0. warm-up exercises

Algebra $(A, \circ, *, \cdot, + \cdots)$ [closure]

$(A, \circ)$, $\circ : A \times A \to A$

↓ semigroup [associativity]

↓ monoid [identity e]

a. where do they belong?

$(\mathbb{R}, +)$, $(\mathcal{P}(X), \cup)$, $(M_n, \cdot)$

$M_n := \{n \times n \text{ matrices}\}$

$e = \mathbb{1}_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

↑ Algebra

$(\mathbb{Q}, +)$ $(\mathbb{Q}, \div)$, $(\mathbb{Z}, \div)$

$(6 \div 3) \div 2$! NOT A algebra

$\neq 6 \div (3 \div 2)$

b. which are commutative?

All but $(M_n, \cdot)$, $(\mathbb{Q}, \div)$

c. Is any one a sub algebra of another?

$(\mathbb{Q}, +)$ => subalgebra of $(\mathbb{R}, +)$

1. Basics of groups

Group = monoid + inverse

- **DEF:** $(G, \circ)$ $\circ : G \times G \to G$ is a group if satisfying:

monoid:
- (Associality) $\forall a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$
- (Identity) $\exists e \in G$ s.t. $\forall a \in G$, $a \circ e = a$.
- (Inverse) $\forall a \in G$, $\exists a' \in G$, s.t. $a \circ a' = a' \circ a = e$

(a' is called inverse of a, a^{-1})

$(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$

- **Abelian group**: commutativity

(Abel) $\forall a, b \in G$, $a \circ b = b \circ a$.

- $(A = \{0,1\}^n, \oplus)$ $\oplus$: bit-wise xor

$x = x_1 \dots x_n$

$y = y_1 \dots y_n$

$x \oplus y = z = z_1 \dots z_n$

$z_i = x_i \oplus y_i$

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Claim: $(A, \oplus)$ is a group. (Abelian)

PE: - (Assoz.) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$

- (identity) $e = 0^n$, $\forall x \quad x \oplus 0^n = x$

- (inverse) $\forall x = x_1 \dots x_n \in A$

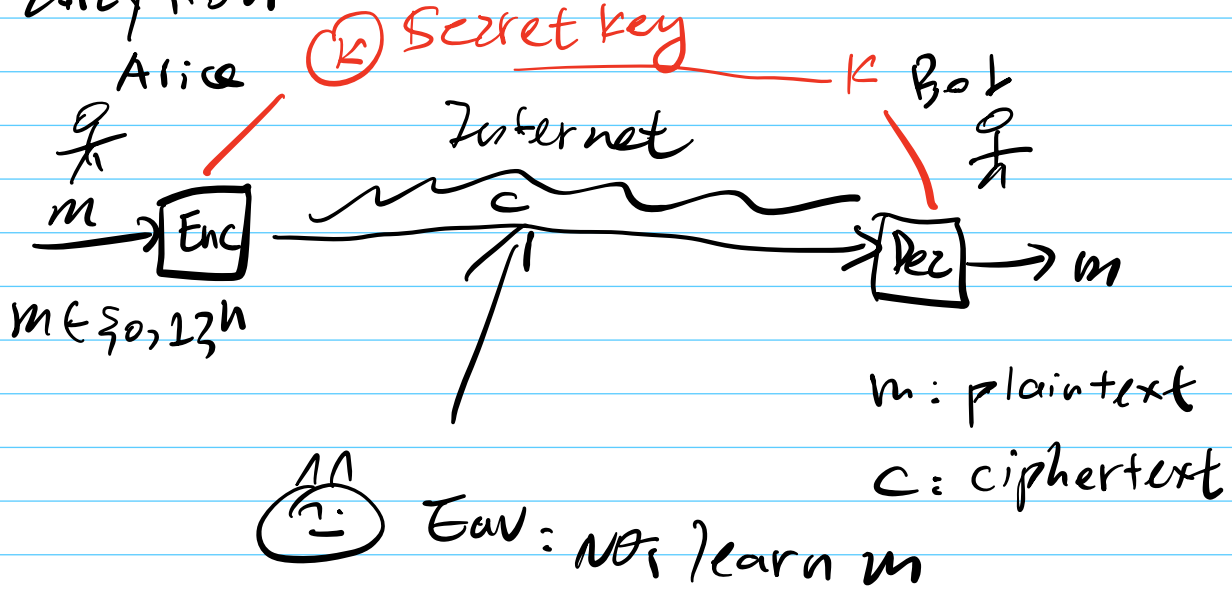
$x^{-1} := x_1 \cdots x_n$

s.t. $x \oplus x^{-1} = e = 0^n$

$\forall a \in \{0,1\} \quad a \oplus a = 0$

2. A first touch on cryptography.

a. Encryption



- Kirkhoff's law:

CRYPTO Algs must be assumed to be known by all, esp. attackers.

$Enc: (m, k) \longmapsto c$

$Dec: (c, k) \longmapsto m$

c. one-time pad (OTP)

- KeyGen: $k \xleftarrow{\$} \{0,1\}^n$
  (uniformly random).
- E: on input $m \in \{0,1\}^n$

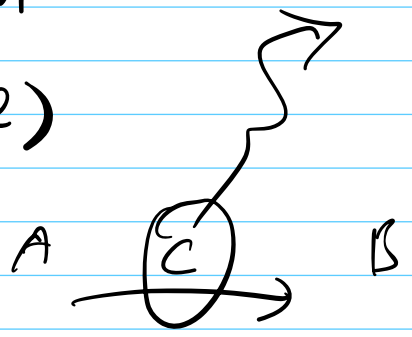
$$c := m \oplus k$$

- D: on ciphertext c

$$m := c \oplus k$$
$$= (m \oplus k) \oplus k$$
$$= m \oplus (k \oplus k)$$
$$= m \oplus 0^n$$
$$= m$$

(e)

→ correctness ✓



→ Security:

observe c
$\xrightarrow{?}$ infer m ✓

observation: works in any group.

★ key exchange

3. Number theory in 30 mins.

a. Divisibility.

- $\mathbb{Z}$: integers $= \{\dots -2, -1, 0, 1, 2 \dots\}$.

  $a \in \mathbb{Z}$. $\|a\|$: length of binary rep.

  $\|5\| = 3$

  101

- $\mathbb{N} = \{0, 1, \dots\}$.

- $k \mid n$: k divides n $\quad 3 \mid 15$

- prime number: p.
  - $p \geq 2$. & divisors are 1 & p.
  - o.w. composite number.

- integer op's
  - $a+b$. $\quad a \cdot b$. $\quad a, b$ n-bit

    $O(n)$ $\quad O(n^2)$

    ↓

    meas. complexity bit op's.

b. modular arithmetic.

- $a, N \in \mathbb{Z}$. $N \geq 2$

  $a = qN + r$

  q: quotient, r: remainder

- $a, b, N \in \mathbb{Z}$: write $a = b \bmod N$ (modulus)

  iff a, b same remainders

divided by N.

- $\mathbb{Z}_N = \{0, \ldots, N-1\}$.
  - mod. add. $+$ mod N $(+_N)$
  - mod. mult. $\cdot$ mod N $(\cdot_N)$.

$N=15$, $2+14 = 1 \mod 15$

$3 \cdot 9 = 12 \mod 15$

$\forall a \in \mathbb{Z}_N$ has a unique additive inverse.

$b \in \mathbb{Z}_N$, s.t. $a+b = 0 \mod N$

Cor: $(\mathbb{Z}_N, +_N)$ is a group.

☹ NOT always $a' \in \mathbb{Z}_N$ (mult. inverse)

s.t. $a \cdot a' = 1 \mod N$.

Ex: $N=6$, $a=2$ $\mathbb{Z}_6$

$2 \cdot 1 = 2$

$\cdot 2 = 4$

$\cdot 3 = 0$

$\cdot 4 = 2$

$\cdot 5 = 4$

mod 6.

- greatest common divisor (gcd)
  - gcd(a,b) : largest int. that divides a & b.

gcd(6,10) = 2

- Euclidean alg. computes gcd(a,b)

in poly(||a||, ||b||, ||N||).

- **Thm:** $a \in \mathbb{Z}_N$ has an mult. inverse iff. $\gcd(a, N) = 1$
  - ↓ coprime.
- $\mathbb{Z}_N^* := \{ a \in \mathbb{Z}_N : \gcd(a, N) = 1 \}$.
  - Ex: $\mathbb{Z}_6^* = \{1, 5\}$ (0, 1, 2, 3, 4, 5)

Cor: $(\mathbb{Z}_N^*, \cdot_N)$ is a group.

- Euler's function: $\phi(N) := |\mathbb{Z}_N^*|$

  FACT: $\phi(P \cdot Q) = (P-1) \cdot (Q-1)$

- Modular exponentiation.
  - $a \in \mathbb{Z}_N$ $b > 0$.
  - $a^b \bmod N$ $\quad \underbrace{a \cdots a}_{b \text{ times}} \bmod N$
  - Repeated squaring alg.

    $a^b \bmod N$ in poly(||a||, ||b||).
- **Thm** (Euler's thm)

  If $N \geq 2$, $a \in \mathbb{Z}_N$, then $a^{\phi(N)} = 1 \bmod N$

4. Factoring & RSA

a. Factoring

- Given: $n = p \cdot q$. p, q n-bit random primes
  Goal: find p.
- Best Alg (Known) (classical) $\sim \exp(n^{1/3} \cdot \log n^{2/3})$

b. RSA problem.

- consider $\mathbb{Z}_N^*$, $\phi(N) = |\mathbb{Z}_N^*|$
  - p, q n-bit random prime.
  - $N = p \cdot q$.
  - pick $e > 0$ s.t. $\gcd(e, \phi(N)) = 1$. ($\neq$ identity)
  - computed. $\exists d$ s.t. $ed = 1 \bmod \phi(N)$.
- Two functions:

$$F_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \qquad F_d : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$$
$$x \mapsto x^e \bmod N \qquad y \mapsto y^d \bmod N$$

- Claim: $(F_e)^{-1} = F_d$
  $\forall x \in \mathbb{Z}_N^*$, $F_d(F_e(x)) = x$

Pf: $\forall x$. $F_e(x) = x^e \bmod N$

$$F_d(F_e(x)) = (x^e)^d = x^{ed} = x^{k \cdot \phi(N)} \cdot x \pmod N$$

$ed = k \cdot \phi(N) + 1$

$$= (x^{\phi(N)})^k \cdot x = x$$

($x^{\phi(N)} = 1$)

Conj.: inverting x^e is hard if d is unknown

c. Exchange a key in public.