Fall 2021 CIS 3362 Homework #6: Public Key Encryption Solutions
Written by Zachariah Abueg

1) In the Diffie-Hellman Key Exchange, let the public keys be p = 53, g = 12, and the secret keys be a = 24 and b = 43, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share? Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

Solution

In the Diffie-Hellman Key Exchange, Alice sends Bob $g^a \pmod p$, Bob sends Alice $g^b \pmod p$, and their shared secret key is $(g^a)^b = (g^b)^a \pmod p$.

Hence, Alice sends Bob $g^a = 12^{24} \pmod{53}$, Bob sends Alice $g^b = 12^{43} \pmod{53}$, and their shared secret key is $(g^a)^b = (12^{24})^{43} = (12^{43})^{24} = (g^b)^a \pmod{53}$. We will use fast modular exponentiation to find these values.

Let's first find what Alice sends to Bob: $12^{24} \pmod{53}$. We begin with $12^2 \pmod{53}$ and continually square our values.

$12^2 = 144 \equiv 38 \pmod{53}$
$12^4 = (12^2)^2 \equiv 38^2 = 1444 \equiv 13 \pmod{53}$
$12^8 = (12^4)^2 \equiv 13^2 = 169 \equiv 10 \pmod{53}$

Now, notice that $12^8 \equiv 10 \pmod{53}$. We *could* keep squaring, finding 12^{16} next and then multiplying $12^{16} \times 12^8$ to get $12^{16+8} = 12^{24}$. However, notice that 12^{24} is just 12^8 cubed: $(12^8)^3 = 12^{8\times3} = 12^{24}$. This lets us do only one more operation rather than two! Furthermore, $12^8 \equiv 10$ is the smallest value we've gotten so far, so cubing it will give us something relatively small. Thus, we use this trick and get

$$12^{24} = (12^8)^3 \equiv 10^3 = 1000 \equiv 46 \pmod{53}.$$

So Alice sends Bob **46 (mod 53)**.

Now let's find what Bob sends to Alice: $12^{43} \pmod{53}$. We will use the calculations from $12^{24} \pmod{53}$ above to do this in one line:

$$12^{43} = 12^{24+8+8+2+1} = 12^{24} \times 12^8 \times 12^8 \times 12^2 \times 12^1 \equiv 46 \times 10 \times 10 \times 38 \times 12 = 2097600 \equiv 19 \pmod{53}.$$

So Bob sends Alice **19 (mod 53)**.

Finally, let's calculate the shared key. We could choose to calculate either $(12^{24})^{43}$ or $(12^{43})^{24} \pmod{53}$. Since the second one, $(12^{43})^{24}$, has the smaller outside exponent, it will probably take fewer calculations, so let's go with that. Since $(12^{43})^{24} \equiv 19^{24} \pmod{53}$, we have

19^{24} (mod 53):
$19^2 = 361 \equiv 43 \equiv -10 \pmod{53}$
$19^4 = (19^2)^2 \equiv (-10)^2 = 100 \equiv 47 \equiv -6 \pmod{53}$
$19^8 = (19^4)^2 \equiv (-6)^2 = 36 \pmod{53}$

Going with the same trick we did for 12^{24} (mod 53), we will cube 19^8 to get

$19^{24} = (19^8)^3 \equiv 36^3 = 46656 \equiv 16 \pmod{53}$.

Thus, Alice and Bob's shared secret key is **16 (mod 53)**.

2) In an RSA scheme, p = 41, q = 17 and e = 543. What is d?

Solution
In RSA, the integer d represents the private key and its value is $d = e^{-1} \pmod{\varphi(n)}$, where $n = pq$ for two primes p, q.

We begin by calculating $\varphi(n)$, which is easily found given p and q:

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

With $p = 41$ and $q = 17$, we have $\varphi(n) = (41-1)(17-1) = 40 \times 16 = 640$.

Thus, we are calculating $d = e^{-1} \pmod{\varphi(n)} = 543^{-1} \pmod{640}$, or the positive integer d such that $543d \equiv 1 \pmod{640}$. We begin by doing the extended Euclidean algorithm on 640 and 543:

$640 = 1 \times 543 + 97$
$543 = 5 \times 97 + 58$
$97 = 1 \times 58 + 39$
$58 = 1 \times 39 + 19$
$39 = 2 \times 19 + 1$

$1 = 39 - 2 \times 19$
$= 39 - 2 \times (58 - 39)$
$= 39 - 2 \times 58 + 2 \times 39$
$= 3 \times 39 - 2 \times 58$
$= 3 \times (97 - 58) - 2 \times 58$
$= 3 \times 97 - 3 \times 58 - 2 \times 58$
$= 3 \times 97 - 5 \times 58$
$= 3 \times 97 - 5 \times (543 - 5 \times 97)$
$= 3 \times 97 - 5 \times 543 + 25 \times 97$
$= 28 \times 97 - 5 \times 543$
$= 28 \times (640 - 543) - 5 \times 543$
$= 28 \times 640 - 28 \times 543 - 5 \times 543$
$= 28 \times 640 - 33 \times 543$

That is, $28 \times 640 - 33 \times 543 = 1$. Now, remember that we want to find the positive integer d such that $543d \equiv 1 \pmod{640}$. With that in mind, let's take the previous equation (mod 640):

$28 \times 640 - 33 \times 543 = 1 \pmod{640}$
$28 \times 0 - 33 \times 543 = 1 \equiv 1 \pmod{640}$
$-33 \times 543 \equiv 1 \pmod{640}$,

where the second step follows because $a \times b \equiv a \times 0 \pmod{b}$ for any integers a, b.

Now, as it stands, we have an equation of the form $543d \equiv 1 \pmod{640}$, where $d = -33$. However, remember that we want to find the *positive* integer d satisfying this equation. Hence, we remap $-33 \pmod{640}$ to a positive integer by adding 640 to -33 once:

$-33 \times 543 \equiv 1 \pmod{640}$
$607 \times 543 \equiv 1 \pmod{640}$

Now, we have our positive integer d satisfying $543d \equiv 1 \pmod{643}$: $\boldsymbol{d = 607.}$

3) In elliptic curve arithmetic, what is the sum of the points (7, 9), (15, 29) on the curve $E_{41}(3, 4)$?

Solution

Let $P = (x_P, y_P) = (7, 9)$ and $Q = (x_Q, y_Q) = (15, 29)$. We are working on the curve $E_p(a, b) = E_{41}(3, 4)$, which means that the equation for the elliptic curve is $y^2 = x^3 + 3x + 4 \pmod{41}$. We will find $P + Q = R = (x_R, y_R)$.

First, we will calculate λ. When we have $P \neq Q$ and are finding $P + Q$, the equation for λ is $\lambda = \frac{y_Q - y_P}{x_Q - x_P} \pmod{p}$. This gives us

$$\lambda = \frac{29-9}{15-7} = \frac{20}{8} \pmod{41}.$$

Now, remember that division in modular arithmetic is not the same as division in real-number arithmetic: when we are dividing in modular arithmetic, we are multiplying by the modular inverse. So here, to divide 20 by 8, we will multiply 20 by the modular inverse of 8 (mod 41):

$$\lambda = \frac{20}{8} = 20 \times 8^{-1} \pmod{41}.$$

We will find $8^{-1} \pmod{41}$, or the positive integer x such that $8x \equiv 1 \pmod{41}$, using the Extended Euclidean Algorithm:

$41 = 5 \times 8 + 1$

$1 = 41 - 5 \times 8$

That is, $41 - 5 \times 8 = 1$. Now, remember that we want to find the positive integer x such that $8x \equiv 1 \pmod{41}$. With that in mind, let's take the previous equation (mod 41):

$41 - 5 \times 8 = 1 \pmod{41}$
$0 - 5 \times 8 \equiv 1 \pmod{41}$
$-5 \times 8 \equiv 1 \pmod{41}$,

where the second step follows because $a + b \equiv 0 + b \pmod{a}$ for any integers a, b.

Now, as it stands, we have an equation of the form $8x \equiv 1 \pmod{41}$, where $x = -5$. However, remember that we want to find the *positive* integer x satisfying this equation. Hence, we remap $-5 \pmod{41}$ to a positive integer by adding 41 to -5 once:

$-5 \times 8 \equiv 1 \pmod{41}$
$36 \times 8 \equiv 1 \pmod{41}$

Now, we have our positive integer x satisfying $8x \equiv 1 \pmod{41}$: $x = 36$. This gives us $8^{-1} \pmod{41} = 36$. Hence,

$$\lambda = 20 \times 8^{-1} = 20 \times 36 = 720 \equiv 23 \pmod{41}.$$

Finally, we calculate the coordinates of the new point, $R = (x_R, y_R)$. The equations for them are

$$x_R = \lambda^2 - x_P - x_Q \pmod{p}$$
$$y_R = \lambda(x_P - x_R) - y_P \pmod{p}$$

With $p = 41$, $\lambda \equiv 23$, $P = (x_P, y_P) = (7, 9)$, and $Q = (x_Q, y_Q) = (15, 29)$, we have

$$x_R = 23^2 - 7 - 15 = 507 \equiv 15 \pmod{41}$$
$$y_R = 23 \times (7 - 15) - 9 = -193 \equiv 12 \pmod{41}$$

And this is our desired point: $(7, 9) + (15, 29) = \underline{(\mathbf{15, 12})}$ on the curve $E_{41}(3, 4)$.

4) In elliptic curve arithmetic, calculate 4 x (5, 12) on the curve $E_{41}(3, 4)$? (Note: This will require you to multiply by two twice.)

Solution

In elliptic curve arithmetic, multiplying a point by 4 is equivalent to adding that point to itself twice: $P + P = 2P$, and $2P + 2P = 4P$.

Let $P = (x_P, y_P) = (5, 12)$. We are working on the curve $E_p(a, b) = E_{41}(3, 4)$, which means that the equation for the elliptic curve is $y^2 = x^3 + 3x + 4 \pmod{41}$.

First, we will calculate λ. When we have $P = Q$ and are adding a point P to itself, the equation for λ is $\lambda = \frac{3{x_P}^2 + a}{2y_P} \pmod{p}$. This gives us

$$\lambda = \frac{3 \times 5^2 + 3}{2 \times 12} = \frac{78}{24} \equiv \frac{37}{24} \pmod{41}.$$

Now, remember that division in modular arithmetic is not the same as division in real-number arithmetic: when we are dividing in modular arithmetic, we are multiplying by the modular inverse. So here, to divide 37 by 24, we will multiply 37 by the modular inverse of 24 (mod 41):

$$\lambda = \frac{37}{24} = 37 \times 24^{-1} \pmod{41}.$$

Now we will find $24^{-1} \pmod{41}$, or the positive integer x such that $24x \equiv 1 \pmod{41}$, using the Extended Euclidean Algorithm:

$41 = 1 \times 24 + 17$
$24 = 1 \times 17 + 7$
$17 = 2 \times 7 + 3$
$7 = 2 \times 3 + 1$

$1 = 7 - 2 \times 3$
$= 7 - 2 \times (17 - 2 \times 7)$
$= 7 - 2 \times 17 + 4 \times 7$
$= 5 \times 7 - 2 \times 17$
$= 5 \times (24 - 17) - 2 \times 17$
$= 5 \times 24 - 5 \times 17 - 2 \times 17$
$= 5 \times 24 - 7 \times 17$
$= 5 \times 24 - 7 \times (41 - 24)$
$= 5 \times 24 - 7 \times 41 + 7 \times 24$
$= 12 \times 24 - 7 \times 41$

That is, $12 \times 24 - 7 \times 41 = 1$. Now, remember that we want to find the positive integer x such that $24x \equiv 1 \pmod{41}$. With that in mind, let's take the previous equation (mod 41):

$12 \times 24 - 7 \times 41 = 1 \pmod{41}$
$12 \times 24 - 7 \times 0 \equiv 1 \pmod{41}$
$12 \times 24 \equiv 1 \pmod{41}$,

where the second step follows because $a \times b \equiv a \times 0 \pmod{b}$ for any integers a, b.

We now see that we have the integer $x = 12$ satisfying the equation $24x \equiv 1 \pmod{41}$. This gives us $24^{-1} \pmod{41} = 12$. Hence,

$$\lambda = 37 \times 24^{-1} = 37 \times 12 = 444 \equiv 34 \pmod{41}.$$

Now, we calculate the coordinates of the new point, $2P = (x_{2P}, y_{2P})$. The equations for them are

$$x_{2P} = \lambda^2 - x_P - x_Q \pmod{p}$$
$$y_{2P} = \lambda(x_P - x_{2P}) - y_P \pmod{p}$$

Keep in mind that in this case, since we are adding P to itself, $x_P = x_Q$ and $y_P = y_Q$.

With $p = 41$, $\lambda \equiv 34$, and $P = (x_P, y_P) = (5, 12) = (x_Q, y_Q) = Q$, we have

$$x_{2P} = 34^2 - 5 - 5 = 1146 \equiv 39 \text{ (mod 41)}$$
$$y_{2P} = 34 \times (5 - 39) - 12 = -1168 \equiv 21 \text{ (mod 41)}$$

And thus, $2P = P + P = (39, 21)$. Now, we add $2P$ to itself to obtain $4P$, going through the same process. We have $2P = (x_{2P}, y_{2P}) = (39, 21)$ and $a = 3$ (which has not changed – we are still on the same elliptic curve), and we will calculate $2P + 2P = 4P$.

First, we begin with λ:

$$\lambda = \frac{3 \times 39^2 + 3}{2 \times 21} = \frac{4566}{42} \equiv \frac{15}{1} = 15 \times 1^{-1} \text{ (mod 41)}.$$

We use the Extended Eucli—oh wait, we don't have to do that?

Yes: notice that 1^{-1} (mod 41) is just the positive integer x that satisfies $1x \equiv 1$ (mod 41). But that integer is simply $x = 1$! (Technically the set of all integers x with $x = 41n + 1$ for all natural numbers n satisfy this equation: $x = 1, 42, 83$, and so on. However, we always want the smallest such positive x. Thus, we have $x = 1$).

Thus,

$$\lambda = 15 \times 1^{-1} = 15 \times 1 = 15 \text{ (mod 41)}.$$

Finally, we calculate the coordinates of the new point, $4P = (x_{4P}, y_{4P})$. Our equations are

$$x_{4P} = \lambda^2 - x_{2P} - x_{2Q} \text{ (mod } p)$$
$$y_{4P} = \lambda(x_{2P} - x_{4P}) - y_{2P} \text{ (mod } p)$$

With $p = 41$, $\lambda \equiv 15$, and $2P = (x_{2P}, y_{2P}) = (39, 21) = (x_{2Q}, y_{2Q}) = 2Q$, we have

$$x_{4P} = 15^2 - 39 - 39 = 147 \equiv 24 \text{ (mod 41)}$$
$$y_{4P} = 15 \times (39 - 24) - 21 = 204 \equiv 40 \text{ (mod 41)}$$

And thus, $2P + 2P = (24, 40)$. Since $2P + 2P = 4P$, we now have our desired point: $4 \times (5, 12) = \underline{\mathbf{(24, 40)}}$ on the curve $E_{41}(3, 4)$.

5) Consider an El Gamal cryptosystem with the prime q = 37 and the primitive root a = 18. Alice picks $X_A = 13$ for her secret key. What is the public key Y_A that Alice posts? Now, consider sending the message M = 31 to Alice. Give two different ordered pairs that you could send to Alice using her public keys to encrypt M. For each, write down which value of k you picked, the corresponding value of K, as well as the cipher text, the ordered pair (C_1, C_2). Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

Solution

In the El Gamal cryptosystem, Alice's public key is $Y_A = a^{X_A} \pmod{q}$. With $a = 18$, $X_A = 13$, and $q = 37$, we have $Y_A = 18^{13} \pmod{37}$. We use fast modular exponentiation to calculate this:

$18^2 = 324 \equiv 28 \pmod{37}$
$18^4 = (18^2)^2 = 28^2 = 784 \equiv 7 \pmod{37}$

Now, notice that $18^4 \equiv 7 \pmod{37}$. We *could* keep squaring, finding 18^8 next and then multiplying $18^8 \times 18^4 \times 18^1$ to get $18^{8+4+1} = 18^{13}$. However, notice that cubing 18^4 will give us $(18^4)^3 = 18^{12}$, which is really close to 18^{13}! Furthermore, $18^4 \equiv 7$ is the smallest value we've gotten so far, so cubing it will give us something relatively small. Thus, we use this trick and get

$18^{12} = (18^4)^3 \equiv 7^3 = 343 \equiv 10 \pmod{37}$.

Finally, we multiply this by 18 to get 18^{13}:

$18^{13} = 18^{12+1} = 18^{12} \times 18^1 \equiv 10 \times 18 = 180 \equiv 32 \pmod{37}$

Thus, $Y_A = 32 \pmod{37}$. Now, we will send Alice the message $M = 31$ with two different encryptions. To encrypt the message, we pick a random k, where $1 \leq k \leq q - 1$. Since we are eventually using k as an exponent in $K = {Y_A}^k \pmod{q}$, I will pick small k to make calculations short and easy.

Let's start with $k = 2$. We first calculate $K = {Y_A}^k \pmod{q}$. With $Y_A = 32$ and $k = 2$, we have

$$K = 32^2 = 1024 \equiv 25 \pmod{37}.$$

Now, we calculate $C_1 = a^k \pmod{q}$ and $C_2 = KM \pmod{q}$. With $a = 18$, $k = 2$, $K = 25$, $M = 31$, and $q = 37$, we have

$$C_1 = 18^2 = 324 \equiv 28 \pmod{37}$$
$$C_2 = 25 \times 31 = 775 \equiv 35 \pmod{37}.$$

This gives us $C = (C_1, C_2) = (28, 35) \pmod{37}$.

Thus, with $\boldsymbol{k = 2}$, we have $\boldsymbol{C_1 = 28 \pmod{37}}$ and $\boldsymbol{C_2 = 35 \pmod{37}}$.

Now, let's pick $k = 3$. We first calculate $K = {Y_A}^k \pmod{q}$. With $Y_A = 32$ and $k = 3$, we have

$$K = 32^3 = 32768 \equiv 23 \pmod{37}.$$

Now, we calculate $C_1 = a^k \pmod{q}$ and $C_2 = KM \pmod{q}$. With $a = 18$, $k = 3$, $K = 23$, $M = 31$, and $q = 37$, we have

$$C_1 = 18^3 = 5832 \equiv 23 \pmod{37}$$
$$C_2 = 23 \times 31 = 713 \equiv 10 \pmod{37}$$

This gives us $C = (C_1, C_2) = (23, 10) \pmod{37}$.

Thus, with $\boldsymbol{k = 3}$, we have $\boldsymbol{C_1 = 23 \pmod{37}}$ and $\boldsymbol{C_2 = 10 \pmod{37}}$.

Note that these encryptions can be done with any k from 1 to $q - 1$, inclusive. Here are the correct values of K and C (mod 37) for each k from 1 to $37 - 1 = 36$, found with some quick code:

$\boldsymbol{k}$	$\boldsymbol{K}$	$\boldsymbol{C}$
1	32	(18, 30)
2	25	(28, 35)
3	23	(23, 10)
4	33	(7, 24)
5	20	(15, 28)
6	11	(11, 8)
7	19	(13, 34)
8	16	(12, 15)
9	31	(31, 36)
10	30	(3, 5)
11	35	(17, 12)
12	10	(10, 14)
13	24	(32, 4)
14	28	(21, 17)
15	8	(8, 26)
16	34	(33, 18)
17	15	(2, 21)
18	36	(36, 6)

$\boldsymbol{k}$	$\boldsymbol{K}$	$\boldsymbol{C}$
19	5	(19, 7)
20	12	(9, 2)
21	14	(14, 27)
22	4	(30, 13)
23	17	(22, 9)
24	26	(26, 29)
25	18	(24, 3)
26	21	(25, 22)
27	6	(6, 1)
28	7	(34, 32)
29	2	(20, 25)
30	27	(27, 23)
31	13	(5, 33)
32	9	(16, 20)
33	29	(29, 11)
34	3	(4, 19)
35	22	(35, 16)
36	1	(1, 31)

6) Time to break a code! This was produced using RSA2BigInt.java. Here are the public keys for the system used.

```
Public key n = 276503917826766849902006184l
Public key e = 92253545271575760672283812l
```

Here is the ciphertext to decipher:

```
195038167899690250214751691
214171160422201655779853660 2
106654869321135983523765373 8
231720262266066246658832523 2
206983403668062601872605818 0
270792048632129421613463075 3
112373083172823378545343444
152241549204075536244924875 9
231871222174753878251146491 5
226794694796500193353843562 9
```

Each number represents a block of 19 uppercase letters.

Good luck!

Arup

Solution (Written by Arup)

Use Pollard-Rho to factor n. Doing so gives:

$$n = 276503917826766849902006184l$$

$$= 36279836279899 * 76214213232259$$

Note: when I ran PollardRho.java with this value it took about 10 seconds while when I ran pollardrho.py, it took about a minute.

Now, we can calculate phi(n):

$$phi(n) = 36279836279898 * 76214213232258$$

$$= 276503917826755600497054968 4$$

Thus, we must now find

$$d = 92253545271575760672283812 1^{-1} \bmod 276503917826755600497054968 4$$

This can be done with modPow in Java, or fast modular exponentiation in Python and the Extended Euclidean Algorithm.

Doing this we find:

```
d = 123784832025427738651451630 5
```

You can also use the Python code I have posted (rsa2.py) and print d after entering in the exact values of p, q and e listed above, to get this value.

Finally, to read the message, we must take each ciphertext integer, raise it to the power d shown above, to obtain the plaintext number. Then we must convert this number to be in "base 26" revealing the message. I've edited rsa2.py to accomplish this, hardcoding p, q and d into the code, skipping the encryption part and adding a loop to process multiple blocks.

The attached edited files are solvep6.py and problem6.in (where I copied the ciphertext, adding one line which specified how many lines of input there were).

When I ran this program, I got the following plaintext:

```
GOTOROOMTHREEFOURFI
VEINHECONADESKINFRO
NTOFYOUTHEREWILLBEA
WINTERSPRINGSLIFEMA
GAZINEFORSEPTOFTHIS
YEARWITHCAROLINEWEL
LSACROSSCOUNTRYRUNN
ERONTHECOVEROPENTOP
AGESIXTYANDYOUWILLS
EETHECLUEIHIDFORYOU
```

Edited with spaces we have:

Go to room 345 in HEC. On a desh in front of you there will be a Winter Springs Life magazine for Sept. of this year with Caroline Wells, a cross country runner, on the cover. Open to page 60 and you will see the clue I hit for you.

PS. Zach let me write this one! - Arup