Homework: /SI110/Models and Tools/Digital Cryptography

1. Read the notes and pay close attention to the Windows version of the md5 command and how to use it. There are several examples. The md5 hash of the string fragglerock is:

2. When we say “AES has a 128-bit block size” what do we mean?

3. Read carefully in the notes the section that describes how to use the aes tool. I have encrypted a message for you using 128-bit AES encryption. Decrypt it!
The key is 2a0757a14360d2432f1f5e6ac0359a5d
The ciphertext is 0a2bfea6495bfdeaedacc7a1548735665a4612e7b4ef968f4722882333fbc632
The decrypted message (plaintext) is:
4. Match the following descriptions with the letter of the appropriate image:

a. ____ Confidential communications with prior arrangements  
   [Diagram a]  

b. ____ Confidential, authenticated & non-repudiation communications without prior arrangements  
   [Diagram b]  

c. ____ Verifying a password  
   [Diagram c]  

d. ____ Digital signature  
   [Diagram d]  

e. ____ password/passphrase encryption  
   [Diagram e]