Homework 2

Due on October 10

1. What would be the 64-bit output of round 1 in DES be using the plaintext and key given below (in hexadecimal format): (CS450: 25 points) (CS650: 15 points)

P = 2D 75 F4 DB A3 3E 3F 89

K = D4 3C B1 9A E4 90 D7 C6

You could either write your own code or use the tool at: http://des.online-domain-tools.com

ANS: I utilized a different website (https://www.emvlab.org/descalc/) because the provided link would not calculate the DES output for me. The output of using the DES encryption algorithm using the Plaintext and Key provided was:

Encryption Output Data:

1D1EE17BC9ACD2F6

Decryption Output Data:

010AD9A9A0E20468

2. Consider the following encrypted text

JLQEBO: TEXQ AFA VLR IBXOK FK PZELLI QLAXV PLK: ELT QL TOFQB JLQEBO: TEXQ AFA VLR TOFQB? PLK: F ALK'Q HKLT, QEBV EXSBK'Q QXRDEQ RP ELT QL OBXA VBQ!

Decrypt is using the tool available at https://www.xarg.org/tools/caesar-cipher/ (CS450: 25 points) (CS650: 15 points)

a) What is the plain text?

ANS: MOTHER: WHAT DID YOU LEARN IN SCHOOL TODAY SON: HOW TO WRITE MOTHER: WHAT DID YOU WRITE? SON: I DON'T KNOW, THEY HAVEN'T TAUGHT US HOW TO READ YET!

b) What is the key?

ANS: **KEY = 3**

3. Given speed of a current ordinary computer, estimate the amount of time necessary to crack a DES encryption by testing all 2^56 possible keys. Make a similar estimate for a 128-bit AES key. (CS450: 50 points) (CS650: 20 points)

Note: For this question, the exact answer is not as important as how the answer was derived. Make necessary assumptions, clarify them and show work.

ANS: Assuming an ordinary computer in 2018 contains a 3 GHz processor and takes

$$(\mathbf{75}\ \boldsymbol{CPU\ cycles})/(\mathbf{1}\ \boldsymbol{brute\ force\ attack\ per\ second})$$

Then the estimated time necessary to crack the DES encryption by testing all 2^{56} keys would be the following:

DES:

(2^{56} keys)*(75 CPU cycles)/(1 brute force attack per second)/(86,400 seconds per day)/(365 days)/(3*10^{9}Hz) = 57.1233 years, about 57 years

AES:

(2^{128} keys)*(75 CPU cycles)/(1 brute force attack per second)/(86,400 seconds per day)/(365 days)/(3*10^{9}Hz) = 2.6976e^{23} years, a very long time!

4. **(GRAD 650)** Assume each S-box substitution takes 8 units of time (because of the eight 6-bit substitutions), each P-box permutation takes 4 units of time (counting 1 unit per byte), each expansion permutation takes 8 units of time (because of the eight 4-bit expansions and permutations) and each initial and final permutation takes 8 units. Compute the number of units of time for an entire 16-round cycle of the DES. (CS450: BONUS 10 points) (CS650: 50 points)

ANS:

IP = Initial Permutation → 8 units

EP = Expansion Permutations → 8 units

SB = S-Box Substitution → 8 units

PB = P-Box Permutation → 4 units

FP = Final Permutation → 8 units

Units of time for 16-round cycle of DES = IP + 16 * (SB + PB + EP) + FP

= 8 + 16 * (8 + 4 + 8) + 8 = 336 units of time