Scott Christensen

09/30/16

C.S. 465

H.W. #6 AES

- Description of the AES library you used (e.g., URL):
  - For my implementation of AES, I used the Java Cipher library. This class library supports cryptographic cipher for encryption and decryption. It supports a number of common cryptographic algorithms, like AES, DES, and RSA. With varying options for padding. I found its documentation here:
    https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html
    http://stackoverflow.com/questions/13102788/is-there-any-sample-java-code-that-does-aes-encryption-exactly-like-this-website

- Source code snippets showing how to encrypt/decrypt using the library

```
String keyHex = "00000000000000000000000000123456";
String plainText =
"GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
GGGGGAAAAAAAAAAAAAAAC";

String plaintextHex = toHexString(plainText.getBytes(Charset.forName("UTF-8")));
SecretKey key = new SecretKeySpec(DatatypeConverter.parseHexBinary(keyHex), "AES");
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding ");
cipher.init(Cipher.ENCRYPT_MODE, key);

byte[] result = cipher.doFinal(DatatypeConverter
.parseHexBinary(plaintextHex));
System.out.println(DatatypeConverter.printHexBinary(result));

cipher.init(Cipher.DECRYPT_MODE, key);
byte[] decryptedBytes = cipher.doFinal(result);
String decryptedText = new String(decryptedBytes, "UTF8");
System.out.println(decryptedText);
```

- Hex output of cipher text in at least two modes (e.g., ECB and CBC)
  - ECB cipher text:
    E1692336570F215D1E4C729611A7AC0FE1692336570F215D1E4C729611A7AC0FE1692336570F215D1E4C729611A7AC0F3D90F45AA5FFAB16C8FFFC7101DB16E073D90664985A3CD0D9A9E21C800B644D
  - CBC cipher text:
    136196AB4690E6FB43CDB761CC7D8FBBFAA152BFDF4D8890DF0C752E7ACBC629E9AB48FF82C71586FB14070F15F0CBE8E380BA1931073A7212CB3DE15C5E63BB7D67412941D01F7E4527471B3834710B

- Lessons learned - list of 2-5 items about your experience
    - I learned that for most cipher algorithms there are multiple padding options that can be used throughout the encryption/decryption process.
    - I learned that there is a big difference in the algorithms when using either cipher block chaining (CBC) or just processing the raw cipher text (ECB).
    - I learned that there actually are decent Java libraries for doing encryption/decryption algorithms and there is a lot of good support on how to use them online.