CIS 3362 Final Exam Review

Date: 12/9/2022 (Friday)
Time: 10:00 am – 12:50 pm
Part A (10 pts): 10 am – 10:30 am topics (Odds and Ends)
Part B (90 pts): 10:30 am – 12:50 pm (Everything else)
Format: Written, Short Answer, Problems
Exam Aids: Four Sheets of Typed/Written Notes - You Bring
Reference sheets (Exam 1, DES, AES) - I provide
Calculator -You Bring

If you need a make up, you need to tell me BEFORE the exam. (Depending on the situation and timing, I will either do the make up before finals end, or assign an incomplete and give the final when it makes sense.)

Everyone who has credit in Webcourses for "FEA" before the final exam should come at 10:30 am. Everyone who does not, should come at 10 am.

Mathematical Tools

Euclidean Algorithm
Extended Euclidean Algorithm
Index of Coincidence
Mutual Index of Coincidence
Prime Number Definition
Fermat's Theorem
Euler Phi Function
Primitive Roots of a Prime
Discrete Log Problem
Miller-Rabin Primality Checking Algorithm
Fermat Factoring
Pollard-Rho Factoring
Discrete Log Problem
Fast Modular Exponentiation

Classical Cryptography Part I

Shift Cipher
Affine Cipher
Substitution Cipher
Vigenere Cipher

Classical Crytography Part II

Playfair
ADFGVX
Hill Cipher
Enigma
Navajo Code
Transposition

Modern Symmetric Ciphers

Bitwise operators
DES
AES

Public Key Cryptography

Diffie-Hellman
RSA
El Gamal
ECC

Odds and Ends

Quantum Cryptography
Hash Functions, Salting Passwords
Birthday Attack
Probability Problems Associated with Birthday Attack

Some Past Final Exam Questions

1) In a set of 100 bits (zeroes and ones), the index of coincidence is $\frac{19}{33}$. Let x be the number of 0s in the set and y be the number of 1s in the set. What is |x - y|?

2) Consider an affine cipher for an alphabet of size 65 with the encryption function

$$f(x) = 28x + 33 \bmod 65$$

Determine the corresponding decryption function $f^{-1}(x)$.

3) Consider the following IP matrix for a DES-like cipher with a block size of 16 bits:

$$IP = \begin{bmatrix} 14 & 9 & 8 & 3 \\ 6 & 12 & 1 & 11 \\ 16 & 7 & 5 & 15 \\ 2 & 4 & 10 & 13 \end{bmatrix}$$

If the input to the IP matrix in HEX is 4F79, what is the output, represented in HEX?

4) What is the result of the multiplication 03 x B6, in the AES field? In order to get credit, you must show all of your work by hand.

5) A generator, g, of a prime p is a number such that the set $\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\}$ contains each of the integers from 1 to p-1 precisely once. We will call a half-generator, g, of a prime number p a number such that the set $\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\}$ contains half of the integers from 1 to p-1 precisely twice. How many half generators are there for a prime p? Please give your answer in terms of the Euler phi function and p with a rationale for your answer. (Note: This one is challenging, but the answer can be derived from the reasoning behind counting the number of generators of a prime p, using a particular generator, g.)

6) (15 pts) One way to calculate φ(n) is to find each unique prime number, p_i that is a factor of n, and multiply n by each term of the form $(p_i - 1)/p_i$. Notice that since p_i is a divisor of n, one can first do the division and then the multiplication and the answer will be accurate without risk of overflow. In the algorithm we maintain two "accumulators" a running value of n and a running value of phi. Both are initialized to n and both will get reduced in different ways over the course of the algorithm, which is described below.

Consider using this algorithm to calculate φ(300). We first discover that 2 is a prime factor of 300. So take 300 and multiply by ½, yielding 150, our running value of phi. In addition, divide out each factor of 2 from 300 to yield 75, what remains after dividing out each copy of 2, our running value of n. Next, we discover that 3 is a prime factor of 75. Thus, we take 150 and multiply by 2/3 yielding 100. In addition, we take 75 and divide out all copies of 3, yielding 25. Finally, we find that 5 is a prime factor of 25, so we multiply 100 by 4/5 yielding 80. Once we divide out all copies of 5 from 25 and get 1, we find that we are done. It follows that φ(300) = 80, which is what our function should return in this instance.

In some instances, we will be left with a prime number instead of 1. Consider, if after dividing by 5 we had 37 left. Then, after dividing by 6, we see that we've tried all values less than or equal to the square root of 37, so we know there's no point in continuing the trial division. In this case, we would multiply our running value of phi by 36/37 after exiting our main loop. (Note: if you continue trial division all the way to n instead of stopping early and do everything else correct, you'll earn 12 of 15 points on this question.)

Write a C function that implements the calculation of phi using the algorithm described above. (Note: no array is needed for this function, just two accumulator variables and a set of nested loops that do the process described above.

7) Consider the elliptic curve $E_{47}(10, 17)$. Let the point P on the curve be (24, 13) and the point Q on the curve be (35, 7). Calculate P + Q.

8) For the purposes of this question, assume that the probability any arbitrary person's birthday is a particular month is exactly $\frac{1}{12}$, for each month. If 4 people are chosen at random, what is the probability that 2 of the people are born in one month and the other 2 people are born in a different month? Express your answer as a fraction in lowest terms.