CALIFORNIA STATE UNIVERSITY
LONG BEACH

Homework #2

CECS 378 – Spring 2020 Cappel

Due: Thursday, February 20 prior to class (5 PM)

Homework #2 is focused on more modern cryptography. 4 total solutions all worth 25 points (100 total).

This assignment will introduce you to several instances of modern cryptography and have you encrypt the plaintext. **Please show all of your work!**

Problem 1 – Simplified DES

Simplified DES (SDES) was designed for educational purposes only, to help students learn about modern cryptanalytic techniques.
SDES has similar properties and structure as DES but has been simplified to make it much easier to perform encryption and decryption by hand with pencil and paper.
Some people feel that learning SDES gives insight into DES and other block ciphers, and insight into various cryptanalytic attacks against them.

Note: The following You-Tube video may be of value when performing the Simplified DES problem:

https://www.youtube.com/watch?v=QcKHfMgcnbw

Let **K** be the key, **K** = 1001100010 in binary format.
Let **P** be the plain text message, **P** = 10011100 in binary format.

Find $\mathbf{K_1}$ the key for round 1, $\mathbf{K_2}$ the key for round 2, & **C** the cipher text message, where **K1**, **K2**, & **C** are in binary format.

Problem 2 – DES

Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for most current applications, it has been highly influential in the advancement of modern cryptography.

Note: The following websites may be of value when performing the DES problem:

http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm

https://www.youtube.com/watch?v=Sy0sXa73PZA (Notice the spreadsheet included with the YouTube video – leverage it!)

http://des.online-domain-tools.com/

https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html

Let **M** be the plain text message, **M** = 44 69 72 74 62 61 67 73 in hex format (where **M** is Dirtbags in ASCII text).
Let **K** be the hexadecimal key, **K** = 43 57 53 31 39 39 38 21 in hex format (where **K** is CWS1998! in ASCII text).

Solve for **C** the cipher text message, where **C** is in hex.

Problem 3 – RSA

Note: A similar problem can be found in Chapter 21 in the textbook (pg. 649).

Perform encryption and decryption using the RSA algorithm, as in Figure 21.8 in the textbook, for the following:

p = 11; q = 3, e = 3, M = 8

Problem 4 – Diffie-Hellman

Note: The following problem can be found in Chapter 21 in the textbook (21.12).

Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α = 2.

a. If user A has public key $Y_a = 9$, what is A's private key X_a?
b. If user B has public key Yb = 3, what is the shared secret key K?