1 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(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) Encrypt 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 $9^{-1} \bmod (5-1)(11-1) = 9^{-1} \bmod 40$. 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 encrypted message. We can decrypt this with $D(m) \equiv m^d \equiv 4^9 \equiv 14 \pmod{55}$. Thus the original message was 14.

(c) The answer from the second part was 14. To encrypt 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 encrypted message was supposed to be 4.

2 RSA with CRT

Note 7

Inspired by the efficiency of solving systems of modular equations with CRT, Bob decides to use CRT to speed up RSA!

He first generates the public key (e,N) and private key d as normal, keeping track of the primes $pq = N$. Recall that e is chosen to be coprime to $(p-1)(q-1)$, and d is then defined as $e^{-1} \pmod{(p-1)(q-1)}$. Next, he stores the following values:

$$d_p \equiv d \pmod{p-1}$$
$$d_q \equiv d \pmod{q-1}$$

After receiving an encrypted message $c = m^e \pmod N$ from Alice, Bob computes the following expressions:

$$x \equiv c^{d_p} \pmod p$$
$$x \equiv c^{d_q} \pmod q$$

The message m then calculated as the solution to the above modular system.

(a) Show that this algorithm is correct, i.e. that $x \equiv m$ is the only solution $\pmod N$ to the above modular system.

(b) Emboldened by his success in using CRT for RSA, Bob decides to invent a new cryptosystem. To generate his keypair, he first generates $N = pq$. Then, he chooses three numbers g, r_1, r_2 ($q \nmid g$ and $p \nmid g$) and publishes the public key $(N, g_1 = g^{r_1(p-1)} \pmod N, g_2 = g^{r_2(q-1)} \pmod N)$. His private key is (p,q).

To encrypt a message, Alice chooses two numbers s_1, s_2 and sends $c_1 = mg_1^{s_1}, c_2 = mg_2^{s_2}$.

Bob decrypts this message by solving the modular system

$$x \equiv c_1 \pmod p$$
$$x \equiv c_2 \pmod q$$

Show that this algorithm is correct, i.e. show that $x \equiv m$ is the only solution $\pmod N$ to the above modular system.

(c) This system is woefully insecure. Show how anyone with access to the public key can recover p, q, given that $g_1 \not\equiv 1 \pmod q$.

Solution:

(a) Note that $x = c^{d_p} \equiv m \pmod p$, and $x = c^{d_p} \equiv m \pmod q$. Therefore, the solution to the modular system must satisfy both constraints, which leaves m as the only solution.

(b) Similarly to the previous question, we have

$$x \equiv mg_1^{s_1} \pmod p$$
$$x \equiv mg_2^{s_2} \pmod q$$

Key to this subpart is the fact that $g_1^{s_1} = g^{s_1 r_1 (p-1)} \equiv 1 \pmod{p}$, and $g_2^{s_2} = g^{s_2 r_2 (q-1)} \equiv 1 \pmod{q}$. Therefore, this system reduces to

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

By the previous subpart, we know that $x \equiv m \pmod{N}$.

(c) We are given a value $g_1 = g^{r_1(p-1)} \pmod{p}$ (as part of the public key) that is $1 \pmod{p}$ (by FLT) but not $1 \pmod{q}$. It follows that $g_1 - 1$ is a multiple of p, and we can find $\gcd(g_1 - 1, N) = p$. From there, we can find $q = \frac{N}{p}$. Note that if $g_1 \equiv 1 \pmod{q}$, this won't work, since then $g_1 - 1$ is a multiple of N and $\gcd(g_1 - 1, N) = N$. However, then $c_1 = m$ for all encryptions, making it insecure regardless.

3 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose $e, d > 1$ in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

Solution:

(a) Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ for all $x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1) + 1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then

$$\begin{aligned} x^{ed} &\equiv x^{k(p-1)+1} \pmod{p} \\ &\equiv x^{k(p-1)} x \pmod{p} \\ &\equiv 1^k x \pmod{p} \\ &\equiv x \pmod{p}, \end{aligned}$$

by using FLT.

And for both cases, we have shown that x is recovered by $D(E(x))$.

(b) Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \pmod{(p-1)(q-1)(r-1)}$. People who wish to send me a secret, x, send $y = x^e \pmod{N}$. We decrypt an incoming message, y, by calculating $y^d \pmod{N}$.

Does this work? We prove that $x^{ed} - x \equiv 0 \pmod{N}$, and thus $x^{ed} = x \pmod{N}$.
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 $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is 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.

To prove that it is divisible by q:

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

To prove that it is divisible by r:

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

4 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in $\mathrm{GF}(p)$ for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \mathrm{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under $\mathrm{GF}(p)$.

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = x^{13}$ over $\mathrm{GF}(13)$; then find a polynomial with degree strictly less than 7 that is equivalent to $g(x) = 2x^{74} + 6x^7 + 3$ over $\mathrm{GF}(7)$.

(c) In $\mathrm{GF}(p)$, prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

Solution:

(a) For f and g to be equivalent, they must satisfy $f(x) \equiv g(x) \pmod p$ for all values of x, including zero. But $f(0) \equiv 0 \pmod p$ and $g(0) \equiv 1 \pmod p$, so they are not equivalent.

(b) Fermat's Little Theorem says that for any nonzero integer a and any prime number p, $a^{p-1} \equiv 1 \bmod p$. We're allowed to multiply through by a, so the theorem is equivalent to saying that $a^p \equiv a \bmod p$; note that this is true even when $a = 0$, since in that case we just have $0^p \equiv 0 \pmod p$.

The problem asks for a polynomial $\tilde{f}(x)$, different from $f(x)$, with the property that $\tilde{f}(a) \equiv a^{13} \bmod 13$ for any integer a. Directly using the theorem, $\tilde{f}(x) = x$ will work. We can do something similar with $g(x) = 2x^{74} + 6x^7 + 3$ modulo 7; since $x^7 \equiv x \pmod 7$, we repeatedly substitute x^7 with x, effectively reducing the exponent by 6. We can only do this as long as the exponent remains greater than or equal to 7, so we end up with $\tilde{g}(x) = 2x^2 + 6x + 3$.

(c) One proof uses Fermat's Little Theorem. As a warm-up, let $d \geq p$; we'll find a polynomial equivalent to x^d. For any integer, we know

$$\begin{aligned} a^d &= a^{d-p}a^p \\ &\equiv a^{d-p}a \pmod p \\ &\equiv a^{d-p+1} \pmod p. \end{aligned}$$

In other words x^d is equivalent to the polynomial $x^{d-(p-1)}$. If $d-(p-1) \geq q$, we can show in the same way that x^d is equivalent to $x^{d-2(p-1)}$. Since we subtract $p-1$ every time, the sequence $d, d-(p-1), d-2(p-1), \ldots$ must eventually be smaller than p. Now if $f(x)$ is any polynomial with degree $\geq p$, we can apply this same trick to every x^k that appears for which $k \geq p$.

Another proof uses Lagrange interpolation. Let $f(x)$ have degree $\geq p$. By Lagrange interpolation, there is a unique polynomial $\tilde{f}(x)$ of degree at most $p-1$ passing through the points $(0, f(0)), (1, f(1)), (2, f(2)), \ldots, (p-1, f(p-1))$, and we know it must be equivalent to $f(x)$ because f also passes through the same p points.

5 Lagrange's Residents

Note 8 A group of humans has settled at the Earth–Moon L5 point, a Lagrange Point near earth. They have a message for their friends on Earth, and its your job to decode it.

A four packet message is sent using a degree 3 polynomial $P(x)$, where $P(0) = m_1$, $P(1) = m_2$, $P(2) = m_3$, and, $P(3) = m_4$. $P(4)$ and $P(5)$ are also sent.

Unfortunately, the channel lost $P(0)$ and $P(3)$, so the earthlings only received:

$(1,3), (2,7), (4,-90), (5,-335)$

Using Lagrange interpolation and a graphical calculator (eg. Desmos), recover $P(0)$ and $P(3)$ to unlock the space explorers' message.

Solution:

(a)

$$\Delta_1(x) = \frac{(x-2)(x-4)(x-5)}{(1-2)(1-4)(1-5)} = \frac{(x-2)(x-4)(x-5)}{-12}$$

(b)

$$\Delta_2(x) = \frac{(x-1)(x-4)(x-5)}{(2-1)(2-4)(2-5)} = \frac{(x-1)(x-4)(x-5)}{6}$$

(c)

$$\Delta_4(x) = \frac{(x-1)(x-2)(x-5)}{(4-1)(4-2)(4-5)} = \frac{(x-1)(x-2)(x-5)}{-6}$$

(d)

$$\Delta_5(x) = \frac{(x-1)(x-2)(x-4)}{(5-1)(5-2)(5-4)} = \frac{(x-1)(x-2)(x-4)}{12}$$

(e)

$$\begin{aligned} p(x) &= 3 \cdot \Delta_1(x) + 7 \cdot \Delta_2(x) - 90 \cdot \Delta_4(x) - 335 \cdot \Delta_5(x) \\ &= \frac{-24x^3 + 133x^2 - 223x + 120}{2} \end{aligned}$$

(f)

$$p(0) = 60$$

(g)

$$p(3) = 0$$

60 is the ASCII code for <.

<3 70

Turns out even space explorers enjoy discrete maths!