E. Dummit's Math 3527 $\sim$ Number Theory I, Spring 2023 $\sim$ Homework 6, due Tue Feb 21st.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Submit scans of your responses via Canvas.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Consider the RSA cryptosystem with key $N = 1\,085\,444\,233 = 31907 \cdot 34019$ and encryption exponent $e = 5$.
   (a) Encrypt the plaintext $m = 277\,891\,194$.
   (b) Find a decryption exponent d.
   (c) Decrypt the ciphertext $c = 878\,460\,400$.

---

2. Eve intercepts a 23-character text message with standard encoding (**a** = 00, **b** = 01, ... , **z** = 25) that was encrypted using RSA. Decrypt the message, given that

$$\begin{aligned} N &= 31894932850759195319489898033516954767432511 23 \\ e &= 65537 \\ c &= 29590532787139612859373394299869430398614231 95. \end{aligned}$$

---

3. Peggy and Victor are performing a Rabin zero-knowledge protocol to prove that Peggy knows s, where

$$\begin{aligned} N &= 488419441734583556321985415212612123740359939381088965700730231638206554681394177 \\ s^2 \pmod{N} &= 364578471930898294925524638136447727960007605573204140075455802888652544203808336. \end{aligned}$$

Peggy and Victor perform five rounds. Peggy sends Victor

$$\begin{aligned} u_1^2 &= 419987940537002829673554859623446087647247049378701209589622515994832674140645748 \\ u_2^2 &= 270893145623915322344834242328268768371424519375297223857305039560421032101793802 \\ u_3^2 &= 001204179001250513038323769136188667129468312291612708387897338022926559640599640 \\ u_4^2 &= 295360259330799676568102779994887111797263481168605647699269117672956353312755331 \\ u_5^2 &= 076085193608240660534079611034851894964763400993326547711532912132418924025617595 \end{aligned}$$

and Victor asks for the values u_1, su_2, su_3, su_4, u_5. Peggy responds with

$$\begin{aligned} u_1 &= 368836285783665928691160226566669484193845816214794656578305054442600293140251910 \\ su_2 &= 061162076090849776429311938634702834494489117638106960807555056103441302535633013 \\ su_3 &= 187951496312843107888323763535831510839656637929611417672687000373287147716755997 \\ su_4 &= 174908257541270590422202403049766598633440061550219493518183063157021792026188460 \\ u_5 &= 018020803226473941195493125743250937332254656547401271200890367477647082876441426 \end{aligned}$$

Does Peggy pass each test? What is the probability that Eve could pass each test if she didn't know s?

---

4. Alice sends an identical message with standard encoding (**a** = 00, **b** = 01, ... , **z** = 25) via RSA to each of Bob, Carol, and David. Each of Bob's, Carol's, and David's RSA public keys use $e = 3$, and their values of N are, respectively,

$$\begin{aligned} N_B &= 497034079788721357683691509517371946038416630529869382475111571267946359212776 19 \\ N_C &= 483945857851267527600982229424337545187725065744820680799879340349812157304532 93 \\ N_D &= 370484665818424219450815371720987260130706712800956432793614072604343951867522 67. \end{aligned}$$

Eve intercepts the three ciphertexts

$$\begin{aligned} c_B &= 059053643854662862955862510252376689384721908551323589669577289643236066344002 51 \\ c_C &= 211382204869611464462066174828118505616297676389940822011119788526766050860818 07 \\ c_D &= 271571254779844048794310197802881273194838250295438487672807386626830830149392 18. \end{aligned}$$

Determine Alice's original message.

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

5. Eve wants to decipher the ciphertext c that Alice sent Bob using Bob's RSA key (N, e). Eve manages to sneak in and use Bob's decryption computer. Luckily, Bob has programmed his computer to remember all of the ciphertexts it has decoded and not allow them to be decoded again, so Eve cannot ask it to decipher the message c. Instead, she asks the computer to decipher the message $2^e c$, yielding the deciphered message w. She can use w to find Alice's original plaintext m very quickly: how?

---

6. Bob and his twin brother Rob share the same 4096-bit RSA modulus N, but use different encryption exponents: Bob uses $e_B = 3$ while Rob uses $e_R = 17$. Alice sends the same plaintext message m to Bob and Rob, encoded using their respective keys, so the ciphertexts are

$$\begin{aligned} c_B &\equiv m^3 \pmod{N} \\ c_R &\equiv m^{17} \pmod{N}. \end{aligned}$$

Explain how, if Eve intercepts both ciphertexts, she can recover the original message m without having to factor N. [Hint: Write m in terms of m^3 and m^{17}.]

---

7. Peggy wants to convince Victor that she knows a secret s, so she publishes her Rabin key $N = pq$ along with $s^2 \pmod{N}$ as usual. However, she proposes a modification of the Rabin zero-knowledge protocol to have only two rounds of interaction: Peggy chooses a random unit u modulo N, Victor then asks her for either u or su modulo N, Peggy sends him the value u^2 along with the quantity he requested, and then Victor then compares the square of his requested quantity to u^2 or $u^2 s^2$.

   (a) Explain how Eve, who only knows (N, s^2) but not s, can pass the test if Victor asks for u.

   (b) Explain how Eve, who only knows (N, s^2) but not s, can pass the test if Victor asks for su.

   (c) Should Victor accept Peggy's modification of the Rabin zero-knowledge protocol? Explain.

---

8. Recall that the Lucas primality criterion says that if $a^{m-1} \equiv 1 \pmod{m}$ and $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m - 1$, then m is prime.

   (a) Use the Lucas primality criterion to show that 1013 is prime, and then establish that 2027 is prime. [Hint: Try $a = 7$ for both.]

   (b) Use the Lucas primality criterion with $a = 10$ to show that the integer

   $N = 843156784620274963828079044664499378320177127026840734436833335222593049312927235387489615873$

   is prime. (You don't need to write all the results of the modular exponentiations, but give at least a few digits.)
