Solutions to Homework 11

Problems marked with **E** are graded on effort, which means that they are graded subjectively on the perceived effort you put into them, rather than on correctness. For bonus questions, we will not provide any insight during office hours or Piazza, and we do not guarantee anything about the difficulty of these questions. We strongly encourage you to typeset your solutions in LaTeX.

If you collaborated with someone, you must state their names. You must write your own solution and may not look at any other student's write-up.

Please note: This homework is due on Tuesday December 8, 2020!

0. If applicable, state the name(s) and uniqname(s) of your collaborator(s).

Solution:

1. What day of the week will it be 376^{376376} days after this homework is due? Show all your work, and do not use a calculator.

Solution: This homework is due on a Tuesday, so we need to determine what day of the week it is 376^{376376} days after a Tuesday. Notice that because we only care about the day of the week, changing 376^{376376} by a whole number of weeks won't change our answer. In other words, we can really answer the question "What day of the week will it be n days after a Tuesday?" and still get the right solution, as long as n is a multiple of 7 away from 376^{376376}, or equivalently if $376^{376376} \equiv n \bmod 7$. Since 7 is prime, recall from Fermat's Little Theorem that for any integer $a \neq 0$,

$$a^{7-1} \equiv 1 \bmod 7.$$

Since

$$376376 = 62729 \cdot 6 + 2,$$

this implies that

$$376^{376376} = 376^{62729 \cdot 6 + 2} = \left(376^{62729}\right)^6 \cdot 376^2 \equiv 376^2 \bmod 7.$$

Moreover, since $376 = 53 * 7 + 5$, we have that

$$376^2 \equiv 5^2 \equiv 25 \equiv 4 \bmod 7.$$

That is, we really only need to answer "What day of the week is it 4 days after a Tuesday", so our final answer is Saturday. □

E 2. In this problem, you will run through an example of RSA. Show all of your work, and do not use a calculator. Let $n = 119$ be the RSA modulus and $e = 7$ be the RSA public key.

(a) What is the private key d?

Solution: Note first that $n = 7 \cdot 17$, so $\phi(n) = (7-1)(17-1) = 96$. So we need to find a d such that $e \cdot d \equiv 1 \bmod 96$. We will use the extended Euclidean algorithm:

x	y	q	r	g	a	b
96	7	13	5	1	3	-41
7	5	1	2	1	-2	3
5	2	2	1	1	1	-2
2	1	2	0	1	0	1
1	0	$\perp$	$\perp$	1	1	0

This yields

$$\begin{aligned} 3(96) - 41(7) &= 1 \\ 3(96) - 41(7) &\equiv 1 \bmod 96 \\ -41(7) &\equiv 1 \bmod 96 \\ 7^{-1} &\equiv -41 \bmod 96 \\ 7^{-1} &\equiv 55 \bmod 96 \end{aligned}$$

So we can take $d = 55$.

We could have also found d from e and $\phi(n)$ manually using back substitution.

Here are the $x = qy + r$ equations we get as we run the Euclidean algorithm on 96 and 7.

$$\begin{aligned} 96 &= 13 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Rearranging them as $r = x - qy$ equations, we get:

$$\begin{aligned} 5 &= 96 - 13 \cdot 7 \\ 2 &= 7 - 1 \cdot 5 \\ 1 &= 5 - 2 \cdot 2 \end{aligned}$$

thus

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (96 - 13 \cdot 7) - 2 \cdot 7 = 3 \cdot 96 - 39 \cdot 7 - 2 \cdot 7 = 3 \cdot 96 - 41 \cdot 7 \end{aligned}$$

Hence, we were able to find that $1 = 3 \cdot 96 - 41 \cdot 7$. Looking at the equation with a modulus of 96, we can see that:

$$1 \equiv (3 \cdot 96) - (41 \cdot 7) \equiv -41 \cdot 7 \bmod 96$$

Hence, $7^{-1} \equiv -41 \equiv 55 \bmod 96$

(b) Sign the message $m = 4$.

Solution: Given a message m, the signature would be $(m, m^d \mod n)$.
First we calculate consecutive powers of 4:

$$\begin{aligned}
4^{2^0} &\equiv 4 \bmod 119 \\
4^{2^1} &\equiv 16 \bmod 119 \\
4^{2^2} &\equiv 256 \equiv 18 \bmod 119 \\
4^{2^3} &\equiv 5476 \equiv 86 \bmod 119 \\
4^{2^4} &\equiv 18 \bmod 119. \\
4^{2^5} &\equiv 86 \bmod 119.
\end{aligned}$$

So,

$$\begin{aligned}
s &\equiv m^d \bmod 119 \\
&\equiv 4^{55} \bmod 119 \\
&\equiv 4^{32+16+4+2+1} \bmod 119 \\
&\equiv 4^{32} \cdot 4^{16} \cdot 4^4 \cdot 4^2 \cdot 4^1 \bmod 119 \\
&\equiv (86 \cdot 18) \cdot (18 \cdot 16) \cdot 4 \bmod 119 \\
&\equiv 1 \cdot 50 \cdot 4 \bmod 119 \\
&\equiv 200 \bmod 119 \\
&\equiv 81 \bmod 119.
\end{aligned}$$

So the message-signature pair would be $(4, 81)$.

(c) Verify that your signature from the previous part is correct.

Solution: Since $81 = 9^2$, first we calculate consecutive powers of 9:

$$\begin{aligned}
9^{2^0} &\equiv 9 \bmod 119 \\
9^{2^1} &\equiv 81 \bmod 119 \\
9^{2^2} &\equiv 6561 \equiv 16 \bmod 119 \\
9^{2^3} &\equiv 18 \bmod 119
\end{aligned}$$

So,

$$\begin{aligned} s^e &\equiv 81^7 \bmod 119 \\ &\equiv 9^{14} \bmod 119 \\ &\equiv 9^{8+4+2} \bmod 119 \\ &\equiv 9^8 \cdot 9^4 \cdot 9^2 \bmod 119 \\ &\equiv 18 \cdot 16 \cdot 81 \bmod 119 \\ &\equiv 50 \cdot 81 \bmod 119 \\ &\equiv 4 \bmod 119 \\ &\equiv m \bmod 119. \end{aligned}$$

3. Harry is brewing a secret potion as a gift for Dobby the elf who is unfortunately infamous for eavesdropping. He needs to tell Hermione to get 7 more herbs for it.

   (a) Relay this message to her by encrypting $m = 7$ with $n = 33$ and $e = 31$. That is, calculate the value of the ciphertext to be sent over to her. Show all your work.

Solution: The value of the ciphertext $c = m^e \bmod n = 7^{31} \bmod 33$.

Since

$$7^{31} = 7^{16} \cdot 7^8 \cdot 7^4 \cdot 7^2 \cdot 7^1$$

we can find this value using fast modular exponentiation as:

$$\begin{aligned} 7^2 &\equiv 7 \cdot 7 \equiv 49 && \equiv 16 \bmod 33 \\ 7^4 &\equiv 7^2 \cdot 7^2 \equiv 16 \cdot 16 \equiv 256 && \equiv 25 \bmod 33 \\ 7^8 &\equiv 7^4 \cdot 7^4 \equiv 25 \cdot 25 \equiv 625 && \equiv 31 \bmod 33 \\ 7^{16} &\equiv 7^8 \cdot 7^8 \equiv 31 \cdot 31 \equiv 961 && \equiv 4 \bmod 33 \end{aligned}$$

Hence

$$c = 7^{31} \equiv 4 \cdot 31 \cdot 25 \cdot 16 \cdot 7 \equiv 7 \bmod 33.$$

   (b) Hermione got Harry's ciphertext but she forgot her private key. Fortunately, you are her friend too and can help her recover it using the other parameters you already know (because the prime numbers used are small and so the system is easy to crack). Calculate Hermione's private key for her and help her decrypt the message. Show all your work.

Solution: We know that $n = 33$. Hence its prime factors are just $p = 11$ and $q = 3$. $\phi(n) = (p-1)(q-1) = 10 \cdot 2 = 20$.

As $e \cdot d \equiv 1 \bmod \phi(n)$, we know that d is the modular inverse of $e \bmod \phi(n) = 31 \bmod 20$.

We can (1) run the Extended Euclidean Algorithm on the inputs 20 and 31 to find d or (2) manually find it using back substitution.

Method 1

x	y	q	r	g	a	b
31	20	1	11	1	-9	14
20	11	1	9	1	5	-9
11	9	1	2	1	-4	5
9	2	4	1	1	1	-4
2	1	2	0	1	0	1
1	0	$\perp$	$\perp$	1	1	0

This yields

$$\begin{aligned} -9(31) + 14(20) &= 1 \\ -9(31) + 14(20) &\equiv 1 \bmod 20 \\ -9(31) &\equiv 1 \bmod 20 \\ 31^{-1} &\equiv -9 \bmod 20 \\ 31^{-1} &\equiv 11 \bmod 20 \end{aligned}$$

So we can take $d = 11$.

Method 2

Here are the $x = qy + r$ equations we get as we run the Euclidean algorithm on 31 and 20:

$$\begin{aligned} 31 &= 1 \cdot 20 + 11 \\ 20 &= 1 \cdot 11 + 9 \\ 11 &= 1 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

Rearranging them as $r = x - qy$ equations, we get:

$$\begin{aligned} 11 &= 31 - 1 \cdot 20 \\ 9 &= 20 - 1 \cdot 11 \\ 2 &= 11 - 1 \cdot 9 \\ 1 &= 9 - 4 \cdot 2 \end{aligned}$$

thus

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4 \cdot (11 - 1 \cdot 9) = 9 - 4 \cdot 11 + 4 \cdot 9 = 5 \cdot 9 - 4 \cdot 11 \\ &= 5 \cdot (20 - 1 \cdot 11) - 4 \cdot 11 = 5 \cdot 20 - 5 \cdot 11 - 4 \cdot 11 = 5 \cdot 20 - 9 \cdot 11 \\ &= 5 \cdot 20 - 9 \cdot (31 - 1 \cdot 20) = 5 \cdot 20 - 9 \cdot 31 + 9 \cdot 20 = 14 \cdot 20 - 9 \cdot 31 \end{aligned}$$

Hence, we were able to find that $1 = 14 \cdot 20 - 9 \cdot 31$. Looking at the equation with a modulus of 20, we can see that:

$$1 \equiv (14 \cdot 20) - (9 \cdot 31) \equiv -9 \cdot 31 \bmod 20$$

Since $-9 \equiv 11 \bmod 20$, we conclude that Hermione's private key is $d = 11$. Now we can decrypt c to find m by calculating $m = c^d \bmod n$ i,e, $7^{11} \bmod 33$. Since

$$7^{11} \equiv 7^8 \cdot 7^2 \cdot 7^1 \bmod 33,$$

using the fast modular exponentiation results from the previous part:

$$7^{11} \equiv 31 \cdot 16 \cdot 7 \equiv 7 \bmod 33.$$

That is, the message was $m = 7$.

4. Mollie and Charmee want to collaboratively write the solutions for the next 376 homework, while keeping them secret from the students. As a first step, they decide to use the Diffie-Hellman protocol with a large prime p and generator g to establish a shared key that is known only to them. Mollie chooses a random $a \in \{1, \ldots, p-1\}$ and sends $A = g^a \bmod p$ to Charmee; similarly, Charmee chooses random $b \in \{1, \ldots, p-1\}$ and sends $B = g^b \bmod p$ to Mollie. Then, they each compute $k = g^{a \cdot b} \bmod p$ as the shared key.

   However, unknown to them, a mischievous student, Malcolm, is able to eavesdrop on and also *modify* all their communications, including the values A, B they send to each other. (This is called a "Malcolm in the Middle" attack.) Specifically, Malcolm chooses an exponent $c \in \{1, \ldots, p-1\}$, and replaces both A and B with $C = g^c \bmod p$.

   (a) Assume that $p = 13$, $g = 8$, $a = 7$, $b = 9$, and $c = 3$. What is the shared key value that Mollie and Charmee were supposed to compute originally? After Malcolm's substitution, what value does Mollie compute? What value does Charmee compute?

Solution: *Note:* There is actually a small error in this problem statement. For Diffie-Hellman, we require that g is a generator of $\mathbb{Z}_p$, yet 8 is not a generator of $\mathbb{Z}_{13}$ (try to prove this!). While this doesn't affect the answer to the question, in a real world scenario, using a non-generator could make the protocol more susceptible to brute force attacks.

If Malcom were not interfering, Mollie would compute

$$A = g^a \bmod p \implies A = 8^7 \equiv 5 \bmod 13.$$

and send this to Charmee,then Charmee would compute

$$B = g^b \bmod p \implies B = 8^9 \equiv 8 \bmod 13.$$

and send this to Alice. With this, Alice can then compute the shared key as

$$k = B^a = 8^7 \equiv 5 \bmod 13$$

and Charmee can compute it as

$$k = A^b = 5^9 \equiv 5 \bmod 13.$$

If Malcom does interfere, he computes

$$C = g^c \bmod p \implies C = 8^3 \equiv 5 \bmod 13.$$

Mollie receives this (believing it came from Charmee), so Mollie computes the key as

$$k_M = C^7 = 5^7 \equiv 8 \bmod 13$$

Similarly, Charmee recieves C thinking it came from Mollie, so she computes her key as

$$k_C = C^9 = 5^9 \equiv 5 \bmod 13.$$

E (b) To privately collaborate, Mollie and Charmee plan to encrypt and send their work in progress to each other, using their shared key in an encryption scheme. Such a scheme involves an encryption algorithm Enc and a decryption algorithm Dec. The encryption algorithm takes a key and message, and outputs a ciphertext. The decryption algorithm takes a key and a ciphertext, outputs a message, and satisfies the following property: for all keys k and messages$m$,

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m.$$

Describe how Malcolm can read Mollie and Charmee's work on the solutions, *without being detected*. That is, Mollie and Charmee should be under the impression that they are communicating privately with each other, with nothing appearing out of the ordinary.

Solution: Malcolm knows the encryption and decryption algorithms Enc and Dec (by Kerckhoff's Principle). As well, since

$$k_M = C^a = (g^c)^a = (g^a)^c \equiv A^c \bmod p,$$

and Malcom knows A, c, and p, he can compute k_M. Similarly, he can compute

$$k_C = B^c \bmod p.$$

Whenever Mollie encrypts a message m and sends $m' = \mathsf{Enc}(k_M, m)$ over the network, Malcolm can then intercept and compute the message $\mathsf{Dec}(k_M, m') = m$. Then, Malcolm can re-encrypt with the key that Charmee expects, sending $m'' = \mathsf{Enc}(k_C, m)$ to Charmee, who will compute $\mathsf{Dec}(k_C, m'') = m$, thus receiving the message intended for her.

Symmetrically, whenever Charmee encrypts a message m and sends $m' = \mathsf{Enc}(k_C, m)$, Malcolm can intercept m', compute the message $\mathsf{Dec}(k_C, m') = m$, and send $m'' = \mathsf{Enc}(k_M, m)$ to Mollie. Then Mollie will compute $\mathsf{Dec}(k_M, m'') = m$, thus receiving the message intended for her.

As long as Malcolm always performs these translation steps, any (encrypted) message sent from Mollie or Charmee will reach the other, and will appear to have been sent directly from the other part. Yet Malcolm will be able to read all of the messages.

5. A long time ago in a galaxy far, far away, on the planet Tatooine, you meet a mysterious man named "Ben" who asks you to decrypt some of the Galactic Empire's transmissions. Having previously spied on the Empire, you know that it uses the Caesar Cipher to encrypt messages, but you do not know the key—nor do you even know what language the Empire uses!

   Your helpful protocol droid, 2FA, informs you that the Empire's alphabet is

   $$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

   and that any well-formed message adheres to the following rule:

   the sum (mod 376) of the digits of any message always equals 254.

   For instance, 281 would not be a well-formed message, because the sum (mod 376) of the digits is 11, not 254.

   (For this problem you may use a computer, but please include an explanation of what you did and explain why the answer you obtained is correct.)

   (a) Your first mission is to decrypt the following ciphertext:

   $$95999876211727160327762313297628160376000327287 7.$$

   Determine what message it encrypts, and what key the Empire used.

   Solution: First, notice that there are only 10 keys to test because the key is an element of the alphabet $\{0, \ldots, 9\}$. Because the keyspace is small, we can simply decrypt the ciphertext with each candidate key, and check which of the resulting candidate message(s) adheres to the rule for well-formed messages.

   After decrypting the ciphertext with each key, we find that the only candidate message that follows the rule comes from key $k = 4$, and is

   $$5155543287738372698332897985328472693266698384 33.$$

   (b) Later on, one of your friends, a smuggler and scoundrel named Han Duo, informs you that every message the Empire sends can be split into pairs of digits that, when interpreted as two-digit decimal numbers, are the values of characters in ASCII. Use this information to interpret the message you obtained above.

   Solution: Splitting the message from part (a) into pairs of symbols, we find that the two-digit decimal numbers are

   51 55 54 32 87 73 83 72 69 83 32 89 79 85 32 84 72 69 32 66 69 83 84 33.

   In ASCII, the corresponding string is

   376 WISHES YOU THE BEST!