E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ Homework 6, due Wed Feb 19th.

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. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Note: For any integers with more than 10 digits appearing in your solution, you may omit everything except the first 5 and last 5 digits. Thus, in place of 6^{100} you may write $65331 \cdots 77376$.

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

1. Consider the Rabin cryptosystem with key $N = 1\,359\,692\,821 = 32359 \cdot 42019$.
   (a) Encode the plaintext $m = 144\,920\,592$.
   (b) Find the four decodings of the ciphertext $c = 823\,845\,737$.

---

2. Consider the RSA cryptosystem with key $N = 1\,085\,444\,233 = 31907 \cdot 34019$ and encryption exponent $e = 5$.
   (a) Encrypt the plaintext $m = 744\,192\,001$.
   (b) Find a decryption exponent d.
   (c) Decrypt the ciphertext $c = 818\,460\,409$.

---

3. 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

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

---

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

$$\begin{aligned} N &= 48841944173458355632198541521261212374035993938108896570073023163820655468139417 7 \\ s^2 \pmod N &= 36457847193089829492552463813644772796000760557320414007545580288865254420380833 6. \end{aligned}$$

Peggy and Victor perform five rounds. Peggy sends Victor

$$\begin{aligned} u_1^2 &= 41998794053700282967355485962344608764724704937870120958962251599483267414064574 8 \\ u_2^2 &= 27089314562391532234483424232826876837142451937529722385730503956042103210179380 2 \\ u_3^2 &= 00120417900125051303832376913618866712946831229161270838789733802292655964059964 0 \\ u_4^2 &= 29536025933079967656810277999488711179726348116860564769926911767295635331275533 1 \\ u_5^2 &= 07608519360824066053407961103485189496476340099332654771153291213241892402561759 5 \end{aligned}$$

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

$$\begin{aligned} u_1 &= 36883628578366592869116022656666948419384581621479465657830505444260029314025191 0 \\ su_2 &= 06116207609084977642931193863470283449448911763810696080755505610344130253563301 3 \\ su_3 &= 18795149631284310788832376353583151083965663792961141767268700037328714771675599 7 \\ su_4 &= 17490825754127059042220240304976659863344006155021949351818306315702179202618846 0 \\ u_5 &= 01802080322647394119549312574325093733225465654740127120089036747764708287644142 6 \end{aligned}$$

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

---

5. Two of the following five integers are prime and the other four are composite:

$$N_1 = 14745122888736358662532345696652590572098984231276050977595866277545953667762474 1$$
$$N_2 = 18172448673260737423503440134443993127014514156537287438135064627663276632896928 1$$
$$N_3 = 25842412674017835212810037073688990681760751808680663275203875878855570430460464 9$$
$$N_4 = 32423465792834705112311323202340971023401238975123984712039847191766565558120033 9$$
$$N_5 = 40886997116432824752426545058382393043440684430314281684135187943954481868570284 1$$
$$N_6 = 54240818463494325767269883491740461154224822887333745936821062491040693758294209 7$$

(a) Try the Fermat test for each of these integers. (Stop after you find the integer is composite, or after 3 tests.)

(b) Try the Miller-Rabin test for each of the integers remaining after part (a). (Stop after you find the integer is composite, or after 3 tests.)

(c) Your results from parts (a)-(b) should have identified the four composite numbers. Why can't either of these tests prove that the remaining two integers are actually prime?

---

6. 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 David. Each of Bob's, Carol's, and David's RSA public keys use $e = 3$, and their values of N are, respectively,

$$N_B = 49703407978872135768369150951737194603841663052986938247511157126794635921277619$$
$$N_C = 48394585785126752760098222942433754518772506574482068079987934034981215730453293$$
$$N_D = 37048466581842421945081537172098726013070671280095643279361407260434395186752267.$$

Eve intercepts the three ciphertexts

$$c_B = 05905364385466286295586251025237668938472190855132358966957728964323606634400251$$
$$c_C = 21138220486961146446206617482811850561629767638994082201111978852676605086081807$$
$$c_D = 27157125477984404879431019780288127319483825029543848767280738662683083014939218.$$

Determine Alice's original message.

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

7. 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

$$c_B \equiv m^3 \pmod{N}$$
$$c_R \equiv m^{17} \pmod{N}.$$

Explain how, if Eve intercepts both ciphertexts, she can recover the original message m without having to factor N.

---

8. 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^2s^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.
