Development and Implementation of Novel Pair Value Encryption System

Rushil Mallarapu

June 6, 2021

1

Use Euler's theorem to compute:

1. $5^{60} \pmod{21}$
2. $2^{35} \pmod{35}$

1.1

First, we verify that 5 and 21 are coprime, which they are. Then, we compute $\phi(21)$ via the standard route of decomposing 21 as its prime factorization $21 = 3 \cdot 7$. Thus, $\phi(21) = \phi(3)\phi(7) = 2 \cdot 6 = 12$. Now, by Euler's theorem, it holds that $5^{12} \equiv 1 \pmod{21}$. Dividing 60 by 12 gives $60 = 5 \cdot 12 + 0$, by the division algorithm. Therefore, $5^{60} \equiv (5^{12})^5 \equiv 1^5 \equiv 1 \pmod{21}$. Thus, $5^{60} \equiv 1 \pmod{21}$.

1.2

As before, we verify that 2 and 35 are coprime, which they are. Next, we compute $\phi(35)$ by decomposing 35 as its prime factorization $35 = 5 \cdot 7$. Thus, $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$. Now, by Euler's theorem, it holds that $2^{24} \equiv 1 \pmod{35}$. Dividing 35 by 24 gives $35 = 1 \cdot 24 + 11$, by the division algorithm. Therefore, $2^{35} \equiv (2^{24})^1 \cdot 2^{11} \equiv 1^1 \cdot 2^{11} \equiv 2048 \pmod{35}$. From here, we can use the division algorithm to divide 2048 by 35, giving $2048 = 58 \cdot 35 + 18$. Thus, $2^{35} \equiv 18 \pmod{35}$.

2

Find the last two digits of 123^{403}.

2.1

We want to find the value of $123^{403} \pmod{100}$. First, we verify that 123 and 100 are coprime, as indeed they are. Now, we find $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = (4-2)(25-5) = 2 \cdot 20 = 40$ as per the usual method. Thus, by Euler's theorem, we have that $123^{40} \equiv 1 \pmod{100}$. Using the division algorithm, we have that $403 = 10 \cdot 40 + 3$. As such, $123^{403} \equiv (123^{40})^1 0 \cdot 123^3 \equiv 1^1 0 \cdot 123^3 \equiv 123^3 \equiv 1860867 \pmod{100}$. Finally, taking the last two digits of this, we have that $123^3 \equiv 67 \pmod{100}$. Thus, the final two digits of 123^{403} are 67.

3

Alice chooses primes $p = 17$ and $q = 23$, as well as public key 7. What is the RSA decryption exponent?

3.1

Here, we start by applying the RSA cryptosystem to generate the modulus $n = pq$, which here is $n = 17 \cdot 23 = 391$. We also compute $\phi(n) = (p-1)(q-1) = 16 \cdot 22 = 352$ Next, the public encryption key is $e = 7$, and it is trivial to verify that 7 and 352 are coprime. Now, we must find the decryption key d by solving $ed \equiv 1 \pmod{\phi(n)}$, or $7d \equiv 1 \pmod{352}$.

To solve this, we start by knowing that $\gcd(7, 352)$ is of course one, so there will be only one unique solution d. Now, we apply the extended Euclidean algorithm to (352, 7).

$$\begin{aligned} &\gcd(352, 7) && 352 = 50 \cdot 7 + 2 \\ =&\gcd(7, 2) && 7 = 3 \cdot 2 + 1 \\ =&\gcd(2, 1) && 2 = 2 \cdot 1 + 0 \\ =&1 \end{aligned}$$

	x	y
352	1	0
7	0	1
2	1	-50
1	-3	151

Therefore, the solution to this congruence is $d \equiv 151 \cdot 1 \equiv 151 \pmod{352}$, and it is easy to verify that $7 \cdot 151 \equiv 1057 \equiv 1 \pmod{352}$. Thus, the decryption exponent is $d = 151$.

4

Use Euler's theorem to show that $n^{17} - n \equiv 0 \pmod{510}$ for all integers n (Hint: factor 510).

4.1

Proof. Consider that the prime factorization of 510 is $2 \cdot 3 \cdot 5 \cdot 17$. Therefore, to show that $510 | n^{17} - n$, we must show that all of the prime factors of 510 divide $n^{17} - n$. Let the set of these prime factors be $p \in \{2, 3, 5, 17\}$. First, notice that $n^{17} - n = n(n^{16} - 1)$. Therefore, if n is some multiple of $p - n = kp -$ the conclusion easily follows, as $p | kp((kp)^{16} - 1)$. Thus, we may assume that n and p are coprime. Then, we may apply Euler's theorem by computing the set $\phi(p) \in 1, 2, 4, 16$. Notice that all values in this set divide 16. Therefore, we may conclude that because $n^{\phi(p)} \equiv 1 \pmod{p}$, it must hold for all p that $n^{16} \equiv 1 \pmod{p}$. This means that $p | (n^{16} - 1)$, which implies that $p | n(n^{16} - 1)$, and therefore that $p | n^{17} - n$. As this holds true for all prime factors of 510, it must also hold for 510. This allows us to conclude that $510 | n^{17} - n$, and therefore that $n^{17} - n \equiv 0 \pmod{510}$, thus completing the proof. $\square$

5

Prove that if n is an odd integer, then n divides $2^{(n-1)!} - 1$.

5.1

We begin by proving a useful lemma.

Lemma 5.1. *For all positive integers n, $\phi(n)|(n-1)!$.*

Proof. Recall the definition of $\phi(n)$ as being the count of integers between 1 and n inclusive which are relatively prime to n. Thus, $\phi(n)$ is bounded between 1 and $n-1$ (as $\gcd(1,n) = 1$ for all n). As a result, given that $1 \leq \phi(n) \leq n-1$, it holds that $\phi(n) \in \{1, 2, \ldots, n-1\}$, which implies that $\phi(n)|(n-1)!$, thus completing the proof. $\square$

Now we may prove the main result.

Proof. We want to show that for an odd integer n, $n|2^{(n-1)!} - 1$, which is equivalent to showing that $2^{(n-1)!} \equiv 1 \pmod{n}$. Note that if n is odd, it will be coprime to 2. Therefore, by Euler's theorem, it holds that $2^{\phi(n)} \equiv 1 \pmod{n}$. Note that by the lemma above, we have that $\phi(n)|(n-1)!$, so there exists some integer k for which $\phi(n) \cdot k = (n-1)!$. Substituting this in, we have that $2^{(n-1)!} \equiv 2^{\phi(n) \cdot k} \equiv (2^{\phi(n)})^k \equiv 1^k \equiv 1 \pmod{n}$. Overall, we have shown that $2^{(n-1)!} \equiv 1 \pmod{n}$, thus completing the proof. $\square$

6

We discussed that $\phi(*)$ is a multiplicative function. Namely, if $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. There are many more multiplicative functions – in fact, the divisor function we introduced at the beginning of the semester is another one! Show that σ, the divisor function, is also multiplicative.

6.1

Proof. Recall that the function $\sigma(d)$ is the number of divisors of d. Now, we want to show that, for integers m, n with $\gcd(m,n) = 1$, $\sigma(mn) = \sigma(m)\sigma(n)$. To begin, consider the grid of numbers as follows:

$$\begin{matrix} 1 & m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & \dots & (n-1)m+2 \\ \vdots & \vdots & \ddots & \vdots \\ m & 2m & \dots & nm \end{matrix}$$

First, notice that every value in the i-th row is congruent to $i \pmod{m}$. As such, there are $\sigma(m)$ rows which are congruent to divisors of m modulo m. Next, there are n elements in each row. We will show that these n elements are a complete residue system modulo n, for which we must show that any two distinct elements of any row are not congruent modulo n. Let these two elements come from one of the rows i where i is congruent to a divisor of m modulo m, as per the first step. Then, our two distinct elements are k_1m+i and k_2m+i. Their difference is $(k_2-k_1)m \pmod{n}$. Here, it is clear that $(k_2-k_1) \neq 0$ by construction and $m \not\equiv 0 \pmod{n}$ by the fact that they are coprime. Therefore, every row forms a complete residue system modulo n. Within each row, $\sigma(n)$ of the elements will be congruent to divisors of n modulo n. Overall, there are $\sigma(m)$ rows in which every element is congruent to a divisor of m, and in each such row, $\sigma(n)$ elements which are also congruent to a divisor of n. Ergo, there must be $\sigma(m)\sigma(n)$ elements which are congruent to divisors of mn, and as all elements are between 1 and mn inclusive, we have that $\sigma(mn) = \sigma(m)\sigma(n)$, thus completing the proof. $\square$