## 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

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)

1. What is the plain text?
2. What is the key?

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.

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)