SYSC 4502 Assignment 4

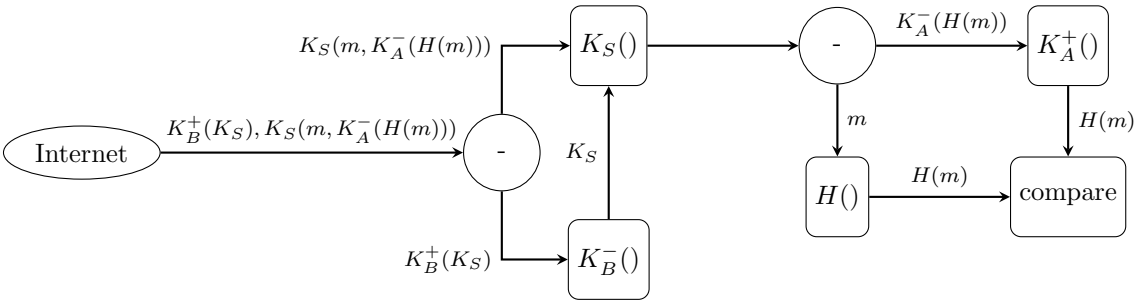
Jessica Morris 100882290

April 7th, 2017

1. (a) The output will be 00000101 repeated eight times.
   (b) The output will be 00000101 repeated seven times, ended with 10000101.
   (c) For (a), the output will be 10100000 repeated eight times. For (b), the output will be 10000101 followed by 10100000 repeated seven times.

2. (a) $n = p \times q = 5 \times 11 = 55$, $z = (p-1)(q-1) = 4 \times 10 = 40$
   (b) $e = 3$ is acceptable because it is less than n, and has no common factors with z.
   (c)
   $$de = 1(\text{mod } z)$$
   $$3d = 1(\text{mod } 40)$$
   $$d = \frac{1(\text{mod } 40)}{3}$$
   The nearest integer that gives $x = 1(\text{mod } 40)$ and is divisible by 3 is 81. Therefore:
   $$d = \frac{81}{3}$$
   $$d = 27$$
   (d) For $m = 8$, the ciphertext c is:
   $$c = m^e \text{mod } n$$
   $$c = 8^3 \text{mod } 55$$
   $$c = 512 \text{mod } 55$$
   $$c = 17$$

3. Bob's steps to decode the package from Alice:



4. (a) The three fields are (ICV = 1010 pre-encryption):

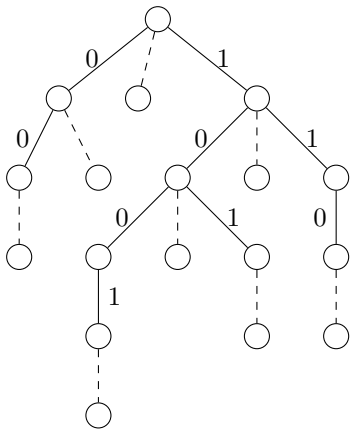
IV	11
message	
ICV	1010

   (b) b

   (c) c

   (d) d

5. Grid-of-Tries:



6.

Header Fields	Actions	Priority
if in_port=1 && (source_addr=10.1.0.1)	output:2	?