Announcements:

- Midterm next Monday 7/12 @ 8pm
  - see Piazza for logistics

public key

(N, e)

private key

d

* $N = pq$ for p, q prime
* e coprime to $(p-1)(q-1)$
* $ed \equiv 1 \pmod{(p-1)(q-1)}$

Alice $\xrightarrow{x}$ Bob: $E(x) = x^e \pmod N$

Bob decrypt: $D(E(x)) = (x^e)^d \pmod N$

$\equiv x \pmod N$

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?

Need $\gcd(e, (p-1)(q-1)) = 1$, but $p-1$ & $q-1$ are even

so $\gcd(2, (p-1)(q-1)) = 2$.

- e should never be even

(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.

- $p-1$ & $q-1$ can't be multiples of 3

So p, q must be of the form $3k+2$

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

$\boxed{N = 85,\ e = 3}$

(d) What is the private key?

$3d \equiv 1 \pmod{64}$

$\boxed{d = 43}$

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

$$E(x) = 10^3 \pmod{85}$$
$$\equiv 65 \pmod{85}$$

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

$$\boxed{\begin{array}{l} \text{FLT:} \quad a^{p-1} \equiv 1 \pmod{p} \\ \qquad a^{k(p-1)} \cdot a \equiv a \pmod{p} \end{array}}$$

$$D(y) = 24^{43} \pmod{85}$$

By CRT:

$$\left.\begin{array}{l} 24^{43} \equiv x_1 \pmod{5} \\ 24^{43} \equiv x_2 \pmod{17} \end{array}\right\} 24^{43} = x_1 b_5 + x_2 b_{17} \pmod{85}$$

$$b_5 \equiv 1 \pmod{5}$$
$$b_5 \equiv 0 \pmod{17}$$
$$b_5 = 17(17^{-1} \bmod 5)$$

$$24^{43} \equiv (-1)^{43} \equiv -1 \equiv 4 \pmod{5}$$
$$24^{43} \equiv \underbrace{7^{43} \equiv 7^{11}}_{\text{FLT}} \equiv (7^2)^5 \cdot 7 \equiv (-2)^5 \cdot 7 \equiv (-1)(-2) \cdot 7 \equiv 14 \pmod{17}$$

$$\left.\begin{array}{l} 24^{43} \equiv 4 \pmod{5} \\ 24^{43} \equiv 14 \pmod{17} \end{array}\right\} 24^{43} = 4 \cdot b_5 + 14 \cdot b_{17} \pmod{85}$$

$$b_5 = 17(17^{-1} \bmod 5) = 51$$
$$b_{17} = 5(5^{-1} \bmod 17) = 35$$

$$24^{43} \equiv 4(51) + 14(35) \pmod{85}$$
$$\equiv 204 + 13 \cdot 5 \pmod{85}$$

$$\equiv 34 + 65 \pmod{85}$$

$$\equiv 99 \pmod{85}$$

$$\equiv 14 \pmod{85}$$

$$\boxed{D(4) = 14}$$

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 $0 \le x < N_i$ 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.

yes, Eve knows p_1 are the same, so $\gcd(p_1q_1, p_1q_2) = p_1$

Now Eve can find q_1, q_2 by dividing N_i/p_1

(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.

Now, none of the N_i's have common factors so Eve cannot use the GCD to divide out any N_i's.

(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?

Eve sees $x^3 \bmod N_1$, $x^3 \bmod N_2$, $x^3 \bmod N_3$.
Since N_i's are relatively prime, Eve can use CRT to find $x^3 \pmod{N_1N_2N_3}$. Since $x < N_i \ \forall i$, $x^3 < N_1N_2N_3$ so Eve can find 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?

Only 101 possible values for Alice's ticket number, Eve can try doing $m^e \pmod{N}$ for $m \in \{0, 1, 2, \ldots, 100\}$ and see which m works.

(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?

Alice sends $x = r^e \pmod{N}$ & $y = (rm)^e = xm^e \pmod{N}$

Eve can find $x^{-1} \pmod{N}$ & multiply this by y getting $m^e \pmod{N}$. Now use part a)