DIS 5A

1 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.

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

2 Just a Little Proof

Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Solution:

Note: This problem is essentially asking you to prove the correctness of RSA.

We know that a is not a divsible by p and a is not divisible by q since $\gcd(a, pq) = 1$.We subtract a from both sides to get

$$\begin{aligned}
a^{(p-1)(q-1)+1} - a &\equiv 0 \pmod{pq} \\
a(a^{(p-1)(q-1)} - 1) &\equiv 0 \pmod{pq}
\end{aligned}$$

Since p, q are primes, we just need to show that the left hand side is divisible by both p and q. Since a is not divisible by p, we can use Fermat's Little Theorem to state that $a^{p-1} \equiv 1 \pmod{p}$.

$$a\big((a^{(p-1)})^{q-1} - 1\big) \equiv a(1^{q-1} - 1) \equiv 0 \pmod{p}$$

Thus $a(a^{(p-1)(q-1)} - 1)$ is divisible by p. We can apply the same reasoning to show that the expression is divisible by q. Therefore we have proved our claim that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Alternative Proof:
Because $\gcd(a, pq) = 1$, we have that a does not divide p and a does not divide q. By Fermat's Little Theorem,

$$a^{(p-1)(q-1)+1} = (a^{(p-1)})^{(q-1)} \cdot a \equiv 1^{q-1} \cdot a \equiv a \pmod{p}.$$

Similarly, by Fermat's Little Theorem, we have

$$a^{(p-1)(q-1)+1} = (a^{(q-1)})^{(p-1)} \cdot a \equiv 1^{p-1} \cdot a \equiv a \pmod{q}.$$

Now, we want to use this information to conclude that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. We will first take a detour and show a more general result (you could write this out separately as a lemma if you want).

Consider the system of congruences

$$\begin{aligned}
x &\equiv a \pmod{p} \\
x &\equiv a \pmod{q}.
\end{aligned}$$

Let's run the CRT symbolically. First off, since p and q are relatively prime, we know there exist integers g, h such that

$$g \cdot p + h \cdot q = 1.$$

We could find these via Euclid's algorithm. By the CRT, the solution to our system of congruences will be

$$x \equiv a \cdot y_1 \cdot q + a \cdot y_2 \cdot p \pmod{pq}.$$

To solve for y_1 and y_2, we must find y_1 such that

$$x_1 \cdot p + y_1 \cdot q = 1$$

and y_2 such that

$$x_2 \cdot q + y_2 \cdot p = 1.$$

This is easy since we already know $g \cdot p + h \cdot q = 1$: the answers are $y_1 = h$ and $y_2 = g$. Finally we can plug in to the solution to get

$$x \equiv a \cdot h \cdot q + a \cdot g \cdot p \equiv a(h \cdot q + g \cdot p) \equiv a \cdot 1 \equiv a \pmod{pq}.$$

Therefore by the CRT we know that the set of solutions that satisfy both $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ is exactly the set of solutions that satisfy $x \equiv a \pmod{pq}$.

So since $a^{(p-1)(q-1)+1} \equiv a \pmod{p}$ and $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$, then by the CRT we know that $a^{(p-1)(q-1)+1}$ satisfies $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

3 RSA Exponent

What's wrong with using the exponent $e = 2$ in a RSA public key?

Solution:

To find the private key d from the public key (N, e), we need $\gcd(e, (p-1)(q-1)) = 1$. However, $(p-1)(q-1)$ is necessarily even since p, q are distinct odd primes, so if $e = 2$, $\gcd(e, (p-1)(q-1)) = 2$, and a private key does not exist. (Note that this shows that e should more generally never be even.)