Alice (N, e) → Bobs web Eve → (N, e)

RSA

↳ cryptography

Bob → (P, q, e) → N, e⁻¹ ≡ d

Questions

(-1) mod 5 → -10 → (-5) → negative mod

Darkweb

Site (Bob) → selling has → P, q

Alice

Send M (N, e)

Public key

B (private key)

insecure

RSA Program

x

secure

RSA Program

Finite size N

name N = pq

(N, e) [d ≡ e⁻¹ mod (p-1)(q-1)]

(x^e)^d ≡ x mod N

Public key (N, e)

N = (pq)

e s.t. gcd (e, (p-1)(q-1)) = 1 coprime

large primes size bits >

RSA 1024

Proof correctness in notes ↳ FLT uses (p-1)(q-1)

FLT ↳ powerful

Private key

d ≡ e⁻¹ mod (p-1)(q-1)

↳ inverse

E(x) = x^e ≡ y Alice [mod N]

D(y) = y^d ≡ x Bob [mod N]

y E(x)

Public key

Private key

linear space ↳ file size → easy calc etc → File size N

Eve (N, e) → public

↳ knows N, e

↳ not p, q or d

→ can't decode.

↳ (1) (Brute force (N is huge)) all values x^e ≡ y mod(N) is my message

(2) mods p-1 q-1 (P, q) from N

↳ prime factoring expensive computationally

↳ primes

(P) or (q) → N/p → q

Known inefficient

Alice computer

(x^e) mod N (repeated squaring) → mod

(Binary files)

↳ almost impossible

d private key

Bobs computer

(1) [y^d mod N ↳ squaring]

(2) e⁻¹ mod (p-1)(q-1)

↳ EGCD

(3) find large primes

↳ ∃ an algo

n = m + 5

(x mod mn)

5 = mod m

0 = mod n

x mod mn

gcd (m, n)

[n = m + 5]

m+5 | x

[n | x]

find (k)

[x = n(k)_1 = mk_2 + 5]

$k_1 \neq k_2$
$nk_1 = mk_2 + 5$

$k = 1 \quad x = n = m+5$
$x = n$
$= m+5$

CS 70 Discrete Mathematics and Probability Theory
Summer 2021 DIS 3A

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?

what does e need to be for d to exist?

(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.

write p, q in terms of $k \in \mathbb{N}$

(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?

dont calc
symbolic using alg we know as abstract

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

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.

(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 trans-

missions. 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?

Answers

a) using e would mean $\gcd(e,(p-1)(q-1)) \neq 1$ ($p-1$, $q-1$ p,q primes => odd; $p-1$ $q-1$ => even)
↳ => no inverse d
↳ p,q prime => odd => (p-1)(q-1) even

b) $(e=3)$ => $\gcd(3,(p-1)(q-1))$ and p,q prime
small values
$[q,p = 3k+2]$ $k \in \mathbb{N}$
$[3k+1]$ $(3k)$ $3k+1-1 = 3k$ $\gcd \neq 1$ p,q not prime
$\gcd(3,3k) = 3$

c) (N,e) $N = [p \cdot q]$ → [factoring]
Public
$[5 \cdot 17, 3]$ → $5 \cdot 17 = 85$

d) $3d \equiv 1 \mod (5-1)(17-1)$ EGCD
$p-1$ $q-1$
$4 \cdot 16 (64)$
$d \equiv -21 \equiv 43$
Private
A
e) $E(x) = x^3 \mod 85$ (e, N) $E(10) \equiv 10^3 \equiv 65 \mod 85$
$10^3 \cdot 10$ → $15 \cdot 10$ → $[150 - 85]$ → 65
B
f) $D(y) = y^{43} \mod 85$ (d, N) has p,q ↳ CRT
$D(24) \equiv (24^{43}) \equiv 14 \mod 85$ use this algo
5 17 (p) (q)
$24^{43} \equiv a_1 \mod 5$ (p)
$24^{43} \equiv a_2 \mod 17$ (q)
$b_1 \rightarrow 17^{-1} \mod 5$
$b_2 \rightarrow 5^{-1} \mod 17$
$\equiv 0 \mod 17$
$\equiv a_2 \mod 17$
$24^{43} \equiv a_1 \cdot b_1 \cdot 17 + [a_2 \cdot b_2 \cdot 5] \mod 85$
$\equiv a_1 \mod 5$ $\equiv 0 \mod 5$
$a_1 = 4$ $a_2 = 14$
$b_1 = 3$ $b_2 = 7$
$4 \cdot 3 \cdot 17 + 14 \cdot 7 \cdot 5 \mod 85$
$\equiv 14$

2a) Take $(\gcd(p_1 q_1, p_1 q_2) = p_1)$ GCD → find p_1 computationally efficient
divide out and get q_2 or q_1
→ find $d \equiv e^{-1} \mod (p-1)(q-1)$ → private key → EGCD
↳ quads
2) p or q → other

2b) No common Factors
↳

2c) by CRT → know this same → send this under diff key

Assume

$x^3 \equiv a_1 \bmod N_1$

$x^3 \equiv a_2 \bmod N_2$

$x^3 \equiv a_3 \bmod N_3$

↳ Eve knows → crt → x^3 → message

↳ finds $x^3 \bmod (N_1 \cdot N_2 \cdot N_3)$

→ also knows $x < N_1, N_2, N_3$

$\Rightarrow x < N_1, N_2, N_3$

$(x = x^3)$

[normal cube root algorithm]

[not a wrap number → if mod 15 → 2 mod 15; no mod]

2a) Brute Force only 101 possible m values

2b) $r^e \equiv y \bmod N$ (evil)

$(mr)^e \bmod N \equiv m^e (r^e) \bmod N \equiv m^e y \bmod N$

↳ using Extend GCD find $y^{-1} \bmod N$ ⇒ (computationally efficient)

↳ $y^{-1} y m^e \equiv m^e \bmod N$

↳ brute force