E. Dummit's Math 3527 ∼ Number Theory I, Spring 2022 ∼ Homework 6, due Fri Feb 11th.

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 Rabin cryptosystem with key $N = 1\,359\,692\,821 = 32359 \cdot 42019$.

   (a) Encode the plaintext $m = 414\,892\,055$.

   (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 $m = 277\,891\,194$.

   (b) Find a decryption exponent d.

   (c) Decrypt the ciphertext $c = 878\,460\,400$.

---

3. 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

$$\begin{aligned} N &= 318949328507591953194898980335169547674325 1123 \\ e &= 65537 \\ c &= 2959053278713961285937339429986943039861423195. \end{aligned}$$

---

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

$$\begin{aligned} N &= 48841944173458355632198541521261212374035993938108896570073023163820655 4681394177 \\ s^2 \pmod{N} &= 36457847193089829492552463813644772796000760557320414007545580288865254420 3808336. \end{aligned}$$

Peggy and Victor perform five rounds. Peggy sends Victor

$$\begin{aligned} u_1^2 &= 4199879405370028296735548596234460876472470493787012095896225159948326741406 45748 \\ u_2^2 &= 2708931456239153223448342423282687683714245193752972238573050395604210321017 93802 \\ u_3^2 &= 0012041790012505130383237691361886671294683122916127083878973380229265596405 99640 \\ u_4^2 &= 2953602593307996765681027799948871117972634811686056476992691176729563533127 55331 \\ u_5^2 &= 0760851936082406605340796110348518949647634009933265477115329121324189240256 17595 \end{aligned}$$

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

$$\begin{aligned} u_1 &= 3688362857836659286911602265666694841938458162147946565783050544426002931402 51910 \\ su_2 &= 0611620760908497764293119386347028344944891176381069608075550561034413025356 33013 \\ su_3 &= 1879514963128431078883237635358315108396566379296114176726870003732871477167 55997 \\ su_4 &= 1749082575412705904222024030497665986334400615502194935181830631570217920261 88460 \\ u_5 &= 0180208032264739411954931257432509373322546565474012712008903674776470828764 41426 \end{aligned}$$

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

---

5. 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.

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^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.

---

8. 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 if $m^{ek} \equiv m \pmod{N}$ 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) For $N = 45737 \cdot 54377$ and $e = 3$, Bob's method gives $d = 1\,657\,960\,491$, but this turns out to be the third-largest of 8 possible decryption exponents. Find the smallest one.
   (c) Suppose that $\gcd(p-1, q-1) = r$. Show that the two simultaneous congruences

$$\begin{aligned} x &\equiv d \pmod{p-1} \\ x &\equiv d \pmod{q-1} \end{aligned}$$

   have at least r solutions modulo $\varphi(N)$. [Hint: Show that any solution to $x \equiv d \pmod{\varphi(N)/r}$ satisfies those congruences.]
   (d) Show that for any odd primes p and q, there are always at least two different decryption exponents modulo $\varphi(N)$.
