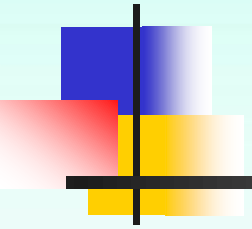
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Практ. 3 2022 КІБ-19

ШИФРЫ ПОДСТАНОВОК

1. Аддитивный.

Символы s из множества $\mathbb{Z}_{31}$

А Б В Г Д Е Є Ж З И І Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ю Я _

_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

$$M = \{s|\ s \in \mathbb{Z}_{31}\}, C = \{c|\ c \in \mathbb{Z}_{31}\},$$

$$K = \{k|\ k \in \mathbb{Z}_{31}^{\geq 0}\ \}$$

$$E(M) = (s + k)(mod\ 31)$$

$$D(C) = (c - k)(mod\ 31)$$

1. Аддитивный.

Ключ $k = 5$

Сообщение

ПРИВІТ_УЧАСНИКМ_ЗМАГАННЯ

_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

$$[30 + 5] mod\ 31 = 4$$

Я → Г

1. Аддитивный.

- **Сформировать программу**
- **Зашифровать сообщение с заданным ключом согласно варианту**
- **Расшифровать сообщение с заданным ключом согласно варианту**

I.1.2. Мультипликативный

Шифрование:

$$M = \{s|\ s \in \mathbb{Z}_n\}, C = \{c|\ c \in \mathbb{Z}_n\},$$
$$K = \{k|\ k \in \mathbb{Z}_n^{>0}\ \}$$
$$E(M) = (s * k)(mod\ n)$$

Дешифрование:

$$K = \{k|\ k \in \mathbb{Z}_{n*}\}$$

Ключи → !!! Мультипликативно инверсны

$$D(C) = \left(c * k^{-1}\right)(mod\ n)$$

Зашифровать, расшифровать с заданным ключом

I.1.3. Аффинный.

Аддитивный X мультипликативный

$$M = \{s|\ s \in \mathbb{Z}_n\}, C = \{c|\ c \in \mathbb{Z}_n\},$$
$$K = \{k|\ k \in \mathbb{Z}_n^{>0}\ \}$$

ШИФРОВАНИЕ

$$E(M) = (s * k)(mod\ n)$$
$$c_i = (s_i * k_1 + k_2)(mod\ n)$$

ДЕШИФРОВАНИЕ

$$D(C) = ((c - k_2) * k_1^{-1})(mod\ n)$$
$$s_i = \left((c_i - k_2) * k_1^{-1}\right)(mod\ n)$$

Зашифровать, расшифровать с заданными ключами

END # 3