Homework2

Back to back comparison DES versus AES:

|  |  |  |
| --- | --- | --- |
|  | DES | AES |
| *Encryption*  *Sub-key Generator* | *AES can encrypt 128 bits of plaintext.*  *the data block is divided into two halves*  *Key length can be of 128-bits, 192-bits and 256-bits.* | *DES can encrypt 64 bits of plaintext.*  *the entire data block is processed as a single matrix*  *Key length is 56 bits in DES.* |
| *Rounds* | *Number of rounds depends on key length: 10(128-bits), 12(192-bits) or 14(256-bits)*  *The rounds in AES are:*  *Byte Substitution,*  *Shift Row,*  *Mix Column*  *Key Addition* | *DES involves 16 rounds of identical operations*  *The rounds in DES are:*  *Expansion,*  *XOR operation with round key, Substitution and Permutation* |
| *Decryption* | *The process of decryption of a DES is very similar to encryption, a common feature of Feistel ciphers in general. In fact, with some arrangements the only difference is the order of the subkeys, which is (or at least was) a big advantage as it makes implementation easier on limited devices, as you can mostly reuse the encryption code for decryption.* | *The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −*  *Add round key*  *Mix columns*  *Shift rows*  *Byte substitution* |