Криптографија
- први део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

27. фебруар 2024.

Литература

- Neal Koblitz: *A course in number theory and criptography*, 2nd edition, Springer-Verlag, 1994.
- William Stein: *Elementary number theory: primes, conguences, and secrets*, 2017.
- Миодраг Живковић: *Криптографија*, 2020.

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)
  - Декодирање

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)
  - Декодирање
- У (де)кодирању нема ничег тајног.

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)
  - Декодирање
- У (де)кодирању нема ничег тајног.
- Криптосистем је пар: Алгоритам за криптовање и алгоритам за декриптовање

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)
  - Декодирање
- У (де)кодирању нема ничег тајног.
- Криптосистем је пар: Алгоритам за криптовање и алгоритам за декриптовање
  - Алгоритми су најчешће свима познати

Криптографија

- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата
  - Декриптовање (дешифровање)
  - Декодирање
- У (де)кодирању нема ничег тајног.
- Криптосистем је пар: Алгоритам за криптовање и алгоритам за декриптовање
  - Алгоритми су најчешће свима познати
  - Увек зависе од параметра који се зове кључ, и који се чува у тајности (потпуно или делимично)

- Обично:
  - Алиса шаље поруку Бобану

- Обично:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (криптоанализа)

- Обично:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол

- Обично:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол
  - Блоковска - групише симболе у биграфе, триграфе,... и њих трансформише

- Обично:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол
  - Блоковска - групише симболе у биграфе, триграфе,... и њих трансформише
- Врсте криптосистема:
  - Симетричан - Алиса и Бобан користе исти кључ за (де)криптовање. Унапред договоре кључ и чувају га у тајности. Кључ се периодично мења. Непрактично када имамо велики број корисника и свако комуницира са сваким.

- Обично:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол
  - Блоковска - групише симболе у биграфе, триграфе,... и њих трансформише
- Врсте криптосистема:
  - Симетричан - Алиса и Бобан користе исти кључ за (де)криптовање. Унапред договоре кључ и чувају га у тајности. Кључ се периодично мења. Непрактично када имамо велики број корисника и свако комуницира са сваким.
  - Асиметричан (криптосистем са јавним кључем) - Алиса и Бобан праве сопствене кључеве, кључ за криптовање објављују, док кључ за декриптовање чувају у тајности.

Пример: Цезарова шифра

Слова $A - Z$ кодирамо са $\{0, \ldots, 25\} = \mathbb{Z}_{26}$, проточна шифра:

$$f(P) = P + b \bmod 26$$

где је $\in \mathbb{Z}_{26}$ кодирани симбол, $b = 16$ тајни кључ.

Пример: Цезарова шифра

Слова $A - Z$ кодирамо са $\{0, \ldots, 25\} = \mathbb{Z}_{26}$, проточна шифра:

$$f(P) = P + b \bmod 26$$

где је $\in \mathbb{Z}_{26}$ кодирани симбол, $b = 16$ тајни кључ.
Алиса хоће да пошаље поруку $'PAYMENOW'$, она кодира

$$'PAYMENOW' \longrightarrow 15\ 0\ 24\ 12\ 4\ 13\ 14\ 22$$
$$\xrightarrow{f} 5\ 16\ 14\ 2\ 20\ 3\ 4\ 12 \longrightarrow 'FQOCUDEM'$$

Пример: Цезарова шифра

Слова $A - Z$ кодирамо са $\{0, \ldots, 25\} = \mathbb{Z}_{26}$, проточна шифра:

$$f(P) = P + b \bmod 26$$

где је $\in \mathbb{Z}_{26}$ кодирани симбол, $b = 16$ тајни кључ.
Алиса хоће да пошаље поруку $'PAYMENOW'$, она кодира

$$'PAYMENOW' \longrightarrow 15\ 0\ 24\ 12\ 4\ 13\ 14\ 22$$
$$\xrightarrow{f} 5\ 16\ 14\ 2\ 20\ 3\ 4\ 12 \longrightarrow 'FQOCUDEM'$$

Бобан може да прочита поруку помоћу алгоритма

$$f^{-1}(C) = C - b \bmod 26$$

Пример: Цезарова шифра

Слова $A - Z$ кодирамо са $\{0, \ldots, 25\} = \mathbb{Z}_{26}$, проточна шифра:

$$f(P) = P + b \bmod 26$$

где је $\in \mathbb{Z}_{26}$ кодирани симбол, $b = 16$ тајни кључ.
Алиса хоће да пошаље поруку $'PAYMENOW'$, она кодира

$$'PAYMENOW' \longrightarrow 15\ 0\ 24\ 12\ 4\ 13\ 14\ 22$$
$$\xrightarrow{f} 5\ 16\ 14\ 2\ 20\ 3\ 4\ 12 \longrightarrow 'FQOCUDEM'$$

Бобан може да прочита поруку помоћу алгоритма

$$f^{-1}(C) = C - b \bmod 26$$

Уопштење: афина шифра

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

где је $a' = a^{-1}$ у $\mathbb{Z}_{26}^*$ и $b' = -a^{-1}b$

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

- Познато: Најфреквентније слово у тексту на енглеском језику је $'E'$.

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

- Познато: Најфреквентније слово у тексту на енглеском језику је $'E'$.
- Цица проналази најфреквентније слово у шифрату, нпр. нека је $'K'$, и претпоставља да је $f('E') = 'K'$, тј. $f^{-1}('K') = 'E'$

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

- Познато: Најфреквентније слово у тексту на енглеском језику је $'E'$.
- Цица проналази најфреквентније слово у шифрату, нпр. нека је $'K'$, и претпоставља да је $f('E') = 'K'$, тј. $f^{-1}('K') = 'E'$
- Слично, упоређује друго најфреквентније слово и закључује $f^{-1}('D') = 'T'$

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

- Познато: Најфреквентније слово у тексту на енглеском језику је $'E'$.
- Цица проналази најфреквентније слово у шифрату, нпр. нека је $'K'$, и претпоставља да је $f('E') = 'K'$, тј. $f^{-1}('K') = 'E'$
- Слично, упоређује друго најфреквентније слово и закључује $f^{-1}('D') = 'T'$
- Цица решава систем

$$\begin{aligned} 10a' &+ b' &&= 4 \bmod 26 \\ 3a' &+ b' &&= 19 \bmod 26 \end{aligned}$$

и закључује да је кључ највероватније $a' = 9$, $b' = 18$

Криптоанализа

$$f(P) = aP + b \bmod 26 \qquad \text{и} \qquad f^{-1}(C) = a'C + b' \bmod 26,$$

- Познато: Најфреквентније слово у тексту на енглеском језику је $'E'$.
- Цица проналази најфреквентније слово у шифрату, нпр. нека је $'K'$, и претпоставља да је $f('E') = 'K'$, тј. $f^{-1}('K') = 'E'$
- Слично, упоређује друго најфреквентније слово и закључује $f^{-1}('D') = 'T'$
- Цица решава систем

$$\begin{aligned} 10a' &+ b' &&= 4 \bmod 26 \\ 3a' &+ b' &&= 19 \bmod 26 \end{aligned}$$

  и закључује да је кључ највероватније $a' = 9$, $b' = 18$
- Ако систем нема (јединствено) решење: уместо 2. најфреквентнијег слова може користити 3., 4., ...

- Закључак: боље радити са већим блоковима слова

- Закључак: боље радити са већим блоковима слова

Пример: Диграфови

Пар слова се кодира нечим из $\{0, 1, \ldots, 26^2 - 1 = 675\}$.

- Закључак: боље радити са већим блоковима слова

Пример: Дигрофови

Пар слова се кодира нечим из $\{0, 1, \ldots, 26^2 - 1 = 675\}$.
Диграф $'NO'$ се кодира са $26 \cdot {}'N' + {}'0' = 26 \cdot 13 + 14 = 352$,
затим се криптује $\underbrace{159}_{\text{кључ}} \cdot 352 + \underbrace{580}_{\text{кључ}} = 440 \bmod 676$ што је
еквивалент $'QY'$.

- Нека је $A \in \mathcal{M}_2(\mathbb{Z}_n)$ инвертибилна матрица, тј. таква да је $\det A$ инвертибилно у $\mathbb{Z}_n$

  Нпр. $n = 26$ и $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$

- Нека је $A \in \mathcal{M}_2(\mathbb{Z}_n)$ инвертибилна матрица, тј. таква да је $\det A$ инвертибилно у $\mathbb{Z}_n$

  Нпр. $n = 26$ и $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$

- Алгоритам за криптовање/декриптовање диграфа

$$\begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f} A \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f^{-1}} A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

- Нека је $A \in \mathcal{M}_2(\mathbb{Z}_n)$ инвертибилна матрица, тј. таква да је $\det A$ инвертибилно у $\mathbb{Z}_n$
  Нпр. $n = 26$ и $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$
- Алгоритам за криптовање/декриптовање диграфа

$$\begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f} A \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f^{-1}} A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

- Алиса жели да пошаље поруку $'NO|AN|SW|ER'$ тј.
  $\begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix}$

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 & 0 & 18 & 4 \\ 14 & 13 & 22 & 17 \end{pmatrix} = \begin{pmatrix} 68 & 39 & 102 & 59 \\ 203 & 104 & 302 & 164 \end{pmatrix} = \begin{pmatrix} 16 & 13 & 24 & 7 \\ 21 & 0 & 16 & 8 \end{pmatrix}$$

што је $'QVNAYQHI'$

- Нека је $A \in \mathcal{M}_2(\mathbb{Z}_n)$ инвертибилна матрица, тј. таква да је $\det A$ инвертибилно у $\mathbb{Z}_n$

  Нпр. $n = 26$ и $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$

- Алгоритам за криптовање/декриптовање диграфа

$$\begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f} A \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{f^{-1}} A^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

- Ако Бобан добије поруку $'FW|MD|IQ'$, он ће је помоћу $A^{-1} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \mod 26$ прочитати као

$$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix} = \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix}$$

што је $'ATTACK'$

Криптосистеми са јавним кључем

- Користе тзв. једносмерне функције $f : X \longrightarrow Y$
  - ако је познато $x \in X$ лако (брзо) се може израчунати $y = f(x)$
  - али ако је познато $y \in Y$ тешко је (неизводљиво у реалном времену) израчунати x тд. $y = f(x)$

Криптосистеми са јавним кључем

- Користе тзв. једносмерне функције $f : X \longrightarrow Y$
  - ако је познато $x \in X$ лако (брзо) се може израчунати $y = f(x)$
  - али ако је познато $y \in Y$ тешко је (неизводљиво у реалном времену) израчунати x тд. $y = f(x)$
- Довољно је да је f инјекција, а најчешће је бијекција

Криптосистеми са јавним кључем

- Користе тзв. једносмерне функције $f : X \longrightarrow Y$
  - ако је познато $x \in X$ лако (брзо) се може израчунати $y = f(x)$
  - али ако је познато $y \in Y$ тешко је (неизводљиво у реалном времену) израчунати x тд. $y = f(x)$
- Довољно је да је f инјекција, а најчешће је бијекција
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)

Криптосистеми са јавним кључем

- Користе тзв. једносмерне функције $f : X \longrightarrow Y$
  - ако је познато $x \in X$ лако (брзо) се може израчунати $y = f(x)$
  - али ако је познато $y \in Y$ тешко је (неизводљиво у реалном времену) израчунати x тд. $y = f(x)$
- Довољно је да је f инјекција, а најчешће је бијекција
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)
  - размену кључа који ће се користити за симетричне системе (без непосредног сусрета)

Криптосистеми са јавним кључем

- Користе тзв. једносмерне функције $f : X \longrightarrow Y$
  - ако је познато $x \in X$ лако (брзо) се може израчунати $y = f(x)$
  - али ако је познато $y \in Y$ тешко је (неизводљиво у реалном времену) израчунати x тд. $y = f(x)$
- Довољно је да је f инјекција, а најчешће је бијекција
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)
  - размену кључа који ће се користити за симетричне системе (без непосредног сусрета)
  - дигитални потпис

Дифи-Хелманова размена (усаглашавање) кључа

- Ако је p прост број, тада је $(\mathbb{Z}_p, +_p, \cdot_p)$ је поље, где је $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z}) = \{0, 1, 2, \ldots, p-1\}$

Дифи-Хелманова размена (усаглашавање) кључа

- Ако је p прост број, тада је $(\mathbb{Z}_p, +_p, \cdot_p)$ је поље, где је $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z}) = \{0, 1, 2, \ldots, p-1\}$
- Мултипликативна група $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ је циклична. тј. постоји генератор (примитивни корен) $g \in \mathbb{Z}_p \setminus \{0\}$ тд. се сви елементи $\mathbb{Z}_p \setminus \{0\}$ могу видети као степени g

Дифи-Хелманова размена (усаглашавање) кључа

- Ако је p прост број, тада је $(\mathbb{Z}_p, +_p, \cdot_p)$ је поље, где је $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z}) = \{0, 1, 2, \ldots, p-1\}$
- Мултипликативна група $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ је циклична. тј. постоји генератор (примитивни корен) $g \in \mathbb{Z}_p \setminus \{0\}$ тд. се сви елементи $\mathbb{Z}_p \setminus \{0\}$ могу видети као степени g
  - Пример: 3 је генератор $\mathbb{Z}_7 \setminus \{0\}$ јер је $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$,

Дифи-Хелманова размена (усаглашавање) кључа

- Ако је p прост број, тада је $(\mathbb{Z}_p, +_p, \cdot_p)$ је поље, где је $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z}) = \{0, 1, 2, \ldots, p-1\}$
- Мултипликативна група $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ је циклична. тј. постоји генератор (примитивни корен) $g \in \mathbb{Z}_p \setminus \{0\}$ тд. се сви елементи $\mathbb{Z}_p \setminus \{0\}$ могу видети као степени g
  - Пример: 3 је генератор $\mathbb{Z}_7 \setminus \{0\}$ јер је $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$, али 2 није генератор јер је $2^1 = 2$, $2^2 = 4$, $2^3 = 1$

Дифи-Хелманова размена (усаглашавање) кључа

- Ако је p прост број, тада је $(\mathbb{Z}_p, +_p, \cdot_p)$ је поље, где је $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z}) = \{0, 1, 2, \ldots, p-1\}$
- Мултипликативна група $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ је циклична. тј. постоји генератор (примитивни корен) $g \in \mathbb{Z}_p \setminus \{0\}$ тд. се сви елементи $\mathbb{Z}_p \setminus \{0\}$ могу видети као степени g
  - Пример: 3 је генератор $\mathbb{Z}_7 \setminus \{0\}$ јер је $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$, али 2 није генератор јер је $2^1 = 2$, $2^2 = 4$, $2^3 = 1$
- Дифи-Хелманова размена кључа се заснива на следећем:
  - ♣ ако знамо $g \in \mathbb{Z}_p^*$ и $n \in \mathbb{N}$ лако је одредити g^n (тј. $g^n \bmod p$)
  - ♠ али ако знамо g и g^n тешко је одредити n

Алгоритам:

- Алиса и Бобан бирају прост број p (приближно 200-цифрен) и генератор $g \in \mathbb{Z}_p^*$ и објављују p и g

Алгоритам:

- Алиса и Бобан бирају прост број p (приближно 200-цифрен) и генератор $g \in \mathbb{Z}_p^*$ и објављују p и g
- Алиса бира свој тајни кључ $a_A \in \mathbb{N}$, рачуна и објављује само $g^{a_A} \bmod p$ (јавни кључ)

Алгоритам:

- Алиса и Бобан бирају прост број p (приближно 200-цифрен) и генератор $g \in \mathbb{Z}_p^*$ и објављују p и g
- Алиса бира свој тајни кључ $a_A \in \mathbb{N}$, рачуна и објављује само $g^{a_A} \bmod p$ (јавни кључ)
- Слично, Бобан бира тајни кључ $a_B \in \mathbb{N}$, рачуна и објављује само $g^{a_B} \bmod p$ (јавни кључ)

Алгоритам:

- Алиса и Бобан бирају прост број p (приближно 200-цифрен) и генератор $g \in \mathbb{Z}_p^*$ и објављују p и g
- Алиса бира свој тајни кључ $a_A \in \mathbb{N}$, рачуна и објављује само $g^{a_A} \mod p$ (јавни кључ)
- Слично, Бобан бира тајни кључ $a_B \in \mathbb{N}$, рачуна и објављује само $g^{a_B} \mod p$ (јавни кључ)
- И Алиса и Бобан могу израчунати $K = (g^{a_A})^{a_B} \mod p = (g^{a_B})^{a_A} \mod p$, и то ће бити њихов усаглашен кључ

Алгоритам:

- Алиса и Бобан бирају прост број p (приближно 200-цифрен) и генератор $g \in \mathbb{Z}_p^*$ и објављују p и g
- Алиса бира свој тајни кључ $a_A \in \mathbb{N}$, рачуна и објављује само $g^{a_A} \mod p$ (јавни кључ)
- Слично, Бобан бира тајни кључ $a_B \in \mathbb{N}$, рачуна и објављује само $g^{a_B} \mod p$ (јавни кључ)
- И Алиса и Бобан могу израчунати $K = (g^{a_A})^{a_B} \mod p = (g^{a_B})^{a_A} \mod p$, и то ће бити њихов усаглашен кључ
- Цица зна само q, g g^{a_A} и g^{a_B}, и помоћу тога не може (брзо) да одреди K

Степеновање поновљеним квадрирањем

Брзи алгоритам за ♣ тј. рачунање g^n у $\mathbb{Z}_p^*$ (све операције су по модулу p):

1. можемо редуковати на $n < p - 1$ због Мале Фермаове теореме $g^{p-1} = 1$ у $\mathbb{Z}_p$

Степеновање поновљеним квадрирањем

Брзи алгоритам за ♣ тј. рачунање g^n у $\mathbb{Z}_p^*$ (све операције су по модулу p):

1. можемо редуковати на $n < p-1$ због Мале Фермаове теореме $g^{p-1} = 1$ у $\mathbb{Z}_p$
2. Записати n бинарно $n = \overline{n_r n_{r-1} \dots n_1 n_0} = \sum_{i=0}^{r} n_i \cdot 2^i$, $n_i \in \{0, 1\}$

Степеновање поновљеним квадрирањем

Брзи алгоритам за ♣ тј. рачунање g^n у $\mathbb{Z}_p^*$ (све операције су по модулу p):

1. можемо редуковати на $n < p-1$ због Мале Фермаове теореме $g^{p-1} = 1$ у $\mathbb{Z}_p$
2. Записати n бинарно $n = \overline{n_r n_{r-1} \dots n_1 n_0} = \sum_{i=0}^{r} n_i \cdot 2^i$, $n_i \in \{0, 1\}$
3. Израчунати 1, g, g^2, $\left(g^2\right)^2 = g^{2^2}$, $\left(g^{2^2}\right)^2 = g^{2^3}$, $\left(g^{2^3}\right)^2 = g^{2^4}$, $\dots$, $\left(g^{2^{r-1}}\right)^2 = g^{2^r}$ (сваки је квадрат претходног)

Степеновање поновљеним квадрирањем

Брзи алгоритам за ♣ тј. рачунање g^n у $\mathbb{Z}_p^*$ (све операције су по модулу p):

1. можемо редуковати на $n < p-1$ због Мале Фермаове теореме $g^{p-1} = 1$ у $\mathbb{Z}_p$
2. Записати n бинарно $n = \overline{n_r n_{r-1} \ldots n_1 n_0} = \sum_{i=0}^{r} n_i \cdot 2^i$, $n_i \in \{0, 1\}$
3. Израчунати 1, g, g^2, $\left(g^2\right)^2 = g^{2^2}$, $\left(g^{2^2}\right)^2 = g^{2^3}$, $\left(g^{2^3}\right)^2 = g^{2^4}$, $\ldots$, $\left(g^{2^{r-1}}\right)^2 = g^{2^r}$ (сваки је квадрат претходног)
4. g^n је производ оних g^{2^i} за које је $n_i = 1$

Степеновање поновљеним квадрирањем

Брзи алгоритам за ♣ тј. рачунање g^n у $\mathbb{Z}_p^*$ (све операције су по модулу p):

1. можемо редуковати на $n < p-1$ због Мале Фермаове теореме $g^{p-1} = 1$ у $\mathbb{Z}_p$
2. Записати n бинарно $n = \overline{n_r n_{r-1} \dots n_1 n_0} = \sum_{i=0}^{r} n_i \cdot 2^i$, $n_i \in \{0, 1\}$
3. Израчунати 1, g, g^2, $\left(g^2\right)^2 = g^{2^2}$, $\left(g^{2^2}\right)^2 = g^{2^3}$, $\left(g^{2^3}\right)^2 = g^{2^4}$, $\dots$, $\left(g^{2^{r-1}}\right)^2 = g^{2^r}$ (сваки је квадрат претходног)
4. g^n је производ оних g^{2^i} за које је $n_i = 1$

Доказ:

$$g^n = g^{\sum_{i=0}^{r} n_i \cdot 2^i} = \prod_{i=0}^{r} g^{n_i \cdot 2^i} = \prod_{\substack{0 \leqslant i \leqslant r \\ n_i = 1}} g^{2^i}$$

Временска сложеност

- за множење k-битног броја a и l-битног броја b треба kl операција, где је $k \sim \log a$ и $l \sim \log b$
- исто за целобројно дељење и узимање остатка по модулу

Временска сложеност

- за множење k-битног броја a и l-битног броја b треба kl операција, где је $k \sim \log a$ и $l \sim \log b$
- исто за целобројно дељење и узимање остатка по модулу
- У нашем алгоритму:
  1. $O\left(\log^2 p\right)$ операција јер је $\log p \sim$ број битова броја p
  2. $O(r \log n) = O\left(\log^2 p\right)$ операција - јер r пута понављамо дељење са 2 и остатак по модулу 2 (а $r \sim \log n \leqslant \log p$)
  3. r квадрирања, а за свако квадрирање треба по $O\left(\log^2\left(g^{2^i}\right)\right) = O\left(\log^2 p\right)$ операција
  4. највише r множења која захтевају по највише $O\left(\log^2 p\right)$ операција
- укупно $O\left(r \log^2 p\right) = O\left(\log^3 p\right)$

Временска сложеност

- за множење k-битног броја a и l-битног броја b треба kl операција, где је $k \sim \log a$ и $l \sim \log b$
- исто за целобројно дељење и узимање остатка по модулу
- У нашем алгоритму:
  1. $O\left(\log^2 p\right)$ операција јер је $\log p \sim$ број битова броја p
  2. $O(r \log n) = O\left(\log^2 p\right)$ операција - јер r пута понављамо дељење са 2 и остатак по модулу 2 (а $r \sim \log n \leqslant \log p$)
  3. r квадрирања, а за свако квадрирање треба по $O\left(\log^2\left(g^{2^i}\right)\right) = O\left(\log^2 p\right)$ операција
  4. највише r множења која захтевају по највише $O\left(\log^2 p\right)$ операција
- укупно $O\left(r \log^2 p\right) = O\left(\log^3 p\right)$
- за множење $g^n = gg \ldots g$ би требало $O\left(n \log^2 p\right)$ операција

Временска сложеност

- за множење k-битног броја a и l-битног броја b треба kl операција, где је $k \sim \log a$ и $l \sim \log b$
- исто за целобројно дељење и узимање остатка по модулу
- У нашем алгоритму:
  1. $O\left(\log^2 p\right)$ операција јер је $\log p \sim$ број битова броја p
  2. $O(r \log n) = O\left(\log^2 p\right)$ операција - јер r пута понављамо дељење са 2 и остатак по модулу 2 (а $r \sim \log n \leqslant \log p$)
  3. r квадрирања, а за свако квадрирање треба по $O\left(\log^2\left(g^{2^i}\right)\right) = O\left(\log^2 p\right)$ операција
  4. највише r множења која захтевају по највише $O\left(\log^2 p\right)$ операција
- укупно $O\left(r \log^2 p\right) = O\left(\log^3 p\right)$
- за множење $g^n = gg \ldots g$ би требало $O\left(n \log^2 p\right)$ операција
- Напомена: алгоритам ради и за модул m који није прост, али може да ради спорије јер уместо Мале Фермаове користи Ојлерову теорему. Видећемо да је израчунавање Ојлерове функције преспоро.

Пример: $57^{1616} \pmod{97}$

Broj 97 je prost i $NZD(57, 97) = 1$ pa možemo primeniti Malu Fermaovu teoremu. Pored toga, iskoristićemo činjenicu da je $80 = 64 + 16$.

$$57^{1616}(mod\ 97) = 57^{96 \cdot 16} \cdot 57^{80}(mod\ 97) = 57^{80}(mod\ 97) = 57^{64} \cdot 57^{16}(mod\ 97)$$

Odredimo vrednosti 57^{2^i}, za $i \in [1, 6]$ po modulu 97:

$$57^2 \equiv 48 \qquad 57^{16} \equiv 91^2 \equiv (-6)^2 \equiv 36$$
$$57^4 \equiv 48^2 \equiv 73 \qquad 57^{32} \equiv 36^2 \equiv 35$$
$$57^8 \equiv 73^2 \equiv 91 \qquad 57^{64} \equiv 35^2 \equiv 61$$

Sada lako računamo vrednost izraza:

$$57^{1616}(mod\ 97) = 57^{64} \cdot 57^{16}(mod\ 97) = 61 \cdot 36(mod\ 97) \equiv 62(mod\ 97)$$

Пример: $43^{257} \pmod{59}$

Broj 59 je prost i $NZD(59, 43) = 1$ pa možemo primeniti Malu Fermaovu teoremu:

$$43^{257}(mod\ 59) = 43^{25}(mod\ 59) = 43^{16} \cdot 43^{8} \cdot 43(mod\ 59)$$

Odredimo vrednosti 43^{2^i}, za $i \in [1, 4]$ po modulu 59:

$$43^2 \equiv 20 \qquad 43^8 \equiv 46^2 \equiv 51$$
$$43^4 \equiv 20^2 \equiv 46 \qquad 43^{16} \equiv 51^2 \equiv 5$$

Sada lako računamo vrednost početnog izraza:

$$43^{253}(mod\ 59) = 43^{16} \cdot 43^{8} \cdot 43(mod\ 59) = 5 \cdot 51 \cdot 43(mod\ 59) = 50$$

Функција која рачуна $a^n \pmod m$:

```
def mod_pow(a, n, m):

    res = 1
    while n > 0:
        # Za svaku jedinicu u binarnom zapisu n
        if n % 2 == 1:
            # Rezultat je stara vrednost rezultata * a^2{i} za i-tu poziciju
            res = (res * a) % m
        a = (a * a) % m
        # n gubi poslednju cifru u binarnom zapisu
        n = n // 2
    return res
```

Напомена: подразумевамо да за улазне податке важи $0 \leqslant a < m$ и $0 \leqslant n < \varphi(m)$.

Дифи-Хелманово усаглашавање кључа у криптосистему са јавним кључем $p = 97,\ g = 5$

Алиса бира тајни кључ $a_A = 36$ и рачуна јавни кључ

$$
\begin{aligned}
g^{a_A} &= 5^{36}(mod\ 97) = 5^{32} \cdot 5^4 (mod\ 97) \\
& 5^4 \equiv 25^2 \equiv 43 \\
& 5^{32} \equiv (5^4)^8 \equiv 43^8 \equiv 6^4 \equiv 35 \\
g^{a_A} &= 43 \cdot 35 (mod\ 97) = 50 (mod\ 97)
\end{aligned}
$$

Дифи-Хелманово усаглашавање кључа у криптосистему са јавним кључем $p = 97,\ g = 5$

Алиса бира тајни кључ $a_A = 36$ и рачуна јавни кључ

$$\begin{aligned} g^{a_A} &= 5^{36}(mod\ 97) = 5^{32} \cdot 5^4 (mod\ 97) \\ & 5^4 \equiv 25^2 \equiv 43 \\ & 5^{32} \equiv (5^4)^8 \equiv 43^8 \equiv 6^4 \equiv 35 \\ g^{a_A} &= 43 \cdot 35 (mod\ 97) = 50 (mod\ 97) \end{aligned}$$

Бобан бира тајни кључ $a_B = 58$ и рачуна јавни кључ

$$\begin{aligned} g^{a_B} &= 5^{58}(mod\ 97) = 5^{32} \cdot 5^{16} \cdot 5^8 \cdot 5^2 (mod\ 97) \\ & 5^2 \equiv 25 \\ & 5^8 \equiv (5^2)^4 \equiv (25^2)^2 \equiv 43^2 = 6 \\ & 5^{16} \equiv (5^8)^2 \equiv 6^2 \equiv 36 \\ & 5^{32} \equiv 35 \\ g^{a_B} &= 25 \cdot 6 \cdot 36 \cdot 35 (mod\ 97) = 44 (mod\ 97) \end{aligned}$$

Алиса рачуна размењени кључ K као

$$
\begin{aligned}
K = \; & (g^{a_B})^{a_A} = 44^{36}(mod\ 97) = 44^{32} \cdot 44^{4}(mod\ 97) \\
& 44^4 \equiv (44^2)^2 \equiv 93^2 \equiv (-4)^2 \equiv 16 \\
& 44^{32} \equiv (44^4)^8 \equiv 16^8 \equiv 62^4 \equiv 61^2 \equiv 35 \\
K = \; & 35 \cdot 16(mod\ 97) = 75(mod\ 97)
\end{aligned}
$$

Алиса рачуна размењени кључ K као

$$\begin{aligned} K = & \ (g^{a_B})^{a_A} = 44^{36}(mod\ 97) = 44^{32} \cdot 44^4(mod\ 97) \\ & 44^4 \equiv (44^2)^2 \equiv 93^2 \equiv (-4)^2 \equiv 16 \\ & 44^{32} \equiv (44^4)^8 \equiv 16^8 \equiv 62^4 \equiv 61^2 \equiv 35 \\ K = & \ 35 \cdot 16(mod\ 97) = 75(mod\ 97) \end{aligned}$$

Бобан рачуна размењени кључ K као

$$\begin{aligned} K = & \ (g^{a_A})^{a_B} = 50^{58}(mod\ 97) = 50^{32} \cdot 50^{16} \cdot 50^8 \cdot 50^2(mod\ 97) \\ & 50^2 \equiv 75 \\ & 50^8 \equiv (75)^4 \equiv (96)^2 \equiv 1 \\ & 50^{16} \equiv (50^8)^2 \equiv 1 \\ & 50^{32} \equiv (50^{16})^2 \equiv 1 \\ K = & \ 75 \cdot 1 \cdot 1 \cdot 1(mod\ 97) = 75(mod\ 97) \end{aligned}$$

- Кад кажемо бира број мислимо користи генератор случајних бројева

- Кад кажемо бира број мислимо користи генератор случајних бројева
- Али: Како се генерише случајан прост број?

- Кад кажемо бира број мислимо користи генератор случајних бројева
- Али: Како се генерише случајан прост број?
- Слабост Дифи-Хелмана:
  - Алиса и Бобан немају други канал комуникације и биће проблем ако се укључи између њих.
  - Ако Цица превари Алису, представи се као Боб, и размене кључ, онда Цица може (а Бобан не може) да чита поруке које Алиса шаље Бобану.
  - Ако се додатно Цица Бобану представи као Алиса, она може да мења Алисине поруке и прослеђује их Бобану.

Коначна поља (подсећање)

- У пракси Дифи-Хелманова размена кључа уместо поља $\mathbb{F}_p$ користи произвољно коначно поље

Коначна поља (подсећање)

- У пракси Дифи-Хелманова размена кључа уместо поља $\mathbb{F}_p$ користи произвољно коначно поље
- Ако је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином (у $\mathbb{Z}_p[x]$) степена d, тада је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ поље
  - Кренули смо од прстена $\mathbb{Z}_p[x]$ = сви полиноми по x са коефицијентима у $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
  - Затим су идентификовани полиноми чија је разлика дељива са $f(x)$

Коначна поља (подсећање)

- У пракси Дифи-Хелманова размена кључа уместо поља $\mathbb{F}_p$ користи произвољно коначно поље
- Ако је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином (у $\mathbb{Z}_p[x]$) степена d, тада је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ поље
  - Кренули смо од прстена $\mathbb{Z}_p[x]$ = сви полиноми по x са коефицијентима у $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
  - Затим су идентификовани полиноми чија је разлика дељива са $f(x)$
  - У $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ је $f(x) = 0$. Ако је $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_d \neq 0$, тада је $x^d = -\frac{a_{d-1}}{a_d}x^{d-1} - \cdots - \frac{a_1}{a_d}x - \frac{a_0}{a_d}$, а самим тим се и сви степени x^k, $k \geqslant d$ могу расписати преко $x^{d-1}, \ldots, x, 1$

Коначна поља (подсећање)

- У пракси Дифи-Хелманова размена кључа уместо поља $\mathbb{F}_p$ користи произвољно коначно поље
- Ако је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином (у $\mathbb{Z}_p[x]$) степена d, тада је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ поље
  - Кренули смо од прстена $\mathbb{Z}_p[x]$ = сви полиноми по x са коефицијентима у $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
  - Затим су идентификовани полиноми чија је разлика дељива са $f(x)$
  - У $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ је $f(x) = 0$. Ако је $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_d \neq 0$, тада је $x^d = -\frac{a_{d-1}}{a_d}x^{d-1} - \cdots - \frac{a_1}{a_d}x - \frac{a_0}{a_d}$, а самим тим се и сви степени x^k, $k \geqslant d$ могу расписати преко $x^{d-1}, \ldots, x, 1$
  - Зато је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ састављен од свих полинома степена мањег од $d = \deg f$, па има p^d елемената

Коначна поља (подсећање)

- У пракси Дифи-Хелманова размена кључа уместо поља $\mathbb{F}_p$ користи произвољно коначно поље
- Ако је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином (у $\mathbb{Z}_p[x]$) степена d, тада је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ поље
  - Кренули смо од прстена $\mathbb{Z}_p[x]$ = сви полиноми по x са коефицијентима у $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
  - Затим су идентификовани полиноми чија је разлика дељива са $f(x)$
  - У $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ је $f(x) = 0$. Ако је $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_d \neq 0$, тада је $x^d = -\frac{a_{d-1}}{a_d}x^{d-1} - \cdots - \frac{a_1}{a_d}x - \frac{a_0}{a_d}$, а самим тим се и сви степени x^k, $k \geqslant d$ могу расписати преко $x^{d-1}, \ldots, x, 1$
  - Зато је $\mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$ састављен од свих полинома степена мањег од $d = \deg f$, па има p^d елемената
  - Сабира се и множи по модулу $f(x)$ (и по модулу p)

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- Ако је $q = p^d$ тада је $\mathbb{F}_q \cong \mathbb{Z}_p[x]/(f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- Ако је $q = p^d$ тада је $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d
- $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} =$ мултипликативна група састављена од елемената из $\mathbb{F}_q$ који имају инверз у односу на $\cdot_f$

Теорема

1. Кардиналност коначног поља мора бити степен простог броја
2. Два коначна поља су изоморфна акко имају исти број елемената

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- Ако је $q = p^d$ тада је $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d
- $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} =$ мултипликативна група састављена од елемената из $\mathbb{F}_q$ који имају инверз у односу на $\cdot_f$
- $\left(\mathbb{F}_q^*, \cdot\right)$ је циклична група

Пример: Таблица множења у $\mathbb{F}_8^* \cong (\mathbb{Z}_2[x]/f\mathbb{Z}_2[x])^*$, где је $f(x) = x^3 + x^2 + 1$

$\cdot$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

- Коришћено $x^3 = -x^2 - 1 = x^2 + 1$ у $\mathbb{F}_8$

Пример: Таблица множења у $\mathbb{F}_8^* \cong (\mathbb{Z}_2[x]/f\mathbb{Z}_2[x])^*$, где је $f(x) = x^3 + x^2 + 1$

$\cdot$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

- Коришћено $x^3 = -x^2 - 1 = x^2 + 1$ у $\mathbb{F}_8$
- Генератор ове групе је x јер је

k	0	1	2	3	4	5	6	7
x^k	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x	1

За $q = p^d$

- можемо поистоветити полиноме

$$a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 + a_0$$

$(0 \leqslant a_i \leqslant d-1$, за све $i)$ са бројем записаним у систему са основом p:

$$\overline{a_{d-1}a_{d-2}\ldots a_1a_0}$$

са највише d цифара

За $q = p^d$

- можемо поистоветити полиноме

$$a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 + a_0$$

$(0 \leqslant a_i \leqslant d-1$, за све $i)$ са бројем записаним у систему са основом p:

$$\overline{a_{d-1}a_{d-2}\ldots a_1a_0}$$

са највише d цифара

- $+$ у $\mathbb{F}_q$ одговара ,,сабирању бројева без преноса“

За $q = p^d$

- можемо поистоветити полиноме

$$a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 + a_0$$

$(0 \leqslant a_i \leqslant d-1$, за све $i)$ са бројем записаним у систему са основом p:

$$\overline{a_{d-1}a_{d-2}\ldots a_1a_0}$$

са највише d цифара

- $+$ у $\mathbb{F}_q$ одговара ,,сабирању бројева без преноса“
- Специјално, $\mathbb{F}_{2^d}$ садржи све бројеве са највише d бинарних цифара и $+$ у $\mathbb{F}_{2^d}$ одговара ексклузивној дисјункцији бит по бит

За $q = p^d$

- можемо поистоветити полиноме

$$a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 + a_0$$

$(0 \leqslant a_i \leqslant d-1$, за све $i)$ са бројем записаним у систему са основом p:

$$\overline{a_{d-1}a_{d-2}\ldots a_1a_0}$$

са највише d цифара

- $+$ у $\mathbb{F}_q$ одговара „сабирању бројева без преноса“
- Специјално, $\mathbb{F}_{2^d}$ садржи све бројеве са највише d бинарних цифара и $+$ у $\mathbb{F}_{2^d}$ одговара ексклузивној дисјункцији бит по бит
- Пример: У $\mathbb{F}_8$ можемо поистоветити $x+1$ са 011 и x^2+x са 110, тада је $011 \cdot 110 = 111$ (из таблице)

Проблем дискретног логаритма ♠

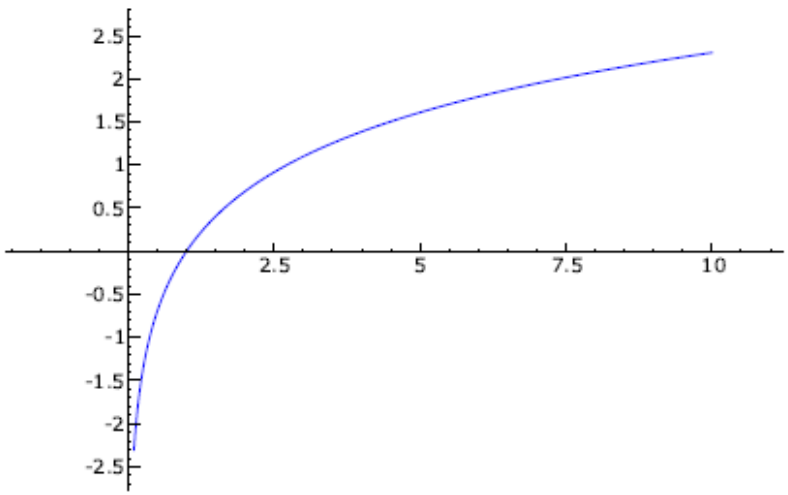
Дефиниција

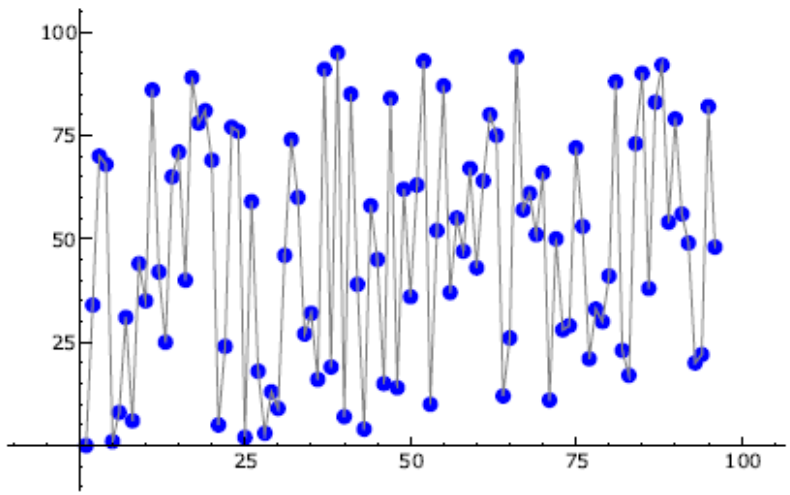
Нека је G група нпр. $\mathbb{F}_q^*$, и нека су $a, g \in G$. Најмањи природан број n (ако постоји) такав да је $a = g^n$ зовемо дискретни логаритам од a у основи g и означавамо са $\log_g a$.

Проблем дискретног логаритма ♠

Дефиниција

Нека је G група нпр. $\mathbb{F}_q^*$, и нека су $a, g \in G$. Најмањи природан број n (ако постоји) такав да је $a = g^n$ зовемо дискретни логаритам од a у основи g и означавамо са $\log_g a$.





Класичан логаритам и дискретни log_2 у групи $\mathbb{Z}_{53}^*$ (други делује непредвидиво)

График нацртан помоћу програма $SAGE$ доступан на `https://www.sagemath.org/`

Код

```
sage: p = 53
sage: R = Integers(p)
sage: a = R.multiplicative_generator()
sage: v = sorted([(a^n, n) for n in range(p-1)])
sage: G = plot(point(v,pointsize=50,rgbcolor=(0,0,1)))
sage: H = plot(line(v,rgbcolor=(0.5,0.5,0.5)))
sage: G + H
```

График нацртан помоћу програма $SAGE$ доступан на `https://www.sagemath.org/`

Код

```
sage: p = 53
sage: R = Integers(p)
sage: a = R.multiplicative_generator()
sage: v = sorted([(a^n, n) for n in range(p-1)])
sage: G = plot(point(v,pointsize=50,rgbcolor=(0,0,1)))
sage: H = plot(line(v,rgbcolor=(0.5,0.5,0.5)))
sage: G + H
```

- R.multiplicative_generator() враћа најмањи генератор циклične групе R (или избацује грешку ако R није циклична)

График нацртан помоћу програма $SAGE$ доступан на `https://www.sagemath.org/`

Код

```
sage: p = 53
sage: R = Integers(p)
sage: a = R.multiplicative_generator()
sage: v = sorted([(a^n, n) for n in range(p-1)])
sage: G = plot(point(v,pointsize=50,rgbcolor=(0,0,1)))
sage: H = plot(line(v,rgbcolor=(0.5,0.5,0.5)))
sage: G + H
```

- R.multiplicative_generator() враћа најмањи генератор цикличне групе R (или избацује грешку ако R није циклична)
- Тачке нису добијене као $(n, \log_a n)$, већ (a^n, n) (и потом су сортиране растуће по 1. координати)