E. Dummit's Math 3527 ~ Number Theory 1, Spring 2024 ~ Homework 6, due Fri Mar 1st.

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 $N = 1085444233 = 31907 \cdot 34019$ and encryption exponent $e = 3$.
   (a) Encrypt the plaintext $m = 277891194$.
   (b) Find a decryption exponent d.
   (c) Decrypt the ciphertext $c = 878460400$.

---

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

$$\begin{aligned} N &= 3189493285075919531948989803351695476743251123 \\ e &= 65537 \\ c &= 08101236748877358034719518790218439426777169 07. \end{aligned}$$

---

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

$$\begin{aligned} N_B &= 4970340797887213576836915095173719460384166305298693824751115712679463592127 7619 \\ N_C &= 4839458578512675276009822294243375451877250657448206807998793403498121573045329 3 \\ N_D &= 3704846658184242194508153717209872601307067128009564327936140726043439518675226 7. \end{aligned}$$

Eve intercepts the three ciphertexts

$$\begin{aligned} c_B &= 2578456526235772579773336162396433038740488653746000680372087663856534625686 1433 \\ c_C &= 8591142161833783340323034144110437060699871009667449419814424711743005011401597 \\ c_D &= 1404133459156814820593564484537059620604464464240217072055424091363336330235150 3. \end{aligned}$$

Determine Alice's original message.

---

4. Two of the following six integers are prime and the other four are composite:

$$\begin{aligned} N_1 &= 1474512288873635866253234569665259057209898423127605097759586627754595366776247 41 \\ N_2 &= 1817244867326073742350344013444399312701451415653728743813506462766327663289692 81 \\ N_3 &= 2584241267401783521281003707368899068176075180868066327520387587885557043046046 49 \\ N_4 &= 3242346579283470511231132320234097102340123897512398471203984719176656555812003 39 \\ N_5 &= 4088699711643282475242654505838239304344068443031428168413518794395448186857028 41 \\ N_6 &= 5424081846349432576726988349174046115422482288733374593682106249104069375829420 97 \end{aligned}$$

   (a) Try the Fermat test with $a = 2, 3, 5$ for each of these integers. (Stop if you find the integer is composite.)
   (b) Try the Miller-Rabin test with $a = 2, 3, 5$ for each of the integers remaining after part (a). (Stop if you find the integer is composite.)
   (c) Your results from parts (a)-(b) should have identified the four composite numbers. Why don't the results prove that the remaining two integers are actually prime?

---

5. 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?

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

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. 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?

---

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: you can just give the first three and last three digits of each.)
