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) $n = p \times q = 5 \times 11 = 55$, $z = (p-1)(q-1) = 4 \times 10 = 40$

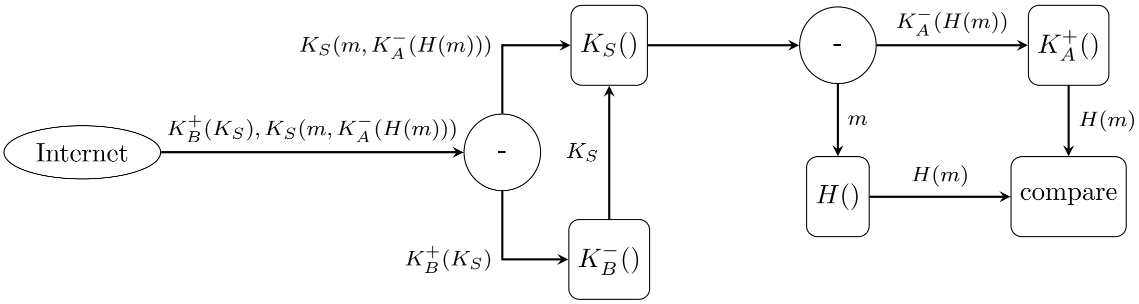
   (b) $e = 3$ is acceptable because it is less than n, and has no common factors with z.

   (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	01011010
ICV	0010

(b) Receiver has key = 1010. Since the IV (11) is unencrypted at the beginning of the packet, the receiver uses the same keystream to decrypt the packet. XOR'ing the received message + ICV with the keystream results in:

$$010110100010 \oplus 111110101000 = 101000001010$$

The first eight bits give $m = 10100000$ and the last four bits give $ICV = 1010$.

(c) If Trudy flips the first ICV bit, then she must also flip either the first or the fifth bit of the message.

(d) The part (a) WEP packet with the first message bit flipped and the first ICV bit flipped is 110110101010. XOR'ing with the 101011 keystream gives:

$$110110101010 \oplus 111110101000 = 001000000010$$

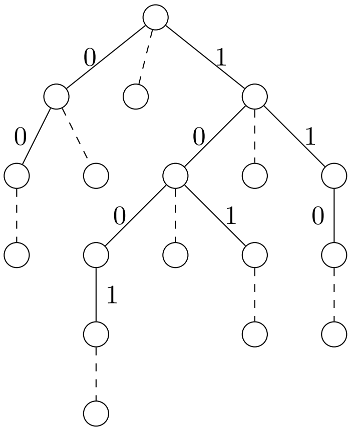
This gives $m = 00100000$ and $ICV = 0010$. The receiver computes the ICV for m to be $0010 \oplus 0000 = 0010$, so the ICV check passes.

Alternately, with the fifth message bit flipped, the receiver receives:

$$010100101010 \oplus 111110101000 = 101010000010$$

This gives $m = 10101000$ and $ICV = 0010$. The receiver computs the ICV for m to be $1010 \oplus 1000 = 0010$, so the ICV check passes.

5. Grid-of-Tries:



6.

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