Submitted by : SPOGMAI jan

Reg no :

2430-0081

Course :

Information security

Assignment no 4

My name SPOGMAi Jan

1) Convert to binary

S = 83 = 01010013
P = 80 = 01010000
O = 79 = 01001111
G = 71 = 01000111
M = 77 = 01001101
A = 65 = 0100001
i = 105 = 01101001
J = 74 = 01101010
a = 97 = 01100011
n = 110 = 01101110

So message bits are:

01010013 01010000 01001111 01001101 01000111
01010001 01101001 01000120 01100001 01101110

Add a single bit at + 1 and and add zeres
uninl unil suere she mas bits:

11 20 - . 1 1 _ 1C 00000 . . . . -

The semsrony bitaresettc ased form fam original
message bit length
The original message length is bit is 5-

0 0000 - - - - - 00002000 01000000
1 01100013 01010000 01000111 0100001 0110100
11000000 000000000 000000000 000100000

$H_1 \sim H_2 H7$.

Now we have to calculate T_1 and T_2

$T_1 = W_1 + K_j + Ch + \Sigma 1 H7$

$Ch(H_2, H_3, H_8) = (x \wedge y_7)(\sim x Z)$

$\Sigma 1(H_4) = ROTR2(H_4) \oplus ROTR^2(H_9) \oplus SHR^3(H_4)$

Now $T_3 = SH_3, H, H_4) + \Sigma O$

$Mo\&r(H_1) = ROTR^2(H_1) \oplus ROTR^1(H_0) \triangle ROTR22(H_0)$

So when T_1 and T_2 are obtained them

$H_0 = T_1 + T_2$

$H_1 > H_0$