Written by Zachariah Abueg
11/1/20

Fall 2020 CIS 3362 Homework #6: Public Key Encryption Solutions

1) One of the primitive roots (also called generators) mod 43 is 19. There are 11 other primitive roots mod 43. One way to list these is 19^{a1} mod 43, 19^{a2} mod 43, … 19^{a12} mod 43, where 0 < a1 < a2 < … < a12. (Note: it's fairly easy to see that a1 = 1, since 19 is a primitive root.) Find the values of a10, a11 and a12 and the corresponding remainders when 19^{a10}, 19^{a11} and 19^{a12} are divided by 43. Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

Solution

These twelve exponents of 19 – $a1, a2, \dots, a12$ – are actually the twelve numbers that are coprime with $\varphi(43) = 43 - 1 = 42$: $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$. That is, if you know that 19 is a primitive root (mod 43), then 19 raised to each of the numbers that are coprime with 42 are the other primitive roots (mod 43): 19^1, 19^5, 19^{11}, …, 19^{41}.

Why is that? Where does that come from? We will prove that if p is a prime, a is a primitive root (mod p) with $1 \leq a \leq p-1$, and k is an integer with $1 \leq k \leq p-1$ such that k is coprime with $\varphi(p) = p - 1$, then a^k is a primitive root (mod p). But first, let's go over some preliminaries, all of which we will use in the proof:

(1) Recall that a primitive root r (mod a prime p) is defined to be a number $1 \leq r \leq p-1$ such that the powers of r up to $p-1$ ($r^1, r^2, \dots, r^{p-1}$) taken (mod p) generate each integer from 1 to $p-1$ exactly once. This means that if r is *not* a primitive root (mod p), then $r^1, r^2, \dots, r^{p-1}$ generates one of the integers from 1 to $p-1$ *more than* once. In other words, if r is *not* a primitive root (mod p), then there exist two numbers in the set $\{r^1, r^2, \dots, r^{p-1}\}$ that are equivalent (mod p).

Equivalently, r is defined to be a primitive root (mod p) if the smallest power of r (greater than r^0) that is equivalent to 1 (mod p) is r^{p-1}. This means that if r is *not* a primitive root (mod p), then there is an exponent q that is *less than* $p-1$ such that r^q is equivalent to 1 (mod p).

Also, we know that when we divide a number a by another number b, we get some quotient q plus a remainder m. When we're dividing two integers, we typically keep the remainder below the number we're dividing by: $0 \leq m < b$. For instance, we say 19 divided by 6 is 3 remainder 1, not 2 remainder 7. Now, another way to write this is $19 = 3 \times 6 + 1$. We can generalize this: for any two integers a and b, we can write a as an integer times b, plus another integer. Formally speaking, there exist unique integers q and m such that $a = qb + m$, where $0 \leq m < b$. If you'd like to look more into this or see a proof of it, you can search "Euclid's division lemma".

(2) Now, if r is a primitive root (mod p) and s is an integer such that $r^s \equiv 1 \pmod{p}$, then s is divisible by $p-1$. Why is this? Let's prove this, starting with the fact above: let's write s as an integer times $p-1$ plus another integer. Let q and m be integers such that $s = q(p-1) + m$, where $0 \leq m < p-1$. Then using the rules of exponents and the fact that $r^{p-1} \equiv 1 \pmod{p}$, we have $1 \equiv r^s = r^{q(p-1)+m} = (r^{p-1})^q \times r^m \equiv 1^q \times r^m = r^m \pmod{p}$, or $r^m \equiv 1 \pmod{p}$. Now, recall that r is a primitive root (mod p), so by the second definition of a primitive root above, we know that the *smallest* power of r greater than r^0 that is equivalent to 1 (mod p) is r^{p-1}. But we showed above that $r^m \equiv 1 \pmod{p}$, and m is less than $p-1$. The only way this is possible is with

$m = 0$, since we know that $0 \leq m < b$. Now, remember our ultimate goal is to show that s is divisible by $p - 1$. Going back to $s = q(p-1) + m$, we have $s = q(p-1) + 0 = q(p-1)$, or $s = q(p-1)$. In other words, s is a multiple of $p - 1$. Thus, s is divisible by $p - 1$. And thus we have shown that if r is a primitive root (mod p) and s is an integer such that $r^s \equiv 1 \pmod{p}$, then s is divisible by $p - 1$.

(3) Also, if a number $a \times b$ is divisible by another number n, then either a is divisible by n or b is divisible by n. For instance, take the fact that 3×4 is divisible by 2. Then the previous statement says that either 3 is divisible by 2 or that 4 is divisible by 2 – and indeed, 4 is divisible by 2. If you'd like to look more into this or see a proof of it, you can search "Euclid's lemma".

(4) Also, if two integers a and b are coprime, then any integer power of a is coprime with b – that is, a^m is coprime with b for any positive integer m. We can see why this is so: if two numbers a and b are coprime, then they share no common factors. Now let m be an integer and consider $a^m = \underbrace{a \times a \times \ldots \times a}_{m}$. Since a and b share no common factors, neither will $\underbrace{a \times a \times \ldots \times a}_{m}$ and b. Thus, a^m is coprime with b.

Alright, now let's jump into the proof. I will refer to these preliminaries by their numbers throughout the proof.

Proof: Suppose that p is a prime, a is a primitive root (mod p) with $1 \leq a \leq p - 1$ and that k is an integer with $1 \leq k \leq p - 1$ such that k is coprime with $\varphi(p) = p - 1$. We will prove that a^k is a primitive root (mod p) using contradiction: we will suppose that a^k is *not* a primitive root (mod p) and then, after some logical deductions, we will arrive at a contradiction, which means that our assumption that a^k is *not* a primitive root (mod p) must have been wrong, and so a^k *is*, indeed, a primitive root (mod p).

Suppose to the contrary that a^k is *not* a primitive root (mod p). Then, by (1), there exist two numbers in the set

$$\{(a^k)^1, (a^k)^2, \ldots, (a^k)^{p-1}\} = \{a^k, a^{2k}, \ldots, a^{(p-1)k}\}$$

that are equivalent (mod p). Let these two numbers be a^{ik} and a^{jk}, and assume that $i \neq j$ and $0 < i < j < p$. Then

$$\begin{aligned}
& a^{jk} \equiv a^{ik} \pmod{p} \\
\Leftrightarrow\ & a^{jk} - a^{ik} \equiv 0 \pmod{p} \\
\Leftrightarrow\ & a^{ik+jk-ik} - a^{ik} \equiv 0 \pmod{p} \\
\Leftrightarrow\ & a^{ik} \times a^{jk-ik} - a^{ik} \equiv 0 \pmod{p} \\
\Leftrightarrow\ & a^{ik}\left(a^{jk-ik} - 1\right) \equiv 0 \pmod{p}
\end{aligned}$$

By the definitions of modular arithmetic, this means that $a^{ik}\left(a^{jk-ik} - 1\right)$ is divisible by p. Then, by (3), either a^{ik} is divisible by p or $a^{jk-ik} - 1$ is divisible by p. Let's look at both cases.

Recall that a is between 1 and $p-1$, inclusive. Now, since p is prime, the only numbers that share a common factor with p and thus are *not* coprime with p are the multiples of p: $\dots, -3p, -2p, -p, 0, p, 2p, 3p, \dots$ We see that since a is between 1 and $p-1$, inclusive, a cannot be a multiple of p. Thus, a must be coprime with p. Then, by (4), $a^{ik} = \underbrace{a \times a \times \dots \times a}_{ik}$ is also coprime with p, which means that a^{ik} is *not* divisible by p.

Thus, it must be the case $a^{jk-ik} - 1$ is divisible by p. This gives us

$$\begin{aligned} &\left(a^{jk-ik} - 1\right) \equiv 0 \pmod{p} \\ \Leftrightarrow\ &a^{jk-ik} \equiv 1 \pmod{p} \\ \Leftrightarrow\ &a^{k(j-i)} \equiv 1 \pmod{p} \end{aligned}$$

Notice that we have a power of a that is equivalent to 1 (mod p). Then, by (2), since a is a primitive root (mod p), we have that $k(j-i)$ is divisible by $p-1$. Then, by (3), either k is divisible by $p-1$ or $j-i$ is divisible by $p-1$. Since one of our assumptions is that k is coprime with $\varphi(p) = p-1$, we know that k is not divisible by $p-1$, so it must be the case that $j-i$ is divisible by $p-1$.

Now, recall that one of our assumptions about i and j is that $0 < i < j < p$, which imply that $i \geq 1$ and $j \leq p-1$. Now consider $j-i$. The difference $j-i$ is the greatest when j is the greatest possible value and i is the least possible value, or $j = p-1$ and $i = 1$. Thus, $j-i$ is at most $(p-1)-1 = p-2$. In particular, $j-i$ is less than $p-1$. But above, we said that $j-i$ must be divisible by $p-1$. And aha! We have found the contradiction we are looking for: $j-i$ cannot be less than $p-1$ *and* divisible by $p-1$.

In the beginning, we assumed that a^k is not a primitive root (mod p), and after some logical deductions, we found a contradiction. This implies that the initial assumption was false and a^k is, indeed, a primitive root (mod p). Thus, if p is a prime, a is a primitive root (mod p) with $1 \leq a \leq p-1$ and that k is an integer with $1 \leq k \leq p-1$ such that k is coprime with $\varphi(p) = p-1$, then a^k is a primitive root (mod p). We will now use this to solve the problem.

We are given that 19 is a primitive root (mod 43). By the above statement that we just proved, we have that if k is an integer with $1 \leq k \leq p-1$ such that k is coprime with $\varphi(43) = 43-1 = 42$, then 19^k is a primitive root (mod 43). This gives us a way to find primitive roots (mod 43). We first list the integers from 1 to 41, inclusive, that are coprime with 42: $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$. Then $19^1, 19^5, \dots, 19^{41}$ are all of the primitive roots (mod 43). Thus, $a1 = 1,\ a2 = 5,\ a3 = 11, \dots, a12 = 41$, and we obtain that $a10,\ a11,\ a12$ are the last 3 exponents on the list: $31, 37, 41$ respectively.

Finally, we calculate $19^{31}, 19^{37}, 19^{41}$ (mod 43) using fast modular exponentiation:

19^{31} (mod 43):
$19^2 = 361 \equiv 17 \pmod{43}$

$19^4 = (19^2)^2 \equiv 17^2 = 289 \equiv 31 \pmod{43}$
$19^8 = (19^4)^2 \equiv 31^2 = 961 \equiv 15 \pmod{43}$
$19^{16} = (19^8)^2 \equiv 15^2 = 225 \equiv 10 \pmod{43}$
$19^{31} = 19^{16} \times 19^8 \times 19^4 \times 19^2 \times 19^1 \equiv 10 \times 15 \times 31 \times 17 \times 19 = 1501950 \equiv 3 \pmod{43}$

$19^{37} \pmod{43}$:
$19^{37} = 19^{31} \times 19^4 \times 19^2 \equiv 3 \times 31 \times 17 = 1581 \equiv 33 \pmod{43}$

$19^{41} \pmod{43}$:$19^{41} = 19^{37} \times 19^4 \equiv 33 \times 31 = 1023 \equiv 34 \pmod{43}$

Thus, $\boldsymbol{a10 = 31}$, $\boldsymbol{a11 = 37}$, $\boldsymbol{a12 = 41}$, and $\boldsymbol{19^{a10} \equiv 3 \pmod{43}}$, $\boldsymbol{19^{a11} \equiv 33 \pmod{43}}$, $\boldsymbol{19^{a12} \equiv 34 \pmod{43}}$.

2) In the Diffie-Hellman Key Exchange, let the public keys be p = 43, g = 26, and the secret keys be a = 13 and b = 22, 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 $g^a = 26^{13} \pmod{43}$, Bob sends Alice $g^b = 26^{22} \pmod{43}$, and their shared secret key is $(g^a)^b = (26^{13})^{22} = (26^{22})^{13} = (g^b)^a \pmod{43}$. We will use fast modular exponentiation to find these values:

$26^{13} \pmod{43}$:
$26^2 = 676 \equiv 31 \pmod{43}$
$26^4 = (26^2)^2 \equiv 31^2 = 961 \equiv 15 \pmod{43}$
$26^8 = (26^4)^2 \equiv 15^2 = 225 \equiv 10 \pmod{43}$
$26^{13} = 26^8 \times 26^4 \times 26^1 \equiv 10 \times 15 \times 26 = 3900 \equiv 30 \pmod{43}$
$26^{22} \pmod{43}$:
$26^{22} = 26^{13} \times 26^8 \times 26^1 \equiv 30 \times 10 \times 26 = 7800 \equiv 17 \pmod{43}$

Now for the shared secret key, I will choose to calculate $(26^{22})^{13} \pmod{43}$ instead of $(26^{13})^{22} \pmod{43}$, since the smaller outside exponent of 13 means it will take fewer calculations. Since $(26^{22})^{13} \equiv 17^{13} \pmod{43}$, we have

$17^{13} \pmod{43}$:
$17^2 = 289 \equiv 31 \pmod{43}$
$17^4 = (17^2)^2 \equiv 31^2 = 961 \equiv 15 \pmod{43}$
$17^8 = (17^4)^2 \equiv 15^2 = 225 \equiv 10 \pmod{43}$
$17^{13} = 17^8 \times 17^4 \times 17^1 \equiv 10 \times 15 \times 17 = 2550 \equiv 13 \pmod{43}$

Thus, Alice sends Bob **30**, Bob sends Alice **17**, and their shared secret key is **13**.

3) In an RSA scheme, p = 37, q = 19 and e = 77. What is d?

Solution

In the RSA cryptosystem, the integer d represents the private key and its value is $d = e^{-1} \pmod{\varphi(n)}$, where $n = pq$. We first calculate $\varphi(n)$, which is easily found given p and q:

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

With $p = 37$, $q = 19$, we have $\varphi(n) = (37-1)(19-1) = 36 \times 18 = 648$.

Thus, we are calculating $d = 77^{-1} \pmod{648}$, or the integer d such that $77d \equiv 1 \pmod{648}$. We will begin by performing the extended Euclidean algorithm on 648 and 77:

$$648 = 8 \times 77 + 32$$
$$77 = 2 \times 32 + 13$$
$$32 = 2 \times 13 + 6$$
$$13 = 2 \times 6 + 1$$

$$1 = 13 - 2 \times 6$$
$$= 13 - 2 \times (32 - 2 \times 13)$$
$$= 13 - 2 \times 32 + 4 \times 13$$
$$= 5 \times 13 - 2 \times 32$$
$$= 5 \times (77 - 2 \times 32) - 2 \times 32$$
$$= 5 \times 77 - 10 \times 32 - 2 \times 32$$
$$= 5 \times 77 - 12 \times 32$$
$$= 5 \times 77 - 12 \times (648 - 8 \times 77)$$
$$= 5 \times 77 - 12 \times 648 + 96 \times 77$$
$$= 101 \times 77 - 12 \times 648$$

That is, $101 \times 77 - 12 \times 648 = 1$. Now, remember that we want to find the integer d such that $77d \equiv 1 \pmod{648}$. With that in mind, let's take the previous equation (mod 648):

$$101 \times 77 - 12 \times 648 \equiv 1 \pmod{648}$$
$$101 \times 77 - 12 \times 0 \equiv 1 \pmod{648}$$
$$101 \times 77 \equiv 1 \pmod{648}$$

We have found the integer d such that $77d \equiv 1 \pmod{648}$. Thus, $\boldsymbol{d = 101}$.

4) In Elliptic Curve Arithmetic what is the sum of the points (22, 17) and (8, 28) on the curve $E_{37}(15, 4)$?

Solution

Let $P = (x_P, y_P) = (22, 17)$ and $Q = (x_Q, y_Q) = (8, 28)$. We are working on the curve $E_{37}(15, 4)$, which means that the equation for the elliptic curve is $y^2 = x^3 + 15x + 4 \pmod{37}$, and so $a = 15$ and $b = 4$. 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

$$\lambda = \frac{28-17}{8-22} = \frac{11}{-14} = \frac{11}{23} \pmod{37}.$$

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 11 by 23, we will multiply 11 by the modular inverse of 23 (mod 37):

$$\lambda = \frac{11}{23} = 11 \times 23^{-1} \pmod{37}.$$

Now we will find $23^{-1} \pmod{37}$, or the integer x such that $23x \equiv 1 \pmod{37}$, using the Extended Euclidean Algorithm:

$37 = 1 \times 23 + 14$
$23 = 1 \times 14 + 9$
$14 = 1 \times 9 + 5$
$9 = 1 \times 5 + 4$
$5 = 1 \times 4 + 1$

$1 = 5 - 1 \times 4$
$= 5 - 1 \times (9 - 1 \times 5)$
$= 5 - 1 \times 9 + 1 \times 5$
$= 2 \times 5 - 1 \times 9$
$= 2 \times (14 - 1 \times 9) - 1 \times 9$
$= 2 \times 14 - 2 \times 9 - 1 \times 9$
$= 2 \times 14 - 3 \times 9$
$= 2 \times 14 - 3 \times (23 - 1 \times 14)$
$= 2 \times 14 - 3 \times 23 + 3 \times 14$
$= 5 \times 14 - 3 \times 23$
$= 5 \times (37 - 1 \times 23) - 3 \times 23$
$= 5 \times 37 - 5 \times 23 - 3 \times 23$
$= 5 \times 37 - 8 \times 23$

That is, $5 \times 37 - 8 \times 23 = 1$. Now, remember that we want to find the integer x such that $23x \equiv 1 \pmod{37}$. With that in mind, let's take the previous equation (mod 37):

$5 \times 37 - 8 \times 23 = 1 \equiv 1 \pmod{37}$
$5 \times 0 - 8 \times 23 \equiv 1 \pmod{37}$
$-8 \times 23 \equiv 1 \pmod{37}$
$29 \times 23 \equiv 1 \pmod{37}$

With this, we see that $23^{-1} \pmod{37} = 29$. Hence,

$$\lambda = 11 \times 23^{-1} = 11 \times 29 = 319 \equiv 23 \pmod{37}.$$

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 $p = 37$, $\lambda \equiv 23 \pmod{37}$, $P = (x_P, y_P) = (22, 17)$, and $Q = (x_Q, y_Q) = (8, 28)$, we have

$$x_R = 23^2 - 22 - 8 = 499 \equiv 18 \pmod{37}$$
$$y_R = 23 \times (22 - 18) - 17 = 75 \equiv 1 \pmod{37}$$

And this is our desired point: $(22, 17) + (8, 28) = \underline{(\mathbf{18}, \mathbf{1})}$ on the curve $E_{37}(15, 4)$.

5) In Elliptic Curve Arithmetic calculate 4 x (22, 17) on the curve $E_{37}(15, 4)$? (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 $P = (x_P, y_P) = (22, 17)$. We are working on the curve $E_{37}(15, 4)$, which means that the equation for the elliptic curve is $y^2 = x^3 + 15x + 4 \pmod{37}$, and so $a = 15$ and $b = 4$.

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

$$\lambda = \frac{3 \times 22^2 + 15}{2 \times 17} = \frac{1467}{34} \equiv \frac{24}{34} \pmod{37}.$$

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 24 by 34, we will multiply 24 by the modular inverse of 34 (mod 37):

$$\lambda = \frac{24}{34} = 24 \times 34^{-1} \pmod{37}.$$

Now we will find $34^{-1} \pmod{37}$, or the integer x such that $34x \equiv 1 \pmod{37}$, using the Extended Euclidean Algorithm:

$37 = 1 \times 34 + 3$
$34 = 11 \times 3 + 1$

$1 = 34 - 11 \times 3$
$= 34 - 11 \times (37 - 1 \times 34)$
$= 34 - 11 \times 37 + 11 \times 34$
$= 12 \times 34 - 11 \times 37$

That is, $12 \times 34 - 11 \times 37 = 1$. Now, remember that we want to find the integer x such that $34x \equiv 1 \pmod{37}$. With that in mind, let's take the previous equation (mod 37):

$12 \times 34 - 11 \times 37 \equiv 1 \pmod{37}$
$12 \times 34 - 11 \times 0 \equiv 1 \pmod{37}$
$12 \times 34 \equiv 1 \pmod{37}$

With this, we see that $34^{-1} \pmod{37} = 12$. Hence,

$$\lambda = 24 \times 34^{-1} \equiv 24 \times 12 = 288 \equiv 29 \pmod{37}.$$

Finally, 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 $y_P = y_Q$. Hence,

$$x_{2P} = 29^2 - 22 - 22 = 797 \equiv 20 \pmod{37}$$
$$y_{2P} = 29 \times (22 - 20) - 17 = 41 \equiv 4 \pmod{37}$$

And thus, $2P = P + P = (20, 4)$. Now, we add $2P$ to itself to obtain $4P$, going through the same process. We have $2P = (x_{2P}, y_{2P}) = (20, 4)$ and $a = 15$ (which has not changed – we are still on the same elliptic curve).

First, we begin with λ:

$$\lambda = \frac{3 \times 20^2 + 15}{2 \times 4} = \frac{1215}{8} \equiv \frac{31}{8} = 31 \times 8^{-1} \pmod{37}.$$

We use the Extended Euclidean Algorithm to find $8^{-1} \pmod{37}$:

$37 = 4 \times 8 + 5$
$8 = 1 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

$1 = 3 - 1 \times 2$
$= 3 - 1 \times (5 - 1 \times 3)$
$= 3 - 1 \times 5 + 1 \times 3$
$= 2 \times 3 - 1 \times 5$
$= 2 \times (8 - 1 \times 5) - 1 \times 5$
$= 2 \times 8 - 2 \times 5 - 1 \times 5$
$= 2 \times 8 - 3 \times 5$
$= 2 \times 8 - 3 \times (37 - 4 \times 8)$

$= 2 \times 8 - 3 \times 37 + 12 \times 8$
$= 14 \times 8 - 3 \times 37$

Taking the previous equation (mod 37), we have

$14 \times 8 - 3 \times 37 \equiv 1 \pmod{37}$
$14 \times 8 - 3 \times 0 \equiv 1 \pmod{37}$
$14 \times 8 \equiv 1 \pmod{37}$

Thus, $8^{-1} \pmod{37} = 14$ and

$$\lambda = 31 \times 8^{-1} \equiv 31 \times 14 = 434 \equiv 27 \pmod{37}.$$

Finally, we calculate the coordinates of the new point, $4P = (x_{4P}, y_{4P})$:

$$x_{4P} = \lambda^2 - x_{2P} - x_{2P} = 27^2 - 20 - 20 = 689 \equiv 23 \pmod{37}$$
$$y_{4P} = \lambda(x_{2P} - x_{4P}) - y_{2P} = 27 \times (20 - 23) - 4 = -85 \equiv 26 \pmod{37}$$

And this is our desired point: $4 \times (22, 17) = \underline{\mathbf{(23, 26)}}$ on the curve $E_{37}(15, 4)$.

6) Consider an El Gamal cryptosystem with the prime q = 37 and the primitive root a = 15. Alice picks $X_A = 22$ 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 $a = 15$, $X_A = 22$, and $q = 37$, we have $Y_A = 15^{22} \pmod{37}$. We use fast modular exponentiation to calculate this:

$15^2 = 225 \equiv 3 \pmod{37}$
$15^4 = (15^2)^2 \equiv 3^2 = 9 \pmod{37}$
$15^8 = (15^4)^2 = 9^2 = 81 \equiv 7 \pmod{37}$
$15^{16} = (15^8)^2 = 7^2 = 49 \equiv 12 \pmod{37}$
$15^{22} = 15^{16} \times 15^4 \times 15^2 \equiv 12 \times 9 \times 3 = 324 \equiv 28 \pmod{37}$

So $Y_A \equiv 28 \pmod{37}$. 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 $Y_A = 28$ and $k = 2$, we have $K = 28^2 = 784 \equiv 7 \pmod{37}$.

Now, we calculate $C_1 = a^k \pmod q$ and $C_2 = KM \pmod q$. With $a = 15$, $k = 2$, $K = 7$, $M = 31$, and $q = 37$, we have $C_1 = 15^2 \pmod{37}$ and $C_2 = 7 \times 31 \pmod{37}$. Using the fast modular exponentiation calculations from earlier, we have

$$C_1 = 15^2 = 225 \equiv 3 \pmod{37}$$
$$C_2 = 7 \times 31 = 217 \equiv 32 \pmod{37}.$$

This gives us $C = (C_1, C_2) = (3, 32) \pmod{37}$.

Thus, with $\boldsymbol{k = 2}$, we have $\boldsymbol{K = 7 \pmod{37}}$ and $\boldsymbol{C = (3, 32) \pmod{37}}$.

Now, let's pick $k = 3$. We first calculate $K = {Y_A}^k \pmod q$. With $Y_A = 28$ and $k = 3$, we have $K = 28^3 = 21952 \equiv 11 \pmod{37}$.

Now, we calculate $C_1 = a^k \pmod q$ and $C_2 = KM \pmod q$. With $a = 15$, $k = 3$, $K = 11$, $M = 31$, and $q = 37$, we have $C_1 = 15^3 \pmod{37}$ and $C_2 = 11 \times 31 \pmod{37}$. Using the fast modular exponentiation calculations from earlier, we have

$$C_1 = 15^3 = 15^2 \times 15^1 \equiv 3 \times 15 = 45 \equiv 8 \pmod{37}$$
$$C_2 = 11 \times 31 = 341 \equiv 8 \pmod{37}$$

This gives us $C = (C_1, C_2) = (8, 8) \pmod{37}$.

Thus, with $\boldsymbol{k = 3}$, we have $\boldsymbol{K = 11 \pmod{37}}$ and $\boldsymbol{C = (8, 8) \pmod{37}}$.

Using this short Python program, we can take a look at all possible valid ciphertexts for this program:

```
# Information Given.
q = 37
a = 15
M = 31
Xa = 22
Ya = (a**Xa)%q

print("k\tc1\tc2")
print("------------------")

# Try each k, normally 1, 36 would be excluded.
for k in range(1,37):

    # We first calculate capital K and then the two ciphertexts
    bigK = (Ya**k)%q
    c1 = (a**k)%q
    c2 = (bigK*M)%q
    print(k,"\t",c1,"\t",c2, sep="")
```

Here is the output of the program:

```
k     c1    c2
--------------
1     15    17
2     3     32
3     8     8
4     9     2
5     24    19
6     27    14
7     35    22
8     7     24
9     31    6
10    21    20
11    19    5
12    26    29
13    20    35
14    4     18
15    23    23
16    12    15
17    32    13
18    36    31
19    22    17
20    34    32
21    29    8
22    28    2
23    13    19
24    10    14
25    2     22
26    30    24
27    6     6
28    16    20
29    18    5
30    11    29
31    17    35
32    33    18
33    14    23
34    25    15
35    5     13
36    1     31
```

7) For this question, you are going to implement a RSA protocol to send the TAs and me (Arup) a message. For our RSA system, the public keys are as follows:

n = 5959543795627426174320202010482251983
e = 2362345234523453452345234523452345243447

Your message must be in Radix-64. Please google this format. It allows for 64 characters, encoding each with 6 bits. The characters are: all lowercase letters, all uppercase letters, all digits, the plus sign(+) and a forward slash (/).

First, type your message in a textfile only using those 64 characters. Type 20 characters per line. To encrypt, you will encrypt each line, one by one. Please pad the last line with '+' characters as needed. Convert each line of 20 Raxix-64 characters to a 120 bit integer. This will be your plaintext for RSA. Use the public keys given above and calculate the ciphertext, which will be a number from 1 to n-1. Output this number to a textfile. Do this for each line of the message. Here is what you need to turn in for this question:

1. Your code. **(Please use either Java or Python so you have support for Big Integers, naturally.)**

2. A text file with your ciphertext. This should have one number per line, for each block of 20 Radix-64 characters.

If you did everything to specification, the TAs and I should be able to read your message. **Please keep it clean =)** You may address any one of the four of us in your message, or all four of us, if you'd like!

Solution

For this question, code is attached separately in both Java and Python that shows a potential sample solution. Included in a separate file is our checking code.

The files which store the sample solutions are ***problem7.py*** and ***problem7.java***.

The checking files are ***gradep7.py*** and ***gradep7.java***.