1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

Solution:

(a) The private key d is defined as the inverse of $e \pmod{(p-1)(q-1)}$. Thus we need to compute $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. Find inverse of e mod $(5-1)(11-1) = 40$. Compute $\text{egcd}(40, 9)$:

$$\begin{aligned} \text{egcd}(40,9) &= \text{egcd}(9,4) && [4 = 40 \bmod 9 = 40 - 4(9)] \\ &= \text{egcd}(4,1) && [1 = 9 \bmod 4 = 9 - 2(4)]. \\ 1 &= 9 - 2(4). \\ 1 &= 9 - 2(40 - 4(9)) \\ &= 9 - 2(40) + 8(9) = 9(9) - 2(40). \end{aligned}$$

We get $-2(40) + 9(9) = 1$. So the inverse of 9 is 9. So $d = 9$.

(b) 4 is the encoded message. We can decode this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. $4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encode the number x we must compute $x^e \bmod N$. Thus, $14^9 \equiv 14 \cdot (14^2)^4 \equiv 14 \cdot (31^2)^2 \equiv 14 \cdot (26^2) \equiv 14 \cdot 16 \equiv 4 \pmod{55}$. This verifies the second part since the encoded message was suppose to be 4.

2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

(a) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

(b) What number is e relatively prime to?

(c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

(d) What is $\gcd(e,(p-1)(q-1))$?

(e) What is the decryption exponent d?

(f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

(g) Bob receives the encrypted message, and applies his decryption function D to it. What is D applied to the received message?

Solution:

(a) $N = pq = 77$.

(b) e must be relatively prime to $(p-1)(q-1) = 60$.

(c) We cannot take $e = 2,3,5$, so we take $e = 7$.

(d) By design, $\gcd(e,(p-1)(q-1)) = 1$ always.

(e) The decryption exponent is $d = e^{-1} \pmod{60} = 43$, which could be found through Euclid's extended GCD algorithm.

(f) The encrypted message is $E(30) = 30^7 \equiv 2 \pmod{77}$. We can obtain this answer via repeated squaring.

$$\begin{aligned}30^7 &\equiv 30 \cdot 30^6 \equiv 30 \cdot (30^2 \bmod 77)^3 \equiv 30 \cdot 53^3 \equiv (30 \cdot 53 \bmod 77) \cdot (53^2 \bmod 77) \equiv 50 \cdot 37 \\ &\equiv 2 \pmod{77}.\end{aligned}$$

(g) We have $D(2) = 2^{43} \equiv 30 \pmod{77}$. Again, we can use repeated squaring.

$$\begin{aligned}2^{43} &\equiv 2 \cdot 2^{42} \equiv 2 \cdot (2^2 \bmod 77)^{21} \equiv 2 \cdot 4^{21} \equiv (2 \cdot 4 \bmod 77) \cdot 4^{20} \equiv 8 \cdot (4^2 \bmod 77)^{10} \\ &\equiv 8 \cdot 16^{10} \equiv 8 \cdot (16^2 \bmod 77)^5 \equiv 8 \cdot 25^5 \equiv (8 \cdot 25 \bmod 77) \cdot 25^4 \equiv 46 \cdot (25^2 \bmod 77)^2 \\ &\equiv 46 \cdot (9^2 \bmod 77) \equiv 46 \cdot 4 \equiv 30 \pmod{77}.\end{aligned}$$

3 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.

Solution:

Recall that the security of RSA depended upon the supposed hardness of factoring $N = P \times Q$. However, since $N = P$ in this problem, we can consider it to have been already factored! Indeed, recall that the private key d in RSA is defined to be the multiplicative inverse of e modulo $(P-1)(Q-1)$, because we can then use the following relation to decrypt the message:

$$m^{k(P-1)(Q-1)+1} \equiv m \pmod{N}$$

Note that in our case where $N = P$, an analogous relation immediately holds by Fermat's Little Theorem:

$$m^{k(P-1)+1} \equiv m \pmod{P}$$

Therefore, if we can find d which is the multiplicative inverse of e modulo $P-1$, we can decrypt the message by simply computing $m^{ed} \pmod{P} = 35^d \pmod{P}$. It is easy to see by inspection that $67 \times 3 = 201 \equiv 1 \pmod{100}$, so the desired multiplicative inverse $d = 3$, which means that $m = 51 \pmod{101}$.

(Otherwise, one can find the multiplicative inverse by applying Extended Euclid's algorithm to $e = 67$ and $P-1 = 100$:

$$\begin{aligned}
(c,a,b) &= \text{extended-gcd}(100,67) = (c, b_1, a_1 - \lfloor 100/67 \rfloor b_1) \quad \text{where} \\
(c,a_1,b_1) &= \text{extended-gcd}(67,33) = (c, b_2, a_2 - \lfloor 67/33 \rfloor b_2) \quad \text{where} \\
(c,a_2,b_2) &= \text{extended-gcd}(33,1) = (c, b_3, a_3 - \lfloor 33/1 \rfloor b_3) \quad \text{where} \\
(c,a_3,b_3) &= \text{extended-gcd}(1,0) = (1,1,0)
\end{aligned}$$

Therefore, $(c,a_2,b_2) = (1,0,1)$, $(c,a_1,b_1) = (1,1,-2)$, and $(c,a,b) = (1,-2,3)$ respectively. We can verify that $1 = c = ax + by = -2 \times 100 + 3 \times 67$. Hence, the multiplicative inverse of 67 modulo 100 is 3.)

4 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

Solution:

$N = pqr$ where p, q, r are all prime. Then, let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. I decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We need to prove that $x^{ed} - x \equiv 0 \pmod{N}$ and thus $x^{ed} \equiv x \pmod{N}$. To prove that $x^{ed} - x \equiv 0 \pmod{N}$, we factor out the x to get $x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$

because $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$. As a reminder, we are considering the number: $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$.

We now argue that this number must be divisible by p, q, and r. Thus it is divisible by N and $x^{ed} - x \equiv 0 \pmod{N}$.
To prove that it is divisible by p:

- If x is divisible by p, then the entire thing is divisible by p.
- If x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}$. Thus it is divisible by p.

The same reasoning shows that it is divisible by q and r.

One can also use a CRT based argument to argue the correctness of 3 prime RSA. Indeed, as discussed in the previous paragraphs, we need to show that $x^{ed} \equiv x \pmod{N}$, where recall that $N = pqr$. In order to do this, observe that it suffices to prove the following three equivalences:

$$x^{ed} \equiv x \pmod{p}, \tag{1}$$
$$x^{ed} \equiv x \pmod{q}, \tag{2}$$
$$x^{ed} \equiv x \pmod{r}. \tag{3}$$

Why does it suffice? If these 3 statements are indeed true, the uniqueness property established in the CRT implies that $x^{ed} \equiv x \mod N$. Note that p, q and r are relatively prime so we are allowed to apply the Chinese Remainder Theorem here.

Recall that $e > 1$ is any natural number that is relatively prime to $p-1$, $q-1$ and $r-1$. And d is the multiplicative inverse of e modulo $(p-1)(q-1)(r-1)$. In particular, this means that $ed = k(p-1)(q-1)(r-1)+1$ for some natural number k. Let us try to use this to verify (1):

$$\begin{aligned} x^{ed} &= x^{k(p-1)(q-1)(r-1)+1} \\ &= x \cdot \left(x^{k(q-1)(r-1)}\right)^{p-1} \\ &\equiv x \pmod{p} \end{aligned}$$

where the last step follows by using Fermat's Little Theorem to claim that for any $a \in \mathbb{N}$, $a^{p-1} \equiv 1 \pmod{p}$. In particular, we choose $a = x^{k(q-1)(r-1)}$ and apply FLT. Note that the original FLT holds with $a = 1, 2, \cdots, p-1$, but we leave it as an exercise to prove that it indeed applies for any natural number $a \in \mathbb{N}$. Thus, we have shown that $x^{ed} \equiv x \pmod{p}$, and a matching argument shows that $x^{ed} \equiv x \pmod{q}$ and $x^{ed} \equiv x \pmod{r}$. This proves equations (1), (2) and (3) and hence shows that $x^{ed} \equiv x \pmod{N}$.