m, (N,e) (p,q,d)

Alice $\xrightarrow{m}$ Bob

(N,e)

security

cannot find x

Eve (N,e), m

correctness

Bob can find x

enc key

$m \equiv e\,x \pmod{p}$

ciphertext

plaintext

$m e^{-1} \bmod p$

dec key

$\equiv e e^{-1} x \equiv x \pmod{p}$

Alice

x

$x^e \bmod N = m$

encrypt

"Hi"

10011000

Bob

p, q private

$N = pq$

e: $\gcd(e, (p-1)(q-1)) = 1$

$d \equiv e^{-1} \pmod{(p-1)(q-1)}$

$m^d \equiv x^{ed} \equiv x \pmod{N}$

decrypt

sagnick@ MTu 9-10 PM online
Mon Thu Sun

CS 70 Fall 2021 — Discrete Mathematics and Probability Theory — DIS 4B

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?

$p-1$ even
$q-1$ even
$(p-1)(q-1)$ even
$\gcd(2,(p-1)(q-1)) \cancel{\geq 2}$ $=1$

$p = 7$
$q = 103$
$2, 3, 5, 7, 11, \ldots$

(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.

$p = \cancel{3k}, \cancel{3k+1}, 3k+2$
$q = \cancel{3k}, \cancel{3k+1}, 3k+2$
$k \in \mathbb{Z}$

p,q prime
$(p-1)(q-1)$ must not be div by 3

$\gcd(3,(p-1)(q-1)) = 1$

$p-1 = 3k$
$\Rightarrow p = 3k+1$

$p-1$
$3, 6, 9, 12, 15,$
$p = 5$ $\quad 5-1=4$
~~$p=7$ $\quad 7-1=6$~~

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

(N, e)

$(17\times 5, 3) = (85, 3)$

(d) What is the private key?

$64 = (5-1)(17-1)$

(p, q, d)

$(5, 17, 43)$

$d \equiv e^{-1} \pmod{(p-1)(q-1)}$

$d \equiv 3^{-1} \equiv 43 \pmod{64}$

$3\times 43 = 129 \equiv 129 - 128 \equiv 1 \pmod{64}$

$128 \equiv 0 \pmod{64}$

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

$x^e \bmod N = 10^3 \bmod 85 \equiv \boxed{65} \pmod{85}$

$10^3 \equiv 100\times 10 \equiv 15\times 10 \equiv 65 \pmod{85}$

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

$y^d \bmod N$

$= 24^{43} \bmod 85$

$24^{43} \equiv x \equiv a \pmod p$ p, q coprime

$24^{43} \equiv x \equiv b \pmod q$

$p^{-1} \bmod q$

$q^{-1} \bmod p$

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

$x \equiv 24^{43} \equiv 7^{43} \equiv (-2)^{21} \cdot 7 \pmod{17}$ $7^2 = 49 \equiv -2 \pmod{17}$

$49 = 3 \cdot 17 - 2$

$x \equiv 4 \cdot q \cdot q^{-1} + 14 \cdot p \cdot p^{-1} \pmod{pq}$

$\equiv (\underbrace{(-2)^4}_{-1})^5 \cdot (-2) \cdot 7 \pmod{17}$

$\equiv (-1) \cdot (-2) \cdot 7 \equiv 14 \pmod{17}$ $43 = 2 \cdot 21 + 1$ $16 = 17 - 1$

$7^{43} = (\underbrace{7^2}_{-2})^{21} \cdot 7^1$

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.

(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?

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?

(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?