CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes

DIS 3B

1 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

(a) What is wrong with using the exponent $e = 2$ in an RSA public key?

(b) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

(c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(d) What is the private key?

(e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

(f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? What is the decrypted message?

Solution:

(a) 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.)

(b) Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

(c) $N = p \cdot q = 85$ and $e = 3$ are displayed publicly. Note that in practice, p and q should be much larger (512-bit) numbers. We are only choosing small numbers here to allow manual computation.

(d) We must have $ed = 3d \equiv 1 \pmod{64}$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $\gcd(x,y) = 1 = ax + by$, and $a = 1$, $b = -21$.

(e) We have $E(x) = x^3 \pmod{85}$, where $E(x)$ is the encryption function. $10^3 \equiv 65 \pmod{85}$, so $E(x) = 65$.

(f) We have $D(y) = y^{43} \pmod{85}$, where $D(y)$ is the decryption function, the inverse of $E(x)$.

$$x \equiv 24^{43} \pmod{85}$$

From CRT we know that for coprime numbers p and q if

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then

$$x = aqq_1 + bpp_1 \pmod{pq}$$

where $p_1 = p^{-1} \pmod{q}$ and $q_1 = q^{-1} \pmod{p}$.

In our case we have $p = 5$ and $q = 17$. So

$$x \equiv 24^{43} \equiv (-1)^{43} \equiv -1 \equiv 4 \pmod{5}$$

and

$$x = 24^{43} \pmod{17}$$
$$x = (7)^{43} \pmod{17}$$
$$x = (7^2)^{21} \cdot 7 \pmod{17}$$
$$x \equiv (-2)^{21} \cdot 7 \pmod{17}$$
$$x = ((-2)^4)^5 \cdot (-2) \cdot 7 \pmod{17}$$
$$x \equiv (-1)^5 \cdot (-14) \pmod{17}$$
$$x \equiv 14 \pmod{17}$$

Hence

$$x = a = 4 \pmod{5} \qquad x = b = 14 \pmod{17}$$

and

$$p_1 = p^{-1} \pmod{17} = 5^{-1} \pmod{17} = 7$$
$$q_1 = q^{-1} \pmod{5} = 17^{-1} \pmod{5} = 3$$

So we have

$$x \equiv aqq_1 + bpp_1 \pmod{pq}$$
$$x = 4 \cdot 17 \cdot 3 + 14 \cdot 5 \cdot 7 \pmod{85}$$
$$x = 4 \cdot 17 \cdot 3 + 490 \pmod{85}$$
$$x = 17 \cdot (12) + 490 \pmod{85}$$
$$x = 17 \cdot (10 + 2) + 490 \pmod{85}$$
$$x \equiv 34 + (-20) \pmod{85}$$
$$x = 14 \pmod{85}$$

so $D(y) = 14$.

2 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.

Alternatively, we could also have used a CRT-based argument. If we look at $y_p = y \bmod p$, then this is the coordinate corresponding to the prime p from the CRT perspective. We know that the coordinates don't interact with each other for addition, multiplication, or exponentiation of numbers. Since e is coprime with $(p-1)(q-1)(r-1)$, it is also coprime with just $p-1$ individually. So, we can compute d_p the multiplicative inverse mod $(p-1)$ of e. How? We just compute via the EGCD a, b so that $1 = ae + b(p-1)$. Here, we can set d_p to be any positive natural number that is congruent to $a \bmod p-1$. (Just in case the a that EGCD gives is negative.) Now, $x_p = y_p^{d_p} \bmod p$ since if $x_p \equiv 0 \pmod{p}$, then zero to any power is zero and we recover it. If x was not a multiple of p, then x_p is not zero and $y_p = x_p^e \bmod p$ by CRT coordinates, and thus $y_p^{d_p} \bmod p = (x_p^e)^{d_p} \bmod p = x_p^{ed_p} \bmod p = x_p^{1+k(p-1)} \bmod p = x_p x_p^{k(p-1)} \bmod p = x_p (x_p^{(p-1)})^k \bmod p = x_p$ where the last line follows from FLT since $x_p^{p-1} \bmod p = 1$. This tells us that we can recover x_p from y_p. We can do the same by analogous reasoning for x_q, x_r as well by constructing analogous d_q and d_r. Once we have x_p, x_q, x_r, we can use the CRT to reconstruct x since p, q, r are pairwise coprime (since they are prime) and hence $x = x_p v_p + x_q v_q + x_r v_r \bmod pqr$ where $v_p = qr * (qr)^{-1}$ and the multiplicative inverse is being calculated mod p, and similarly for $v_q = pr * (pr)^{-1}$ and $v_r = pq * (pq)^{-1}$. The subscript of the v tells what the relevant multiplicative inverse is calculated relative to.

3 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1, 3)$, $(p_2q_2, 3)$, and $(p_3q_3, 3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?

Solution:

(a) Normally, the difficulty of cracking RSA hinges upon the believed difficulty of factoring large numbers. If Eve were given just p_1q_1, she would (probably) not be able to figure out the factors.

However, Eve has access to two public keys, so yes, she will be able to figure it out. Note that $\gcd(p_1q_1, p_1q_2) = p_1$. Taking GCDs is actually an efficient operation thanks to the Euclidean Algorithm. Therefore, she can figure out the value of p_1, and from there figure out the value of q_1 and q_2 since she has p_1q_1 and p_1q_2.

(b) Since none of the N's have common factors, she cannot find a GCD to divide out of any of the Ns. Hence the approach above does not work.

(c) Eve observes $x^3 \pmod{N_1}$, $x^3 \pmod{N_2}$, $x^3 \pmod{N_3}$. Since all N_1, N_2, N_3 are pairwise relatively prime, Eve can use the Chinese Remainder Theorem to figure out $x^3 \pmod{N_1N_2N_3}$. However, once she gets that, she knows x, since $x < N_1$, $x < N_2$, and $x < N_3$, which implies $x^3 < N_1N_2N_3$. Uh oh!
(Side note: for a more concrete walk through of CRT, refer to the Chinese Remainder Problem in discussion 2C.)