Eric Cai

Ted Krovetz

CSC 152

November 15, 2017

Homework 5

1. 123456789 mod (216 – 2) > (123456789 div 216)2 + (123456789 mod 216)

111010110111100110100010101 >> 16 = 11101011011 << 2 = 111010110111 + 1100110100010101 =

1100001110100010 = 50082

//1101101111001011 = 56267

2.

h1 h2 h3 h4 h5

--+------------------

0 | 2 3 0 1 3

1 | 3 2 1 0 0

2 | 0 1 3 2 1

3 | 0 0 2 2 3

4 | 2 1 1 3 2

5 | 0 3 3 2 0

P(0,1) = 0 P(1,2) = 0 P(2,3) = 2/5 P(3,4) = 0 P(4,5) = 0

P(0.2) = 0 P(1,3) = 0 P(2,4) = 1/5 P(3,5) = 2/5

P(0,3) = 1/5 P(1,4) = 1/5 P(2,5) = 3/5

P(0,4) = 1/5 P(1,5) = 1/5

P(0,5) = 1/5

*Ε = 3/5*

3. FINDPREIMAGE(y): given y, find x such that H(x) = y

FIND2NDPREIMAGE(x): given x1, H(x1) = H(x2)

FINDPREIMAGE (y)

While(x != y)

If (H(x) == y)

Return x;

X++;

FIND2NDPREIMAGE (x)

While(H(x1) != H(FINDPREIMAGE(y)))

If (H(x1) != H(x2)

Return x;

X++;

FIND2NDPREIMAGE(x) is harder as a 2ndPreImageSolver implies a PreImageSolver

4. p = 367, q = 373 n = 136891

e = 5

d = 5-1 mod 136152

egcd(136152, 5)

136152 = (27230)5 + 2

2 = 136152 + (-27230)5

egcd(5,2)

5 = (2)2 + 1

1 = 5 + (-2)2

= 5 + (-2)[(136152 + (-27230)5]

= 5 + (-2)(136152) + (54460)5

= (-2)(136152) + (54461)5

egcd(2,1)

2 = (2)1 + 0

0 = 2 + (-2)1

= 136152 + (-27230)5 + (-2)[(-2)(136152) + (54461)5]

= 136152 + (-27230)5 + (4)136152 + (-108922)5

= (5)136152 + (136152)5

= (5)136152 + (136152)5

egcd(1,0)

Encryption:55 mod 136891 = 3125

Decryption: 312554461mod 136891 = 5

1. 1213 mod 13 > 121101 mod 13

|  |  |
| --- | --- |
| 1\*12 mod 13 = 1 | 121 |
| 122 \* 12 mod 13 = 1 | 1211 |
| (1442)2 mod 13 =1 | 12110 |
| (1442)2\*12 mod 13 = 1 | 121101 |

1. 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0xA, 0xB, 0xC, 0xD, 0xE, 0xF,