Brett Tomita

CECS 378

Assignment 2

1. 1 key is required for 2 people to communicate via a symmetric cipher, and is shared by the sender and recipient
2. A message authentication code is the result of using a secret key to generate a small block of data from a message, and is appended to the message
3. The 6 ingredients in a public key encryption scheme are:
   1. Plaintext
      * Readable message or data that is fed into the algorithm as input
   2. Encryption Algorithm
      * Performs various transformations on the plaintext
   3. Public and private key
      * Pair of keys that have been selected; one for encryption, one for decryption
   4. Ciphertext
      * Scrambled message produced as output. Depends on plaintext and key. 2 different keys produce 2 different ciphertexts
   5. Decryption Algorithm
      * Accepts ciphertext and matching key & produce original plaintext
4. No, in CBC mode, the input is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext, so the error will affect the next block. This results in an incorrect message being sent to the receiver
   1. For security, a three loop CBC would be better since the input for encryption/decryption is XOR’d 3 times instead of once.
   2. For performance, a one loop CBC would be better since the encryption is done in one step rather than 3
5. CFB Encrypt: *C*n = *P*n XOR S*s*[E(*K*, Cn-1)] CFB Decrypt: *P*n = *C*n XOR S*s*[E(*K*, Cn-1)]

CTR Encrypt: Cn = Pn­ XOR E(K, C+ N - 1) CTR Decrypt: Pn = Cn XOR E(K, C + N – 1)

* 1. CTS works by XORing the next block of plaintext and previous block of ciphertext/IV, and encrypting it up until Pn-1. The final ciphertext is the XOR of the last j bits of plaintext and the last j bits of the previous ciphertext
  2. CTS Decrypt: Pn = Cn XOR *leftmost j bits* Pn-1 = E(K, Cn-1 XOR Pn-2)

1. Yes, hash the subkey w/ ½ the block, xor the second ½
2. 1. N = 33

Fn = (3-1)\*(11-1) = 20