RSA

CS 70 Discussion 4A

Raymond Tsao

2025-02-19

Note: These slides are unofficial course materials. Please use the notes as the only single source of truth.

Problem 1: RSA Intro

(a) Fermat's little theorem: For any prime p

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{30} \equiv 1 \pmod{31}$$

FLT allows us to quickly reduce exponents! (But only works for primes)

Euler Totient theorem: For any integer n

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Where $\phi(n)$ is the number of integers coprime to n!

There is a nice formula for $\phi(n)$ (HW Problem 2)

Problem 1: RSA Intro

(bi) Let $x = 141^{161}$, we want $x \ (mod\ 11 \cdot 17)$

Strategy 1: Use Euler Totient

Strategy 2: Take $mod\ 11$ and $mod\ 17$ separately and use CRT to get $mod\ 11 \cdot 17$

$$x = 141^{161} \equiv 9^{161} \ (mod\ 11)$$

$9^{10} \equiv 1 \ (mod\ 11)$

$$\equiv 9^{16 \cdot 10 + 1} \ (mod\ 11)$$

$$\equiv 9^{16 \cdot 10} \cdot 9^{1} \ (mod\ 11)$$

$$\equiv 1 \cdot 9^{1} \equiv 9 \ (mod\ 11)$$

$$x = 141^{161} \equiv 5^{161} \equiv 5 \ (mod\ 17)$$

Problem 1: RSA Intro

(bi) Now apply CRT!

$$x \equiv 9 \pmod{11}$$
$$x \equiv 5 \pmod{17}$$

$$x = 9a + 5b$$

Step 1: "Basis" solutions

$$a \equiv 1 \pmod{11} \qquad b \equiv 0 \pmod{11}$$
$$a \equiv 0 \pmod{17} \qquad b \equiv 1 \pmod{17}$$

Step 2: Solve for a and b

$$a = 34$$
$$b = 154$$

Solution:

$$x = 34(9) + 5(154) = 1076 \equiv 141 \pmod{187}$$

Problem 1: RSA Intro

(bi) A (slightly) more clever way

$$x = 141^{161} \equiv 141 \ \ (mod\ 11)$$

$$x = 141^{161} \equiv 141 \ \ (mod\ 17)$$

So

$$x - 141 \equiv 0 \ \ (mod\ 11)$$

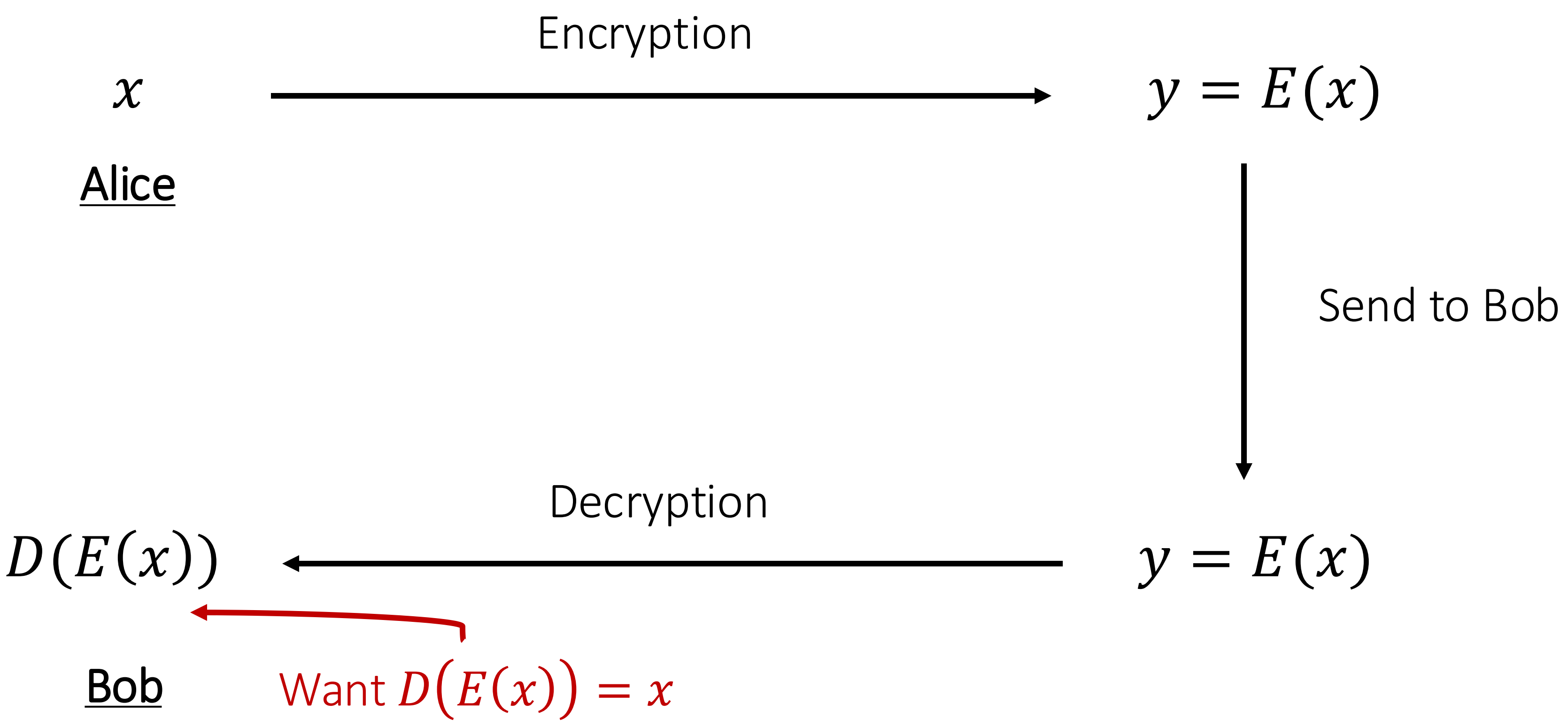
$$x - 141 \equiv 0 \ \ (mod\ 17)$$

So

$$x - 141 \equiv 0 \ \ (mod\ 11 \cdot 17)$$

Problem 1: RSA Intro

Alice want to send message x to Bob



Problem 1: RSA Intro

Setting up RSA

- Step 1: Choose (large) primes p, q
- Step 2: Define $\mathrm{N} = pq$
- Step 3: Choose e coprime to $(p-1)(q-1)$ ⟵ Public key: (N, e)
- Step 4: Choose $d \equiv e^{-1} \mod((p-1)(q-1))$ ⟵ Private key: d

Problem 1: RSA Intro

Alice want to send message x to Bob

Public key: (N, e)

x — Encryption → $y = E(x)$

$E(x) = x^e \ (mod\ N)$

Alice

Send ↓

Private key: d

$D(E(x))$ ← Decryption — $y = E(x)$

$D(y) = y^d \ (mod\ N)$

Bob

Problem 1: RSA Intro

(bii)

Strategy 3: Can we treat 141^{161} $(mod\ 187)$ as a RSA encoding/decoding scheme

Is this $e, d,$ or ed?

$$141^{161}\ (mod\ 187)$$

Message: $x = 141$

$N = 187, p = 11, q = 17$

Note that $161 = 7 \cdot 23$

And $7 \cdot 23 \equiv 1\ \ (mod\ 160)$

e d

Problem 2: RSA Warm-Up

(a, b, c)

Setting up RSA

e cannot be even!

- Step 1: Choose (large) primes p, q — $p = 5, q = 17$
- Step 2: Define $\mathrm{N} = pq$ — $N = pq = 85$
- Step 3: Choose e coprime to $(p-1)(q-1)$ — $e = 3$
- Step 4: Choose $d \equiv e^{-1} \mod((p-1)(q-1))$ — $d = 3^{-1}\, mod\; 64 = 43$

Public key: $(\mathrm{N}, \mathrm{e}) = (85, 3)$

Private key: $\mathrm{d} = 15$

Problem 2: RSA Warm-Up

(d) Alice send message $\mathbf{10}$ to Bob

x —— Encryption ——→ $y = E(x)$

$E(x) = x^3 \ (mod\ 85)$

<u>Alice</u>

Problem 2: RSA Warm-Up

(d) Alice send message 10 to Bob

Public key: $(85, 3)$

x

Alice

Encryption

$E(x) = x^3 \ (mod\ 85)$

$y = E(x)$

Problem 2: RSA Warm-Up

(d) Alice send message 10 to Bob

Public key: $(85, 3)$

10

Alice

Encryption

$E(x) = x^3 \ (mod\ 85)$

$y = E(x)$

Problem 2: RSA Warm-Up

(d) Alice send message 10 to Bob

Public key: $(85, 3)$

10

Alice

Encryption

$E(10) = 10^3 \ (mod\ 85)$

$y = E(x)$

Problem 2: RSA Warm-Up

(d) Alice send message 10 to Bob

Public key: $(85, 3)$

10

Alice

Encryption

$E(10) = 10^3 \ (mod\ 85)$

$y = 65$

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Decryption

$D(y)$ ← $y = 19$

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

Bob

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Decryption

Private key: 15

$D(y)$ ← $y = 19$

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

Bob

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Private key: 15

$D(y)$

Decryption

$y = 19$

$D(19) = 19^{43}\ (mod\ 85)$

Bob

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Decryption

Private key: 15 $\quad 59 \longleftarrow y = 19$

$D(19) = 19^{43} \ (mod\ 85)$

Bob

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Private key: 15

59

Bob

Decryption

$D(19) = 19^{43}\ (mod\ 85)$

$y = 19$

Step 1: Use FLT to reduce $mod\ 5, mod\ 17$

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Decryption

Private key: 15

59 ← $y = 19$

$D(19) = 19^{43}\ (mod\ 85)$

<u>Bob</u>

Step 1: Use FLT to reduce $mod\ 5, mod\ 17$

$$x \equiv 4\ \ (mod\ 5)$$

$$x \equiv 8\ \ (mod\ 17)$$

Problem 2: RSA Warm-Up

(e) Bob recieves 19 from Alice

Private key: 15

59

Bob

Decryption

$D(19) = 19^{43}\ (mod\ 85)$

$y = 19$

Step 1: Use FLT to reduce $mod\ 5, mod\ 17$

$$x \equiv 4\ \ (mod\ 5)$$

$$x \equiv 8\ \ (mod\ 17)$$

Step 2: Use CRT to find the solution $mod\ 85$

Problem 2: RSA Warm-Up

(f) Assumptions in RSA

Assumption 1: Factorizing $N = pq$ is hard

- Otherwise we can find the private key!

Assumption 2: Given y it is hard to solve

$$y \equiv x^e \ (mod\ N)$$

- Otherwise we can just solve for the message x!

Secret word: Chinchilla

Secret word: Meerkat