CALIFORNIA STATE UNIVERSITY
LONG BEACH

Homework #2

CECS 378 – Spring 2021 Cappel

Due: Wednesday, February 17th prior to class (11:59 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 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.

K = 1001100010
P = 10011100

P = 10011100
IP = 01011010
EP = 0101 0101
K1 = 1011 0000

1110 0101

11 01
1101

1101
0101
100 1010
1010 1000
0100 0001
0001 0011
0101 0010

0101
1100
1010

0110 1000

0011 0100

K1 = 10110000
K2 = 00010011
C = 0011 0100

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 and spreadsheet will 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 to solve this problem!)

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.

Using the excel sheet provided I obtain the following cipher C

C:53 97 e0 17 62 32 86 24

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

n = p * q = 33
n' = (p-1) * (q-1) = 20
e= = 3
de mod20 = 1 -> d * 3 mod20 = 1 -> d = 7
encryption :
m^e modn = 17
decryption :
M= 17^7 mod 33 = 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?

   Y = x^x_a mod11

   9 = 2^x_a mod11 -> x_a = 6

b. If user B has public key $Y_b = 3$, what is the shared secret key K?

K = (y_b)^x_a mod q
= 3^6 mod 11
= 3
K = 3