CIS 3362 Quiz #4: Number Theory, Diffie-Hellman, RSA, El-Gamal Solutions
Date: 11/9/2022

1) (5 pts) Determine the prime factorization of 205,876,800.

$205876800 = 100 \times 2058768 = (2^2)(5^2) \times (2^4)(128673)$
$= (2^6)(5^2) \times (3^2)(14297)$
$= (2^6)(3^2)(5^2) \times (17)(841)$

Here we use the calculator to divide out as many copies of 2, 3, and 5. Then we search more primes until we find that 17 divides evenly into 14297. Finally, we find that the prime 29 divides into 841 (twice).

$2^6 3^2 5^2 17^1 29^2$

Grading: 1 pt per term

2) (5 pts) Determine φ(205,876,800) **and give your answer in prime factorized form.**

$\varphi(2^6 3^2 5^2 17^1 29^2) = (2^6 - 2^5)(3^2 - 3^1)(5^2 - 5^1)(17 - 1)(29^2 - 29^1)$
$= 32 \times 6 \times 20 \times 16 \times 29 \times (29 - 1)$
$= 2^5 \times 2 \times 3 \times 2^2 \times 5 \times 2^4 \times 29 \times 2^2 \times 7$
$= 2^{14} \times 3^1 \times 5^1 \times 7^1 \times 29^1$

$2^{14} 3^1 5^1 7^1 29^1$

Grading: 1 pt write down phi formula in terms of their answer from #1
4 pts getting that result to prime factorized form, give partial as needed

3) (5 pts) Determine the remainder when 22^{3068} is divided by 439. Note that 439 is prime. **For full credit use Fermat's Theorem.**

Based on Fermat's Theorem, note that $22^{438} \equiv 1 \pmod{439}$.
Also note that 3068 = 7 x 438 + 2. Using this information, we have:

$22^{3068} = 22^{438(7)+2} = (22^{438})^7(22^2) \equiv 1^7 \times 484 \equiv 45 \pmod{439}$

It follows that the desired remainder is **45.**

Grading: 2 pts for exponent split (7 x 438 + 2)
2 pts for substituting 1 for Euler's and revealing 22^2
1 pt to reduce 484 to correct answer.

4) (5 pts) Consider running the Miller-Rabin primality test with the input n = 417. In the algorithm, a random value of a is chosen and exponentiated. Over the course of the algorithm, a is potentially raised to five different powers. What are those powers? (Note: In the stated algorithm, these values are somewhat hidden, so you have to use logic to deduce them.)

n-1 = 416, repeatedly divide this by 2:

416 → 208 → 104 → 52 → 26 → 13

The five powers the algorithm raises the random value a to is:

13, 26, 52, 104, and 208.

Grading: 1 pt for each correct response.

5) (6 pts) Use the Fermat Factoring Method to factor 53,387. Please fill out the table below and then provide the desired factorization below. You are supposed to provide an intermediate form first in the blanks below, then simplify it to the product of two odd integers on the right. Note: More rows than necessary are provided.

x	x^2 - 53387	Perfect Square?
232	437	No
233	902	No
234	1369	Yes (37)

53,387 = (234 – 37) x (234 + 37) = 197 x 271

Grading: 1 pt for each row that is correct, 1 pt for 234-37, 1 pt for 234+37, 1 pt for final answer.

6) (6 pts) In the Diffie-Hellman Key Exchange, the public elements are p = 47 and g = 5. Let Alice pick secret key a = 10, and Bob pick secret key b = 14. **Using Fermat's Theorem to reduce the work, determine the shared secret key they will pick.** (Your answer must be an integer in between 1 and 46, inclusive.)

The secret key exchanged in Diffe-Hellman is g^{ab} mod p. In this case, the value is $5^{10(14)}$ mod 47. Remember that 47 is prime, so $5^{46} \equiv 1 \pmod{47}$. It follows that:

$5^{10(14)} = 5^{140} = 5^{46x3 + 2} = (5^{46})^3 \times 5^2 \equiv 1^3 \times 5^2 \equiv 25 \pmod{47}$

Shared Key = 25

Grading: If they do the whole process, then 3 pts for finding 5^{10} or 5^{14} and then another 3 pts for taking that value and raising it to the "opposite" exponent.

If they do it like I did above, 2 pts for identifying what the key will be, 2 pts for using Fermat's to reduce it, 2 pts for the answer.

7) (8 pts) In an RSA system, n = 187 and e = 27, what is d? **Please express your answer as the smallest possible positive integer.**

We must first factor n = 187 = 11 x 17. It follows that $\varphi(187) = (11 - 1)(17 - 1) = 160$. We know that $d = e^{-1} \bmod 160$, thus we must determine $27^{-1} \bmod 160$ via the Extended Euclidean Algorithm:

160 = 5 x 27 + 25
27 = 1 x 25 + 2
25 = 12 x 2 + 1

25 – 12 x 2 = 1
25 – 12(27 – 25) = 1
25 – 12 x 27 + 12 x 25 = 1
13 x 25 – 12 x 27 = 1
13(160 – 5 x 27) – 12 x 27 = 1
13 x 160 – 65 x 27 – 12 x 27 = 1
13 x 160 – 77 x 27 = 1

Taking this equation mod 160 we find

$-77 \times 27 \equiv 1 \pmod{160}$, since the first term is equivalent to 0 mod 160.

It follows that $27^{-1} \equiv -77 \equiv 83 \pmod{160}$.

Indeed, $83 \times 27 = 2241$ and $2241 \equiv 1 \pmod{160}$.

Thus **d = 83.**

Grading: 1 pt – factorize n
1 pt – phi(n)
2 pts – Euclidean Algorithm
3 pts – Extended Euclidean
1 pt – Extracting Answer

If n isn't factorized properly, automatic 0/8. If Euclidean is incorrect, max 3/8.

8) (9 pts) In an El-Gamal cryptosystem, the public elements are q = 29, α = 8 and the Alice's private key is X_A = 12. Bob has sent the following ciphertext to Alice: (10, 4). Decrypt the ciphertext to reveal the plaintext. Since the plaintext number is in between 0 and 25, please convert this back to a single letter, using the A = 0, B = 1, etc. convention. **Please show each step of the process, in particular: (1) The calculation of K, (2) The calculation of K^{-1} and (3) Revealing the plaintext value → letter.**

(1) $K = (C_1)^{XA} = 10^{12} \bmod 29 =$ **20** via calculator. (Alternatively, by hand $10^2 = 13 \bmod 29$, $10^4 = -5 \pmod{29}$ and $10^8 = 25 \pmod{29}$, then $10^{12} = 10^8 10^4 \equiv 25(-5) \equiv -125 \equiv 20 \pmod{29}$

(2) We calculate $K^{-1} \bmod q$, via the Extended Euclidean Algorithm:

$29 = 1 \times 20 + 9$
$20 = 2 \times 9 + 2$
$9 = 4 \times 2 + 1$

$9 - 4 \times 2 = 1$
$9 - 4(20 - 2 \times 9) = 1$
$9 - 4 \times 20 + 8 \times 9 = 1$
$9 \times 9 - 4 \times 20 = 1$
$9(29 - 20) - 4 \times 20 = 1$
$9 \times 29 - 9 \times 20 - 4 \times 20 = 1$
$9 \times 29 - 13 \times 20 = 1$
Taking this equation mod 29, we find that $K^{-1} \equiv -13 \equiv 16 \pmod{29}$

(3) $P = K^{-1}C_2 = 16 \times 4 = 64 \equiv$ **6 (mod 29), letter G.**

M = G (or 6)

Grading: 3 pts for K, 5 pts for K^{-1} (note -13 is perfectly fine here), 1 pt to extract answer. Give full credit for either G or 6.

8) (1 pt) What sound does a Nestle Crunch Bar make when you bite into it?

Crunch (Give to all)