**Daniel Frey**

**CS 4920-001**

**Assignment 3**

**2/28/18**

**1.**

**a.** in binary notation: 0000 1011 0000 0010 0110 0111

1001 1011 0100 1001 1010 0101

in hexadecimal notation: 0 B 0 2 6 7 9 B 4 9 A 5

**b.** L0, R0 are derived by passing the 64-plaintext

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

**c.** Expand R0 to 48 bits:

E(R0) = 01110 100001 010101 010101 011110 100001 010101 010101

**d.** A = 011100 010001 011100 110010 111000 010101 110011 110000

**e.** (1110) = (14) = 0 (base 10) = 0000 (base 2)

(1000) = (8) = 12 (base 10) = 1100 (base 2)

(1110) = (14) = 2 (base 10) = 0010 (base 2)

(1001) = (9) = 1 (base 10) = 0001 (base 2)

(1100) = (12) = 6 (base 10) = 0110 (base 2)

(1010) = (10) = 13 (base 10) = 1101 (base 2)

(1001) = (9) = 5 (base 10) = 0101 (base 2)

(1000) = (8) = 0 (base 10) = 0000 (base 2)

**f.** B = 0000 1100 0010 0001 0110 1101 0101 0000

**g.** P(B) = 1001 0010 0001 1100 0010 0000 1001 1100

**h.** R1 = 0101 1110 0001 1100 1110 1100 0110 0011

**i.** L1 = R0. The ciphertext is the concatenation of L1 and R1.