Assignment 5—Chapters 8

CptS 425/580—Network Security
Assigned: 2 March 2009
Due: 9 March 2009, 4:15pm

Explain and/or justify all of your answers. Short answers are sufficient, but one-word (e.g., 'yes', 'no') answers will not receive full credit. State any assumptions that you make. Turn in a printout of your assignment and also email an electronic copy to the instructor.

Chapter 8

Answer the following questions from the Exercises (pgs 120-122).
10 Pts Question 8.3
10 Pts Question 8.6
15 Pts Question 8.17
10 Pts Question 8.18
10 Pts Question 8.21

AES

FIPS-197 lists the following pseudo-code for AES:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte state[4,Nb]
   state = in
   AddRoundKey(state, w[0, Nb-1])      // See Sec. 5.1.4
   for round = 1 step 1 to Nr–1
      SubBytes(state)                  // See Sec. 5.1.1
      ShiftRows(state)                 // See Sec. 5.1.2
      MixColumns(state)                // See Sec. 5.1.3
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for
   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
   out = state
end
```

15 Pts Like DES, AES is a hybrid cipher because it uses both substitution and transposition techniques. Classify the four subfunctions of AES (SubBytes, ShiftRows, MixColumns, and AddRoundKey) as either substitution, transposition, or product steps. Justify your answer.