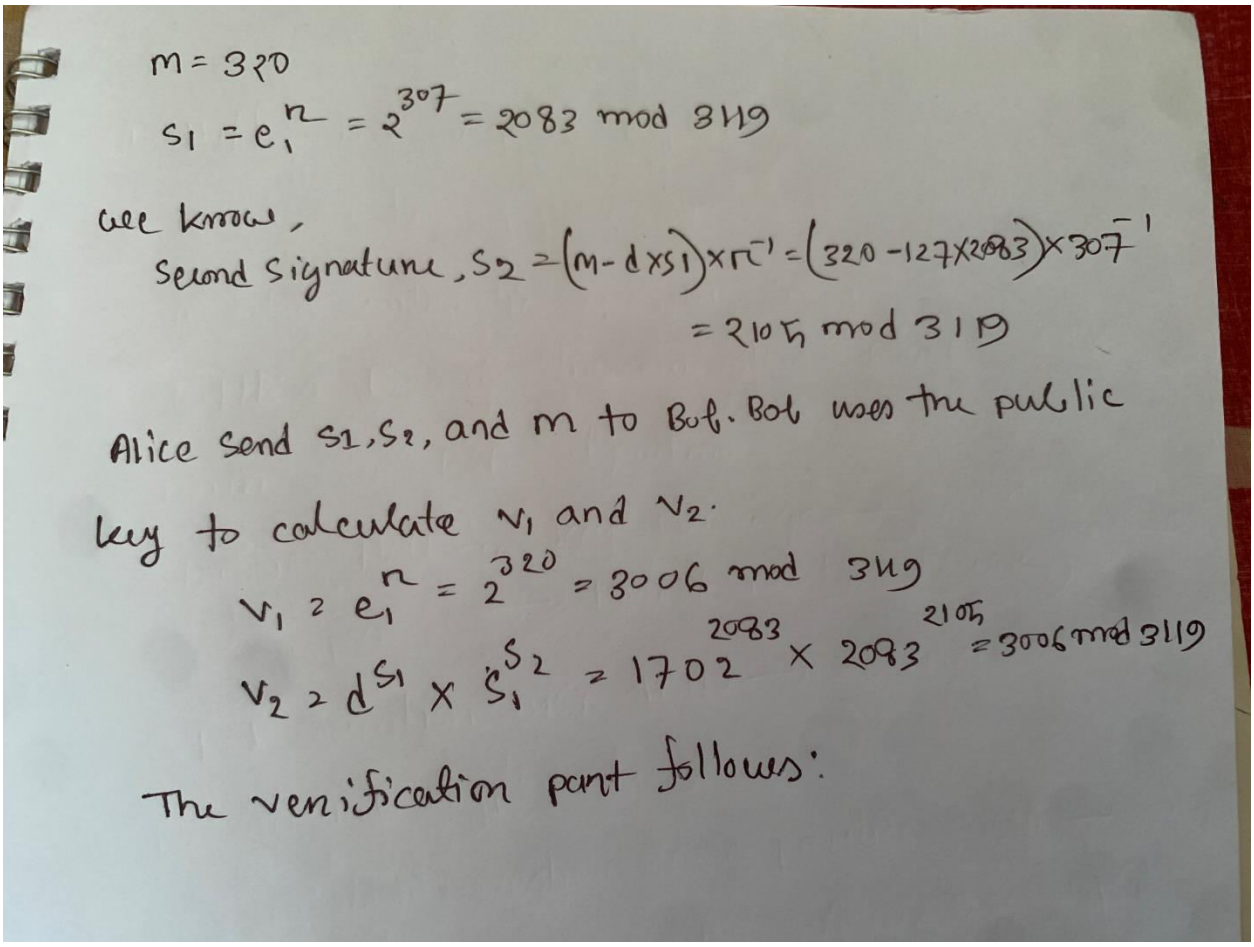
3. The sender computes the second signature s2 using the equation

s2 = (M-dXs1)Xr-1mod(p-1)

Where P= large prime number

M= original message that needs to be signed

Here in the above problem :



Verification:

This process works as follows.

1.The receiver performs the 1st part of verification called v1 using the equation

V1=eM1modP

2.The receiver performs the 2nd part of verification called as v2 using the equation

v2=es12s(s2)1modp

Eg

V1=eM1modp=1014mod19=16

And

V2=es12s(s2)1modp=43*34modp=5184 mod 19 = 16

So, v1=v2, the signature is valid.