Euler's Theorem and Public-Key Encryption

Lecture 16, CS 284, Autumn 2021

David Cash

Outline

1. Recall groups and prove Euler's Theorem
2. The groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$
3. Public Key Encryption Definitions
4. RSA Encryption

Outline

1. Recall groups and prove Euler's Theorem
2. The groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$
3. Public Key Encryption Definitions
4. RSA Encryption

Definition of a Group (Recall)

Def A non-empty set G with binary operation $\circ$ is called a group if the following hold:

(Identity) ① There exists $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.

(Inverses) ② For all $g \in G$ there is $h \in G$ such that $g \circ h = h \circ g = e$.

(Associativity) ③ For all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

G is called an abelian group if it also satisfies

(Commutativity) ④ For all $g, h \in G$, $g \circ h = h \circ g$.

Notation

- $g^a = \underbrace{g \circ g \circ \cdots \circ g}_{a \text{ times}}$

- g^{-1} is the inverse of g

- $g^{-a} = \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{a \text{ times}}$

Claim $g^a \circ g^b = g^{a+b}$

Claim $(g^a)^b = g^{ab}$

Example

$G = \{0,1\}^n$, operation bitwise XOR. $x \oplus y$

ID: 0^n $\quad x \oplus 0^n = 0^n \oplus x = x$

Inverse: $x^{-1} = x$ $\quad$ ∵ $x \oplus x^{-1} = x \oplus x = 0^n$ (identity)

Assoc: $(x \oplus y) \oplus z = x \oplus (y \oplus z)$

Comm: $x \oplus y = y \oplus x$

Identity is Unique in a Group.

Claim Let G be a group. If $e_1, e_2 \in G$ both satisfy the condition for being an identity, then $e_1 = e_2$.

Identity is Unique in a Group.

Claim Let G be a group. If $e_1, e_2 \in G$ both satisfy the condition for being an identity, then $e_1 = e_2$.

Proof We are given that

$$e_1 \circ g = g \circ e_1 = g \text{ for all } g \in G, \qquad (*)$$

and

$$e_2 \circ g = g \circ e_2 = g \text{ for all } g \in G. \qquad (**)$$

Apply $(*)$ with $g = e_2$: $e_1 \circ e_2 = e_2$. Next apply $(**)$ with $g = e_1$ to get $e_1 \circ e_2 = e_1$. Since $e_1 \circ e_2 = e_2$ and $e_1 \circ e_2 = e_1$, $e_1 = e_2$.

Inverses are Unique in a Group

Claim Let G be a group and $g \in G$. If $h_1, h_2 \in G$ both satisfy the condition for being an inverse of g, then $h_1 = h_2$.

Inverses are Unique in a Group

Claim Let G be a group and $g \in G$. If $h_1, h_2 \in G$ both satisfy the condition for being an inverse of g, then $h_1 = h_2$.

Proof We are given that $g \circ h_1 = h_1 \circ g = e$, and $g \circ h_2 = h_2 \circ g = e$.

Consider $h_2 \circ g \circ h_1$. Since h_1 is an inverse of g,

$$h_2 \circ g \circ h_1 = h_2 \circ (g \circ h_1) = h_2 \circ e = h_2.$$

But h_2 is also an inverse of g, so

$$h_2 \circ g \circ h_1 = (h_2 \circ g) \circ h_1 = e \circ h_1 = h_1.$$

Thus $h_2 \circ g \circ h_1 = h_2$ and $= h_1$, so $h_1 = h_2$.

Cancelation in Groups

Lets start omitting the "$\circ$"

Claim Let G be a group and $g, h, k \in G$. If $gh = kh$, then $g = k$.

Cancelation in Groups

Lets start omitting the "$\circ$"

Claim Let G be a group and $g, h, k \in G$. If $gh = kh$, then $g = k$.

Proof The following are equivalent:

$$① \quad gh = kh$$

existence of inverses

$$② \quad (gh)h^{-1} = (kh)h^{-1}$$

Associativity

$$③ \quad g(hh^{-1}) = k(hh^{-1})$$

Def of Inv.

$$④ \quad ge = ke$$

Def of Ident.

$$⑤ \quad g = k$$

Order of a Group + An Interesting Theorem

Def The order of group G is simply $|G|$, the size of G as a set when G is finite.

Theorem Let G be an abelian group of (finite) order m. Then for every $g \in G$,

$$g^m = e.$$

$G = \{0,1\}^n$

$|G| = 2^n$

$g \in G$

$\underbrace{g \oplus g \oplus \cdots \oplus g}_{2^n} = 0^n$

A Lemma used to Prove Theorem

<u>Lemma</u> Let G be an abelian group of order m, and let $g_1, g_2, \dots, g_m$ be the elements of G written in some order. Let $g \in G$ and define $h_1 = gg_1$, $h_2 = gg_2, \dots, h_m = gg_m$. Then $h_1, h_2, \dots, h_m$ are all distinct. Thus $h_1 \dots h_m$ is just all of the elements of G, possibly in a different order.

<u>Proof</u>: If $h_i = h_j$ then $gg_i = gg_j$. By Cancelation, $g_i = g_j$. But we assumed these were distinct, so this is a contradiction.

Theorem Let G be an abelian group of (finite) order m. Then for every $g \in G$,

$$g^m = e.$$

Theorem Let G be an abelian group of (finite) order m. Then for every $g \in G$,

$$g^m = e.$$

Proof We claim that $g_1 \circ g_2 \circ \cdots \circ g_m = (gg_1) \circ (gg_2) \circ \cdots \circ (gg_m)$.

By the lemma, both sides are products of all elements of G, possibly in a different order. But since G is abelian, order does not change the product.

Next, the right hand side equals $g^m (g_1 \circ g_2 \circ \cdots \circ g_m)$, so

$$g_1 \circ g_2 \circ \cdots \circ g_m = g^m (g_1 \circ g_2 \circ \cdots \circ g_m).$$

How to finish? Cancel $g_1 \circ g_2 \cdots g_m$ on both sides: $e = g^m$.

Theorem Let G be an abelian group of (finite) order m. Then for every $g \in G$,

$$g^m = e.$$

Corollary Let G be a finite abelian group of order $m > 1$. Then for any $g \in G$ and any integer i, $g^i = g^{[i \bmod m]}$.

<u>Corollary</u> Let G be a finite abelian group of order $m > 1$. Then for any $g \in G$ and any i, $g^i = g^{[i \bmod m]}$.

<u>Proof</u> Use division with remainder to find q, r such that

$$i = qm + r, \qquad 0 \leq r < m.$$

Then $r = [i \bmod m]$. We set

$$g^i = g^{qm+r} = g^{qm} \circ g^r = (g^m)^q \circ g^r = e^q \circ g^r = g^r$$

which is $g^{[i \bmod m]}$.

Corollary Let G be a finite abelian group of order $m>1$. Let $e>0$ be an integer relatively prime to m. Then the function f_e,

$$f_e : G \to G, \qquad g \mapsto g^e$$

$f_e(g) = g^e$

is a permutation. Moreover, if d is an inverse of e modulo m, then

$$f_d : G \to G \qquad g \mapsto g^d$$

$f_d(g) = g^d$

is the inverse of f_e.

For all g

$f_d(f_e(g)) = g$

$= f_e(f_d(g))$

Proof For any $g \in G$

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{ed}.$$

Since we can mod down the exponent by the group order,

$$g^{ed} = g^{[ed \bmod m]}. \quad = g^1 = g$$

Since d is an inverse of e modulo m, $[ed \bmod m] = 1$, and we get

$$f_d(f_e(g)) = g.$$

This show f_d is the inverse of f_e, and that f_e must be a perm!

Outline

1. Recall groups and prove Euler's Theorem
2. The groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$
3. Public Key Encryption Definitions
4. RSA Encryption

$\mathbb{Z}_N$: Groups with Modular Addition

$\mathbb{Z}/N\mathbb{Z}$ math notation

Def For a positive integer N, define $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$.

$|\mathbb{Z}_N| = N$

Claim For each positive integer N, $\mathbb{Z}_N$ with operation

$$x \circ y = [x + y \bmod N]$$

is a group.

Proof:

ID : 0

INV : inverse of $x = N - x$ if $x \neq 0$, o/w 0

Assoc: ✓

$$\begin{aligned} x \circ (N-x) &= [x + N - x \bmod N] \\ &= [N \bmod N] \\ &= 0 \in \mathbb{Z}_N \end{aligned}$$

Groups with Modular Multiplication

Is $\mathbb{Z}_N$ also a group with operation $x \circ y = [xy \bmod N]$?

Groups with Modular Multiplication

Is $\mathbb{Z}_N$ also a group with operation $x \circ y = [xy \bmod N]$?

↳ No! $0 \in \mathbb{Z}_N$ causes problems. (What is identity? Inverse of 0?)

Groups with Modular Multiplication

Is $\mathbb{Z}_N$ also a group with operation $x \circ y = [xy \bmod N]$?

↳ No! $0 \in \mathbb{Z}_N$ causes problems. (What is identity? Inverse of 0?)

What if we toss out 0? $\mathbb{Z}_N \setminus \{0\}$

Groups with Modular Multiplication

Is $\mathbb{Z}_N$ also a group with operation $x \circ y = [xy \bmod N]$?

↳ No! $0 \in \mathbb{Z}_N$ causes problems. (What is identity? Inverse of 0?)

What if we toss out 0?

↳ No, see example.

<u>Example</u> $\mathbb{Z}_4 \setminus \{0\} = \{1,2,3\}$ is still not a group with $x \circ y = [xy \bmod 4]$.

The group operation isn't even valid! $2 \in \mathbb{Z}_4$, but $2 \circ 2 = [2 \cdot 2 \bmod 4] = 0 \notin \mathbb{Z}_4$.

The Group $\mathbb{Z}_N^*$

<u>Intuition:</u> Need to throw out not just $0 \in \mathbb{Z}_N$, but everything that does not have an inverse.
modular

<u>Def</u> For a positive integer N, define

$$\mathbb{Z}_N^* = \{ x \mid 1 \leq x < N,\ \gcd(x, N) = 1 \}.$$

<u>Claim</u> For each positive integer N, $\mathbb{Z}_N^*$ with operation $x \circ y = [xy \bmod N]$ is a group.

<u>Proof Sketch</u>: <u>ID</u> 1 ✓ <u>INV</u> x^{-1} is modular inverse of $x \bmod N$ <u>ASSOC</u>: ✓

The Order of $\mathbb{Z}_N^*$

Examples

$\mathbb{Z}_4^* =$

ON BOARD

$\mathbb{Z}_5^* =$

$\mathbb{Z}_{15}^* =$

Def The "Euler-phi function" φ is defined to be $\varphi(N) = |\mathbb{Z}_N^*|$.

\varphi

not \phi

Two Special Cases of $\phi(n)$

Claim If p is prime, then $\phi(p) = p-1$.

Example $|\mathbb{Z}_5^*| = 5-1 = 4$

Claim If $p \neq q$ are both prime, then $\phi(pq) = (p-1)(q-1) = pq - p - q + 1$

Proof $\mathbb{Z}_{pq} = \{0 \; 1 \; \dots p \dots q \dots 2p \dots 2q \dots \dots pq-1\}$

$\rightarrow$ q mults of p

$\rightarrow$ p mults of q

Euler's Theorem (!)

Theorem For any positive integer N, and integer a relatively prime to N,

$$a^{\varphi(N)} \equiv 1 \mod N.$$

Proof In $\mathbb{Z}_N^*$, $g^{|\mathbb{Z}_N^*|} = 1$ for any $g \in \mathbb{Z}_N^*$.

$\varphi(N)$

Outline

1. Recall groups and prove Euler's Theorem
2. The groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$
3. Public Key Encryption Definitions
4. RSA Encryption

Public-Key Encryption Syntax

Def A *public-key encryption scheme* Π consists of three algorithms $\Pi = (\text{Keygen}, \text{Enc}, \text{Dec})$, where

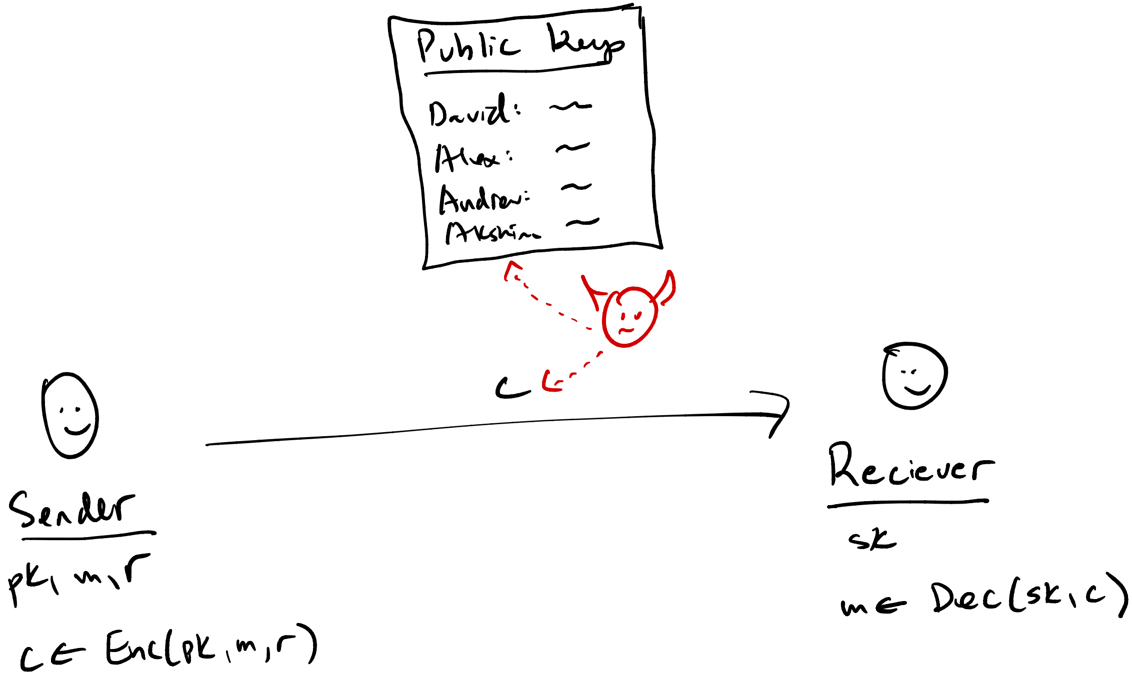
- Keygen is randomized, takes no input besides random bits, and outputs two keys (pk, sk).
- Enc is randomized (with input r written explicitly), takes two more inputs pk, m, and outputs a ciphertext.
- Dec is deterministic, takes inputs sk, c and outputs m.

Correctness of Public-Key Encryption

Π is correct if for all (pk, sk) output by Keygen, and all messages m, and all r,

$$\mathrm{Dec}(sk, \mathrm{Enc}(pk, m, r)) = m.$$

Chosen-Plaintext Attack Security: Motivation



- has pk and c, but not sk or r
- wants info about m; can influence what sender encrypts

Chosen-Plaintext Attack Security: Definition

Def Let $\Pi = (\text{Keygen}, \text{Enc}, \text{Dec})$ be a public-key encryption scheme, and let $\mathcal{A}$ be an adversary. Define $\text{Expt}_\Pi^{cpa}(\mathcal{A})$ by

$\underline{\text{Expt}_\Pi^{cpa}(\mathcal{A})}$

1. Run $(pk, sk) \leftarrow \text{Keygen}()$
2. Give pk to $\mathcal{A}$. It chooses two messages m_0, m_1.
3. Pick $b \in \{0,1\}$, random r, compute $c \leftarrow \text{Enc}(pk, m_b, r)$.
4. Give c to $\mathcal{A}$. It outputs $\hat{b}$.
5. If $\hat{b} = b$ output 1. Else output 0.

Define $\text{Adv}_\Pi^{cpa}(\mathcal{A}) = \left| \Pr[\text{Expt}_\Pi^{cpa}(\mathcal{A}) = 1] - \frac{1}{2} \right|$.

Chosen-Plaintext Attack Security: Discussion

* No oracle for Enc; Just "one shot" for $\mathcal{A}$.
  - ↳ But giving an oracle actually does not change definition much.

* Deterministic Enc algorithm $\Rightarrow$ Can't have good CPA security

The End