Assignment 4—Chapters 8
CptS 425/580—Network Security
Assigned: 27 September 2005
Due: 6 Oct. 2005, 5:45pm

Explain and/or justify all of your answers. Short answers are sufficient, but ‘Yes’/’No’-type answers will not receive full credit. If you make any assumptions, please state them.

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 4.21

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 that uses two basic techniques that are common to classical ciphers. If the ‘SubBytes’ and ‘AddRoundKey’ functions were removed from the above pseudo-code would the resultant cipher still be a hybrid cipher? If not, how should the new cipher be classified?