Securitatea Sistemelor Informatice

- Curs 8.4 -
Teoria numerelor pentru criptografie

Adela Georgescu

Facultatea de Matematică și Informatică
Universitatea din București
Anul universitar 2022-2023, semestrul I

Notații

- $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
- $\mathbb{N} = \{0, 1, 2, ...\}$
- $\mathbb{Z}_{+} = \{..., -2, -1, 0, 1, 2, ...\}$
- Pentru $a, n \in \mathbb{N}$ notăm $gcd(a, n)$ ca fiind cel mai mare divizor comun (greatest commun divisor) al lui a și n.
- Exemplu: $gcd(30, 50) = 10$.

Intregi modulo N

- pentru $n \in \mathbb{Z}_+$ notăm
  - $\mathbb{Z}_n = \{0, 1, ..., n-1\}$
  - $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$
  - $\phi(n) = |\mathbb{Z}_n^*|$

Intregi modulo N

- pentru $n \in \mathbb{Z}_+$ notăm
  - $\mathbb{Z}_n = \{0, 1, ..., n-1\}$
  - $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$
  - $\phi(n) = |\mathbb{Z}_n^*|$
- Exemplu: n=12

Intregi modulo N

- pentru $n \in \mathbb{Z}_+$ notăm
  - $\mathbb{Z}_n = \{0, 1, ..., n-1\}$
  - $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$
  - $\phi(n) = |\mathbb{Z}_n^*|$
- Exemplu: n=12
  - $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Intregi modulo N

- pentru $n \in \mathbb{Z}_+$ notăm
  - $\mathbb{Z}_n = \{0, 1, ..., n-1\}$
  - $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$
  - $\phi(n) = |\mathbb{Z}_n^*|$
- Exemplu: n=12
  - $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
  - $\mathbb{Z}_{12}^*$ =$\{$1,5,7,11$\}$

Intregi modulo N

- pentru $n \in \mathbb{Z}_+$ notăm
  - $\mathbb{Z}_n = \{0, 1, ..., n-1\}$
  - $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$
  - $\phi(n) = |\mathbb{Z}_n^*|$
- Exemplu: n=12
  - $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
  - $\mathbb{Z}_{12}^*$ ={1,5,7,11}
  - $\phi(12) = 4$

Impărțire și rest

- $a = qn + r$ cu $0 \leq r < n$.
  Considerăm împărțirea lui a la n.
  Atunci q este catul împărțirii iar r este restul și notăm

$$a \bmod n = r$$

- Exemplu: $17 \bmod 3 = 2$.
- $a = b \bmod n$ dacă $a \bmod n = b \bmod n$.

Grupuri și invers

- Dacă $n \in \mathbb{Z}_+$ atunci $G = \mathbb{Z}_n^*$ împreună cu operația "*" definită

$$a * b = ab \bmod n$$

pentru $a, b \in G$ formează un grup si are cele trei proprietăți:

- asociativitatea: operatia * este asociativă
- element neutru: există un element $1 \in G$ așa încat $a * 1 \bmod n = 1 * a \bmod n = a$, $\forall a \in G$.
- element inversabil: pentru orice $a \in G$ exista un unic $b \in G$ asa incat $a * b = b * a = 1 \bmod n$.
  b se numeste inversul lui a și îl notăm cu $a^{-1} \bmod n$.

Grupuri și invers

- Dacă $n \in \mathbb{Z}_+$ atunci $G = \mathbb{Z}_n^*$ împreună cu operația "*" definită

$$a * b = ab \bmod n$$

pentru $a, b \in G$ formează un grup si are cele trei proprietăți:

  - asociativitatea: operatia * este asociativă
  - element neutru: există un element $1 \in G$ așa încat $a * 1 \bmod n = 1 * a \bmod n = a$, $\forall a \in G$.
  - element inversabil: pentru orice $a \in G$ exista un unic $b \in G$ asa incat $a * b = b * a = 1 \bmod n$.
    b se numeste inversul lui a și îl notăm cu $a^{-1} \bmod n$.
  - Exemplu: $5^{-1} \bmod 12$ este acel număr $b \in G$ care satisface $5b \bmod 12 = 1$

Grupuri și invers

- Dacă $n \in \mathbb{Z}_+$ atunci $G = \mathbb{Z}_n^*$ împreună cu operația "*" definită

$$a * b = ab \bmod n$$

pentru $a, b \in G$ formează un grup si are cele trei proprietăți:

  - asociativitatea: operatia * este asociativă
  - element neutru: există un element $1 \in G$ așa încat $a * 1 \bmod n = 1 * a \bmod n = a$, $\forall a \in G$.
  - element inversabil: pentru orice $a \in G$ exista un unic $b \in G$ asa incat $a * b = b * a = 1 \bmod n$.
    b se numeste inversul lui a și îl notăm cu $a^{-1} \bmod n$.
  - Exemplu: $5^{-1} \bmod 12$ este acel număr $b \in G$ care satisface $5b \bmod 12 = 1$
  - deci b = 5.

Scurtături computaționale

- calculați $5 * 8 * 10 * 16 \bmod 21$.
- Prima variantă: Calculăm mai întai $5 * 8 * 10 * 16 = 6400$ si apoi calculam $6400 \bmod 21 = 16$
- A doua variantă (mai rapidă):
  - $5 * 8 \bmod 21 = 40 \bmod 21 = 19$
  - $19 * 10 \bmod 21 = 190 \bmod 21 = 1$
  - $1 * 16 \bmod 21 = 16$

Ordinul unui grup

- Ordinul unui grup G este numărul de elemente din acel grup, îl notăm cu $|G|$.
- Exemplu: Ordinul lui $\mathbb{Z}_{21}^* = 12$ pentru că

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

- Fie G un grup de ordin m si $a \in G$. Atunci:
  - $a^m = 1$.
  - Pentru orice $i \in \mathbb{Z}$, $a^i = a^{i \bmod m}$.

Ordinul unui grup

- Ordinul unui grup G este numărul de elemente din acel grup, îl notăm cu $|G|$.

- Exemplu: Ordinul lui $\mathbb{Z}_{21}^* = 12$ pentru că

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

- Fie G un grup de ordin m si $a \in G$. Atunci:
  - $a^m = 1$.
  - Pentru orice $i \in \mathbb{Z}$, $a^i = a^{i \bmod m}$.
  - Exemplu: Calculați 5^{74} mod 21.

Ordinul unui grup

- Ordinul unui grup G este numărul de elemente din acel grup, îl notăm cu $|G|$.
- Exemplu: Ordinul lui $\mathbb{Z}_{21}^* = 12$ pentru că

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

- Fie G un grup de ordin m si $a \in G$. Atunci:
  - $a^m = 1$.
  - Pentru orice $i \in \mathbb{Z}, a^i = a^{i \bmod m}$.
  - Exemplu: Calculați $5^{74} \bmod 21$.
  - Răspuns: Fie $\mathbb{Z}_{21}^*$ si $a = 5$. Atunci $m = 12$ și

Ordinul unui grup

- Ordinul unui grup G este numărul de elemente din acel grup, îl notăm cu $|G|$.
- Exemplu: Ordinul lui $\mathbb{Z}_{21}^* = 12$ pentru că

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

- Fie G un grup de ordin m si $a \in G$. Atunci:
  - $a^m = 1$.
  - Pentru orice $i \in \mathbb{Z}, a^i = a^{i \bmod m}$.
  - Exemplu: Calculați $5^{74} \bmod 21$.
  - Răspuns: Fie $\mathbb{Z}_{21}^*$ si $a = 5$. Atunci $m = 12$ și
  - $5^{74} \bmod 21 = 5^{74 \bmod 12} \bmod 21 = 5^2 \bmod 21 = 4$.