Exam #3 Review

(1) I will not be here.

(2) Proctors: Justin Rehg, Jade Bowyer
↳ pass out papers

(3) 1 SHEET OF NOTES
(11" x 8.5" both sides) typed or written

(4) CALCULATOR

(5) NOT HERE FRI, THURS → BUSY

TOPICS

GCD
Fermat Thm
ϕ function
Euler's Thm
Miller-Rabin Primality Test
Discrete Log Problem
Factoring: Fermat, Pollard-Rho
Diffie-Hellman Key Exchange
RSA
El-Gamal
Knapsack Cryptosystem (8.7 typed)

11/6/19 (2)

CIS 3362 Test #3: Public Key Encryption

Date: 11/17/2017

Name: _____

Note: For questions with numeric answers, put a box around your final answer.
Aids: You may use a calculator and 2 sheets of notes

1) (8 pts) What is the prime factorization of 419325984?

$2^5 3^4 7^1 11^2 191^1$

Trial Division on Cal

2) (8 pts) What is φ(419325984)?

$\phi(2^5 3^4 7^1 11^2 191^1)$

$= (2^5 - 2^4)(3^4 - 3^3)(7^1 - 7^0)(11^2 - 11^1)(191^1 - 191^0)$

put in cal

$= 108345600$

3) (12 pts) Using Fermat's Theorem, determine 2536^{42841} mod 6121. (Note: 6121 is a prime number.

$2536^{6120} \equiv 1 \mod 6121$

by Fermat's

$2536^{42841} \equiv 2536^{7(6120)+1}$

$\equiv (2536^{6120})^7 \times 2536^1$

$\equiv 1 \times 2536 \mod 6121$

$\equiv \boxed{2536} \mod 6121$

4) (12 pts) Using Euler's Theorem, determine $638^{15363} \bmod 5525$.

$5525 = 5^2 \times 13 \times 17$

$\phi(5525) = (5^2 - 5^1)(13-1)(17-1)$

$= 20 \times 12 \times 16$

$= 3840 \Rightarrow 638^{3840} \equiv 1 \bmod 5525$ by euler's thm.

$638^{15363} \equiv 638^{3840 \cdot 4 + 3} \equiv (638^{3840})^4 638^3 \equiv 1^4 \cdot 638^3$

$\equiv 259694072$

$\equiv \boxed{2497} \bmod 5525$

5) (12 pts) In an RSA scheme, p = 11, q = 41 and e = 189. What is d?

$n = 11 \times 41 = 451$

$\phi(n) = (11-1)(41-1) = 10 \times 40 = 400$

$d \equiv e^{-1} \bmod 400$

$189^{-1} \bmod 400$

$400 = 2 \times 189 + 22$

$189 = 8 \times 22 + 13$

$22 = 1 \times 13 + 9$

$13 = 1 \times 9 + 4$

$\boxed{9 = 2 \times 4 + 1}$

$43 \times 400 - 91 \times 189 = 1 \bmod 400$

$-91 \times 189 \equiv 1 \bmod 400$

$d \equiv -91 \equiv \boxed{309} \bmod 400$

$9 - 2 \times \boxed{4} = 1$

$9 - 2(13 - 9) = 1$

$9 - 2 \times 13 + 2 \times 9 = 1$

$3 \times \boxed{9} - 2 \times 13 = 1$

$3(22 - 13) - 2 \times 13 = 1$

$3 \times 22 - 3 \times 13 - 2 \times 13 = 1$

$3 \times 22 - 5 \times \boxed{13} = 1$

$3 \times 22 - 5(189 - 8 \times 22) = 1$

$3 \times 22 - 5 \times 189 + 40 \times 22 = 1$

$43 \times \boxed{22} - 5 \times 189 = 1$

$43(400 - 2 \times 189) - 5 \times 189 = 1$

$43 \times 400 - 86 \times 189 - 5 \times 189 = 1$

$43 \times 400 - 91 \times 189 = 1$

11/6/19 (4)

6) (10 pts) Alice's Public El Gamal keys are q = 31, and α = 11. Alice's secret key $X_A = 9$. Bob has sent a message to Alice. The ciphertext he has sent to Alice is $C_1 = 3$, $C_2 = 18$. What is the plaintext?

$C_1 = 3$

$C_2 = 18$

$K = C_1^{X_A} \bmod q$

$= 3^9 \bmod 31$

$= 29$

$M = K^{-1} \times C_2 \bmod q$

$15 \times 29 - 14 \times 31 = 1 \bmod 31$

$15 \times 29 \equiv 1 \bmod 31$

$K^{-1} = 15$

$M = 15 \times 18 \bmod 31$

$\equiv 22 \bmod 31$

$31 = 1 \times 29 + 2$

$29 = 14 \times 2 + 1$

$29 - 14 \times 2 = 1$

$29 - 14(31 - 29) = 1$

$29 - 14 \times 31 + 14 \times 29 = 1$

$15 \times 29 - 14 \times 31 = 1$

7) (12 pts) Write a short brute force function in C below so that it returns 1 if its input parameter g is a generator mod p, and returns 0 otherwise. You may assume that p is a prime, $p < 10^4$ and that $1 < g < p-1$.

```
// Returns 1 if g is a generator mod p, 0 otherwise.
int isGenerator(int g, int p) {
    int res = g;
    for (int i = 0; i<p-2; i++) {
        if (res == 1) return 0;
        res = (res * g) % p;
    }
    return 1;
}
```