CIS 3362 Final Exam Review

Date: 12/9/2020 (Wednesday)
Time: 10:00 am – 12:50 pm
Format: Four Timed Sections
Part A: 10:00 am – 10:35 am, late 10:45 am
Part B: 10:40 am – 11:15 am, late 11:25 am
Part C: 11:20 am – 11:55 am, late 12:05 pm
Part D: 12:00 pm – 12:40 pm, late 12:50 pm
Exam Aids: All Course Notes,
All posted reference sheets (Exam 1, DES, AES)
Calculator
Strongly Suggested to Type So there aren't issues with timing.
Any part not received gets a 0.

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.)

Part C: Number Theory, Part of Public Key

1. Prime Factorization
2. Fermat's Theorem
3. Euler Phi Function
4. Euler's Theorem
5. Discrete Log Problem
6. Generators/Primitive Roots of Primes
7. # of Generators of a prime
8. Primality Testing (Miller-Rabin)
9. Fermat Factoring
10. Pollard-Rho Factoring
11. Diffie-Hellman Key Exchange
12. RSA Encryption

Part D: Rest of Public Key, Odds and Ends

1. El Gamal Cryptosystem
2. Elliptic Curve Definition
3. Adding points on Elliptic Curves (Division is multiplication by mod inverse)
4. Quantum Cryptography Idea
5. Group Diffie-Hellman
6. Probabilities in Birthday Attack
7. Hashing Idea, Salting Passwords
8. Use of RSA twice for Digital Signature

Looking at Fall 2019 Exam

9) First we factor n…I guessed around 20 and tried both 17, and 19 and found 551 = 19 x 29 phi(551) = phi(19)*phi(29) = 18*28 = 504

$d = 275^{-1} \bmod 504$ (run EEA)

11) Curve $E_{37}(2, 3)$. What is (15, 2) + (25, 29)?

Lambda = (29-2)/(25-15) mod 37 = 27 x 10^{-1} mod 37

$10^{-1} = -11 \bmod 37$ (or you can write it as 26)

Lambda = 27 x (-11) = -297 = -1

X = (lambda^2 – xp – xq) = 1 – 15 – 25 = -39 = **35 mod 37**

Y = (lambda(xp-xr)-yp = -1(15 - -2) – 2 = -17 – 2 = -19 = **18 mod 37**

(35, 18)

12) There are a total of 12^4 possible answers to what month is your birthday asked to an ordered set of 4 people.

Of these 12^4 responses, we want to count the ones where there are 2 of one month and 2 of another month.

Jan May May Jan

Jan Jan May May

Jan May Jan May

12 ways to fill the first month

3 ways to choose which of the other three slots match it

11 ways to fill the last two slots

Probability is (12 x 3 x 11)/(12 x 12 x 12 x 12) = 11/576

Fall 2018 Final

8) n = 221, phi(n) = 192

(p-1)(q-1) = 192, n = pq, so q = n/p

q-1 = 192/(p-1)

q = 1 + 192/(p-1)

p*q = n

p(1 + 192/(p-1)) = 221

p(p-1)(1 + 192/(p-1)) = 221(p-1)

p(p-1) + 192p = 221p – 221

p^2 – p + 192p = 221p – 221

p^2 – 30p + 221 = 0

Fall 2017 Final

In Diffie Hellman, if I am only asking for the secret key, you could just write out the final answer and use Fermat's to simplify it.

$13^{12*15} = 13^{180} \bmod 83$

$13^{82} = 1 \bmod 83$

$13^{180} = 13^{164}13^{16} \bmod 83$

$= 13^{16} \bmod 83$