Криптографија
- први део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

18. - 21. фебруар 2025.

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.

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (tajno, skrivено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (pisanje)

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- Слање поруке обухвата:
  - Кодирање - трансформише поруку (отворени текст, слика,...) у низ цифара или битова
  - Криптовање (шифровање) - трансформише кодирану поруку у шифрат
  - Слање шифрата

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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)

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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.

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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

- $\kappa\rho\upsilon\pi\tau o\varsigma$ (тајно, скривено) + $\gamma\rho\alpha\phi\epsilon\iota\nu$ (писање)
- 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)

- Стандардни ликови:
  - Алиса шаље поруку Бобану

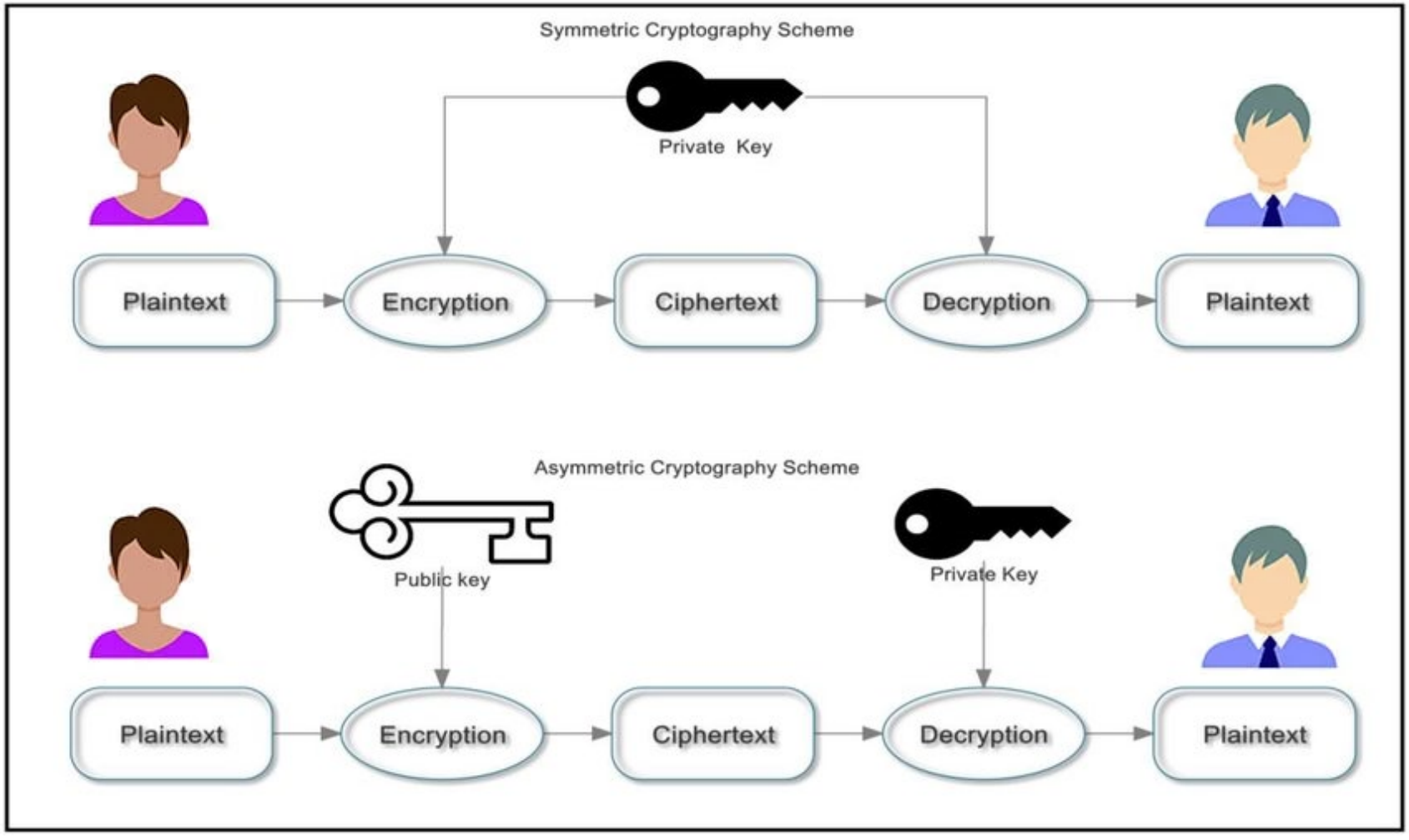
- Стандардни ликови:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (ово се зове криптоанализа)

- Стандардни ликови:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (ово се зове криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол или бит по бит

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

- Стандардни ликови:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (ово се зове криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол или бит по бит
  - 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.

- Стандардни ликови:
  - Алиса шаље поруку Бобану
  - Цица краде шифрат и покушава да га декриптује не знајући кључ (ово се зове криптоанализа)
- Врсте шифре:
  - Проточна - трансформише симбол по симбол или бит по бит
  - 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.


Symmetric Cryptography Scheme
Private Key
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Asymmetric Cryptography Scheme
Public key
Private Key
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

- Недостаци криптосистема:
  - код симетричних: Алиса и Бобан морају да имају додатни канал комуникације за размену кључа, дуже коришћење истог кључа смањује сигурност, лакши су за криптоанализу

- Недостаци криптосистема:
  - код симетричних: Алиса и Бобан морају да имају додатни канал комуникације за размену кључа, дуже коришћење истог кључа смањује сигурност, лакши су за криптоанализу
  - код асиметричних: споро извршавање. Обично се користе за пренос кратке поруке када је потребна висока сигурност

- Недостаци криптосистема:
  - код симетричних: Алиса и Бобан морају да имају додатни канал комуникације за размену кључа, дуже коришћење истог кључа смањује сигурност, лакши су за криптоанализу
  - код асиметричних: споро извршавање. Обично се користе за пренос кратке поруке када је потребна висока сигурност
- Најбоље резултате даје комбиновање симетричних и асиметричних

- Недостаци криптосистема:
  - код симетричних: Алиса и Бобан морају да имају додатни канал комуникације за размену кључа, дуже коришћење истог кључа смањује сигурност, лакши су за криптоанализу
  - код асиметричних: споро извршавање. Обично се користе за пренос кратке поруке када је потребна висока сигурност
- Најбоље резултате даје комбиновање симетричних и асиметричних
  - Обично се за слање поруке користи симетричан криптосистем, а његов кључ се размењује асиметричим криптосистемом.
  - По том принципу ради HTTPS протокол (Hypertext Transfer Protocol Secure)

Пример: Цезарова шифра

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

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

где је $P \in \mathbb{Z}_{26}$ 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 $P \in \mathbb{Z}_{26}$ 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 $P \in \mathbb{Z}_{26}$ 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 $P \in \mathbb{Z}_{26}$ 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 $a' = a^{-1}$ (инверз по модулу 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: сигурније је радити са већим блоковима слова,

- Закључак: сигурније је радити са већим блоковима слова, али је и спорије, па треба наћи баланс

- Закључак: сигурније је радити са већим блоковима слова, али је и спорије, па треба наћи баланс

Пример: Диграфови

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

- Закључак: сигурније је радити са већим блоковима слова, али је и спорије, па треба наћи баланс

Пример: Диграфови

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 $'QY'$.

Друга идеја:

- 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 $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$

Друга идеја:

- 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

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

Друга идеја:

- 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 $'ATTACK'$

Једнократна шифра (One-Time Pad)

- Ово је најједноставнија проточна шифра
- порука M се кодира бинарно
- кључ K (који је исто записан бинарно) мора да буде исте дужине као M

Једнократна шифра (One-Time Pad)

- Ово је најједноставнија проточна шифра
- порука M се кодира бинарно
- кључ K (који је исто записан бинарно) мора да буде исте дужине као M
- криптовање се врши бит по бит, сабирањем бита из M и бита из K по модулу 2

Једнократна шифра (One-Time Pad)

- Ово је најједноставнија проточна шифра
- порука M се кодира бинарно
- кључ K (који је исто записан бинарно) мора да буде исте дужине као M
- криптовање се врши бит по бит, сабирањем бита из M и бита из K по модулу 2
- идентично се ради и декриптовање (истим кључем)

Једнократна шифра (One-Time Pad)

- Ово је најједноставнија проточна шифра
- порука M се кодира бинарно
- кључ K (који је исто записан бинарно) мора да буде исте дужине као M
- криптовање се врши бит по бит, сабирањем бита из M и бита из K по модулу 2
- идентично се ради и декриптовање (истим кључем)
- Пример: Порука $'Go'$ се кодира са 0100011101101111

шифровање		*дешифровање*
0100011101101111		0011101011100010
$\oplus\ 0111110110001101$	*низ кључа*	$\oplus\ 0111110110001101$
0011101011100010		0100011101101111
		Go

Једнократна шифра (One-Time Pad)

- Ово је најједноставнија проточна шифра
- порука M се кодира бинарно
- кључ K (који је исто записан бинарно) мора да буде исте дужине као M
- криптовање се врши бит по бит, сабирањем бита из M и бита из K по модулу 2
- идентично се ради и декриптовање (истим кључем)
- Пример: Порука $'Go'$ се кодира са 0100011101101111

шифровање		*дешифровање*
0100011101101111		0011101011100010
$\oplus\ 0111110110001101$	*низ кључа*	$\oplus\ 0111110110001101$
0011101011100010		0100011101101111
		Go

- кључ се сме да користи само једном, поновна употреба истог кључа доводи до цурења података

Шифра транспоновањем (пермутовањем)

- Текст се дели блокове од n слова (n је тајни кључ)

Шифра транспоновањем (пермутовањем)

- Текст се дели блокове од n слова (n је тајни кључ)
- Блокови се исписују један испод другог

Шифра транспоновањем (пермутовањем)

- Текст се дели блокове од n слова (n је тајни кључ)
- Блокови се исписују један испод другог
- Текст се прочита вертикално

Шифра транспоновањем (пермутовањем)

- Текст се дели блокове од n слова (n је тајни кључ)
- Блокови се исписују један испод другог
- Текст се прочита вертикално
- Пример:

THIS IS THE PLAINTEXT THAT WE ARE ENCRYPTING.

THISI
STHEP
LAINT
EXTTH
ATWEA
REENC
RYPTI
NG

TSLEARRNHTAXTEYGIHITWEPSENTENTIPTHACI.

- Шифра транспонованьем је у историји често коришћена јер се лако реализује на механичким уређајима

- Шифра транспоновањем је у историји често коришћена јер се лако реализује на механичким уређајима
- Савремени симетрични криптосистеми комбинују све наведене шифре
  - више пута узастопно примењују различите криптосистеми са различитим кључевима, практично поново шифрују шифрат
  - најпознатији пример таквог криптосистема је AES (Advanced Encryption Standard)

Криптосистеми са јавним кључем

- Користе два различита кључа:
  - јавни кључ за криптовање
  - тајни кључ за декриптовање

Криптосистеми са јавним кључем

- Користе два различита кључа:
  - јавни кључ за криптовање
  - тајни кључ за декриптовање
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)

Криптосистеми са јавним кључем

- Користе два различита кључа:
  - јавни кључ за криптовање
  - тајни кључ за декриптовање
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)
  - размену кључа који ће се користити за симетричне системе (као замена за додатни канал комуникације)

Криптосистеми са јавним кључем

- Користе два различита кључа:
  - јавни кључ за криптовање
  - тајни кључ за декриптовање
- Могу се користити за:
  - размену порука (али су спорији од симетричних система)
  - размену кључа који ће се користити за симетричне системе (као замена за додатни канал комуникације)
  - дигитални потпис

- Заснивају се на тзв. једносмерним функцијама $f : X \longrightarrow Y$
  - 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. $y = f(x)$

- Заснивају се на тзв. једносмерним функцијама $f : X \longrightarrow Y$
  - 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

- Заснивају се на тзв. једносмерним функцијама $f : X \longrightarrow Y$
  - 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
- Пример коришћења једносмерне функције f (невезано од криптосистема):
  - Меил (или било који други сервис) за сваког корисника чува пар $(N, f(P))$ где је N корисничко име и P шифра
  - Када се приликом пријављивања унесу N и P', лако се рачуна $f(P')$ и проверава да ли се поклапа са $f(P)$
  - У случају да Цица украде податке $(N, f(P))$, она не може да израчуна P

- Најчешће: временска сложеност f и f^{-1} је $O(n^k)$ и $O(l^n)$, редом, за велико n ($=$ број коришћених битова) и (мале) константе k и l

- Најчешће: временска сложеност f и f^{-1} је $O(n^k)$ и $O(l^n)$, редом, за велико n (= број коришћених битова) и (мале) константе k и l
- Процесор извршава око 10^{10} операција у секунди

	10	20	30	40	50	60
n	10^{-9} seconds	$2 \cdot 10^{-9}$ seconds	$3 \cdot 10^{-9}$ seconds	$4 \cdot 10^{-9}$ seconds	$5 \cdot 10^{-9}$ seconds	$6 \cdot 10^{-9}$ seconds
n^2	10^{-8} seconds	$4 \cdot 10^{-8}$ seconds	$9 \cdot 10^{-8}$ seconds	$1.6 \cdot 10^{-7}$ seconds	$2.5 \cdot 10^{-7}$ seconds	$3.6 \cdot 10^{-7}$ seconds
n^3	10^{-7} seconds	$8 \cdot 10^{-7}$ seconds	$2.7 \cdot 10^{-6}$ seconds	$6.4 \cdot 10^{-6}$ seconds	$1.2 \cdot 10^{-5}$ seconds	$2.2 \cdot 10^{-5}$ seconds
n^5	10^{-5} seconds	0.00032 seconds	0.00243 seconds	0.01024 seconds	0.03125 seconds	0.07776 seconds
2^n	10^{-7} seconds	10^{-4} seconds	0.107 seconds	1 : 50 minutes	1.3 days	3.66 years
3^n	$6 \cdot 10^{-6}$ seconds	0.34 seconds	5 : 43 hours	38.55 years	22764 centuries	$1.34 \cdot 10^9$ centuries

Коначна поља (подсећање)

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

Коначна поља (подсећање)

- 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 $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ 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

Коначна поља (подсећање)

- 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 $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ 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 $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$,

Коначна поља (подсећање)

- 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 $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ 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 $2^1 = 2$, $2^2 = 4$, $2^3 = 1$

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 $f(x)$

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 $x^{d-1}, \ldots, x, 1$

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

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

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
- Мала Фермаова теорема: $a^{q-1} = 1$ за све $a \in \mathbb{F}_q^*$

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)