Homework 2

Due: Lesson 13

(50 pts)

Help Policy

AUTHORIZED RESOURCES: Any, except another cadet's program.

NOTE:

- Never copy another person's work and submit it as your own.
- Do not jointly create a program.
- You must document all help received from sources other than your instructor or instructor-provided course materials (including your textbook).
- **DFCS will recommend a course grade of F for any cadet who egregiously violates this Help Policy or contributes to a violation by others.**

1. [5] We saw in class that the Shift Cipher is very weak, in general. Suppose the 26 keys of the Shift Cipher are used with equal probability 1/26 (yes, even k=0). Prove that if you only encrypt a single message of just one character, then no matter what the plaintext probability distribution is, the Shift Cipher has perfect secrecy. Use English to supplement your math (make your proof understandable).

2. [5] We have a cryptosystem with three plaintext letters '*a*', '*b*', and 'c' which occur with probabilities of 0.8, 0.15, and 0.05 respectively. There are three keys k_1, k_2, and k_3 which occur with equal probability. The resulting encryption table for the three keys is as follows:

	a	*b*	*c*	
k_1	C	A	B	(In other words $E_{k1}(a) \rightarrow C$)
k_2	A	B	C	
k_3	B	C	A	

   a. Calculate the entropy of the plaintext H(P).
   b. Calculate the entropy of the plaintext, given the ciphertext H(P|C).
   c. How much information does the ciphertext give you about the plaintext? What about if *k*3 encrypted '*a*' to '*C*' and '*b*' to '*B*' instead? How would that effect H(P|C) (answer theoretically not numerically)?

3. [5] Find integers *x* and *y* such that $27x + 98y = 1$.

4. [5] Find 15^{-1} (mod 101) using the Extended Euclidean algorithm. Based on your results, what is 101^{-1} (mod 15)?

5. [5] Find the gcd(98, 756).

6. [5] Find the inverse of 901 (mod 2968). Show all the steps.

7. [5] Find all possible solutions for x:

   a. $12x \equiv 28 (\text{mod } 42)$
   b. $12x \equiv 30 (\text{mod } 42)$

8. [5] Find all possible solutions for x:

   a. $x^2 \equiv 8 (\text{mod } 31)$
   b. $x^2 \equiv 16 (\text{mod } 24)$
   c. $x^2 \equiv 5 (\text{mod } 17)$

9. [10] Write a small program that implements the Extended Euclidean algorithm to find the greatest common divisor. The program should output the *gcd* and *x* and *y*. Input should be two non-negative integers a and b, with $a \geq b$. Your program should also provide an option to calculate the inverse of a number with some modulus for the user. Submit a screen shot showing all the working features of your program along with a print out of your code.

2.107 Algorithm Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, and return(d,x,y).
2. Set $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, and return(d,x,y).