E. Dummit's Math 3527 ~ Number Theory 1, Fall 2026 ~ Homework 7, due Tue Nov 3rd.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. **Use of generative AI in any manner is not allowed on this or any other course assignments.**

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

1. Eve steals the computer Bob uses to decode messages sent via Rabin encryption. Eve asks the computer to decode the message m^2, where

   $m = 282006548310266500521595796103735803923312201934083188120704096090962921710642902266245001$

   and it returns the value

   $w = 169171645092006578241300799123542803090460485666471678762142554544526241248418101659881815.$

   Given that Bob's public key is

   $N = 340424449758185542695947485837945311955875942240280273796932383801516352255982079556106287,$

   find the two prime factors of N. (If writing by hand, you can just give the first six and last six digits of each.)

---

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

   $$\begin{aligned} N &= 513005942752265818136884766599492475562150098362 33 \\ e &= 65537 \\ c &= 425322312108240482509267912832007102477491429539 27. \end{aligned}$$

---

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,

   $$\begin{aligned} N_B &= 49703407978872135768369150951737194603841663052986938247511157126794635921277619 \\ N_C &= 48394585785126752760098222942433754518772506574482068079987934034981215730453293 \\ N_D &= 37048466581842421945081537172098726013070671280095643279361407260434395186752267. \end{aligned}$$

   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.

---

4. 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 $c_B \equiv m^3 \pmod N$ and $c_R \equiv m^{17} \pmod N$. Explain how, if Eve has both ciphertexts c_B and c_R, she can quickly find the original message m without having to factor N.

---

5. Eve wants to decipher the ciphertext c that Alice sent Bob using Bob's RSA key (N, e) so she sneaks in to 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. 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 four rounds. Peggy sends Victor

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

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

$$\begin{aligned} u_1 &= 368836285783665928691160226566669484193845816214794656578305054442600293140251910 \\ su_2 &= 061162076090849776429311938634702834494489117638106960807555056103441302535633013 \\ su_3 &= 304092941078945109049230333896497884481456911326257133666419464524378438307207 93 \\ su_4 &= 174908257541270590422202403049766598633440061550219493518183063157021792026188460 \end{aligned}$$

On which rounds does Peggy pass the test? What is the probability that Eve could pass all four rounds if she didn't know s?

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

7. In our discussion of RSA, Bob computes the decryption exponent d as the inverse of e modulo $\varphi(N)$. The goal of this problem is to show that Bob's choice is not always the smallest, as there are always several different possible decryption exponents modulo $\varphi(N)$. (We say k is a decryption exponent for e modulo N when $m^{ek} \equiv m \pmod N$ for every message m.)

   (a) Show that any integer k satisfying $k \equiv d \pmod{p-1}$ and $k \equiv d \pmod{q-1}$ is a decryption exponent. [Hint: Work mod p and mod q separately.]

   (b) Show that any decryption exponent k must satisfy $k \equiv d \pmod{p-1}$ and $k \equiv d \pmod{q-1}$. [Hint: Take m to be a primitive root mod p; you may assume one exists.]

   (c) For $N = 45737 \cdot 54377$ and $e = 3$, Bob's method gives $d = 1657960491$, but this turns out to be the third-largest of 8 possible decryption exponents. Find the smallest one.

   Remark: In general, if $\gcd(p-1, q-1) = r$, using (a) and (b) one can show that there will be r different decryption exponents modulo $\varphi(N)$.

---

8. Recall that a Carmichael number is a composite integer n such that $a^n \equiv a \pmod n$ for every integer a.

   (a) Show that any Carmichael number must be squarefree (i.e., not divisible by the square of any prime). [Hint: If p^2 divides n, try $a = p$.]

   (b) Suppose n is a Carmichael number. By part (a), we can write $n = p_1 p_2 \cdots p_d$ for distinct primes p_i. Show that for each i, $p_i - 1$ divides $n - 1$. [Hint: Take a to be a primitive root modulo p_i.]

   (c) Suppose n is composite, squarefree, and for every prime divisor p of n, $p-1$ divides $n-1$. Show that n is a Carmichael number. [Hint: Use an argument similar to the one in class used for 561.]

   (d) Conclude that n is a Carmichael number if and only if n is composite, squarefree, and for every prime divisor p of n, $p-1$ divides $n-1$. (This is known as Korselt's criterion.)

   (e) Suppose $n = pq$ is the product of two primes. Show that n is not a Carmichael number. Deduce that any Carmichael number must have at least three distinct prime factors.

   Remark: Several of the composite numbers from the factorization problems have been Carmichael numbers: this is, of course, intentional, so that the Fermat compositeness test will fail on them!
