RSA

Setup:

two primes p, q $\quad N = pq$

Public key: (N, e)

Private key: $d = e^{-1} \pmod{(p-1)(q-1)}$

Message: $x \in [0, N]$

Encryption:

$$E(x) = x^e \pmod{N}$$

Decryption:

Receive $y = E(x)$

$$D(y) = y^d \pmod{N}$$

Adversary can see:
Public key: (N, e)
Encrypted Message: y
but cannot decrypt!!

Why it Works (see notes for full proof)

$$D(y) = y^d = x^{ed} = x^{k(p-1)(q-1)+1}$$

$$\Updownarrow$$

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

(FLT) $\Rightarrow$ $\equiv x \pmod{p}$, $\equiv x \pmod{q}$ $\Rightarrow$ (CRT) $\Rightarrow \equiv x \pmod{N}$

CS 70 Discrete Mathematics and Probability Theory
Spring 2021 DIS 4A

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?

77

(b) What number is e relatively prime to?

$(7-1)(11-1) = 60$

(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.

7

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

1

(e) What is the decryption exponent d?

$7^{-1} \pmod{60}$

$= 43$

7×61
7×121
7×181
7×241
7×301
$301 = 7 \times 43$

$(60, 7)$ $1, 2, -17$
$\downarrow$ $\uparrow$
$(7, 4)$ $1, -1, 2$
$\downarrow$ $\uparrow$
$(4, 3)$ $1, 1, -1$
$\downarrow$ $\uparrow$
$(3, 1)$ $1, 0, 1$
$\downarrow$ $\uparrow$
$(1, 0) \rightarrow 1, 1, 0$

(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?

$E(30) = 30^7 \pmod{77}$

$\equiv \boxed{2} \pmod{77}$

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

$D(2) \equiv 2^{43} \pmod{77}$

$\equiv \boxed{30}$

2 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.

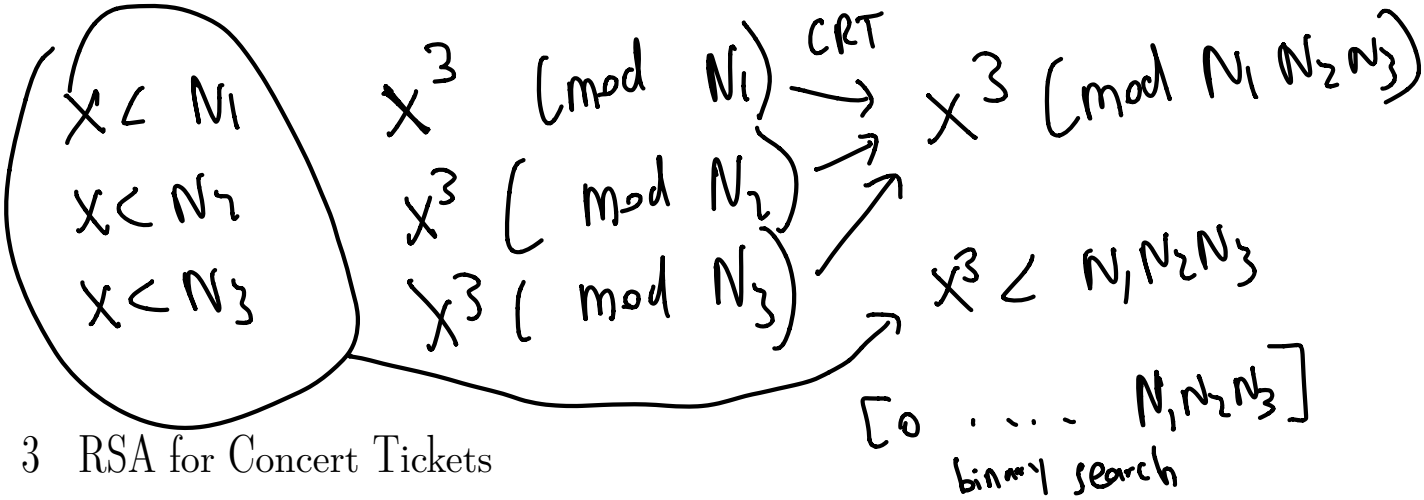
$\gcd(p_1q_1, p_1q_2) = \boxed{p_1}$

$\frac{p_1q_1}{p_1} = q_1$ $\quad$ $\frac{p_1q_2}{p_1} = q_2$

(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.

$\gcd(p_1q_1, p_2q_2) = 1$

(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?



3 RSA for Concert Tickets

Alice wants to tell Bob her concert ticket number, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her ticket number.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number is. How did she do it?

$0 \ldots N$ Eve tries $0^e \; 1^e \; 2^e \ldots 100^e$

$m^e \pmod{N}$

$\downarrow$

y

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

$$r^e \pmod N$$

$$(rm)^e \pmod N \equiv r^e m^e \pmod N$$

$$\text{egcd}(r^e, N)$$

$$\downarrow$$

$$(r^e)^{-1} \pmod N$$

$$\downarrow$$

$$(r^e)^{-1} r^e m^e \equiv m^e \pmod N$$