CSCD27 Fall 2014 Assignment Assignment 1

Name: Ye Zheng(Vincent)

SN: 998478829

Question #	Score
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
Total	

Acknowledgements:

"I declare that I have not used any outside help in completing this assignment."

Name: Ye Zheng(Vincent) Date: October 10, 2014

Q1. Already send it in email

Q2. Already send it in email

Q3. Aleady send it in email

Q4. Here is the way to detect the gcc has been compromised:

1. Use XL compiler to compile a brand new gcc from source code

2. Compare the binary file between the newest gcc, and old gcc

3. Even through functionality for both gcc is same, but the binary code for that two version will be different, if old gcc has been compromised. In that case, we just using the newest one (The one just compiled with XL compiler to replace the old gcc)

Q5. On Average, brute-force attack need to try half of keyspace to success, therefore, the time to perform brute-force will be in this forumula $\frac{keyspace\ we\ need\ to\ try}{\frac{3.4*10^9}{80}*16}$

Since DES using 56-bit keyspace, and we need to try at least $2^56/2$ times, substitute $(2^56)/2$ into that formula, we get 52983525.027888188s, approximately 1.68 years.

For 3DES the keyspace is 56 * 3 = 168 bit, substitute $2^{168/2}$ into the formula, we get $2.7510619e+41$s, approximately $8.71778e33$ years.

For AES-128, keyspace is 128 bit, and substitute $2^{128}/2$ into the formula, we get $2.5020762e+29s$, approximately $7.92877037516265043e+21$ year

For AES-256, keyspace is 256 bit, and substitute $2^{256}/2$ into the formula, we get $8.5141242e+67s$, approximately $2.6980207768018975e+60$ year

Q6.

Q7. On Encryption:

We break down the plaintext into two same bit, call L_i, and R_i, i means the round of encrypt
On Each round $L_i = R_{i-1}$, and $R - i = L_{i-1} \oplus F(R_{i-1}, K_i)$
User will provider the keys for each round, and using it for encryption

On Decryption:

We have cipher text, the keys for each round during the encryption. The algorithm for decrytion is same as encryption, except the K_i is in reverse order.

Q8.

Q9. For DES, the total number of key will be 2^{56}, therefore the probability to find the unique key (it said unique it means only ONE key will break the secret key that Alice and Bob know) will be $\frac{1}{2^{56}}$, which change to percentage will be approximate 1.7%

Q10.

Q11. The way to hacked just modified the IV to match the old plaintext $\oplus$ IV, we know old plaintext, we know the IV and we know the new plaintext, all we need just calculate the new IV.
Let result = old plaintext $\oplus$ IV = e9788d1a330d6bb22b74984f88c76187
The hex decimal for the new plain text message will be 476976652050617472 6f6e2024393837, using the new plain text message, xor with the result, we get ae11fb7f135d0ac6591bf66facfe59b0

So we just modify the cipher text to this b1710117cfe1cc5549bbb45f0bad1c8c ae11fb7f135d0ac6591bf66facfe59b0