Доброго всем антивирусного здоровья!

Тема очередной лекции по дисциплине КМЗИ: *Блочные шифры*. *Алгоритм* DES.

Методические материалы:

* Книга «Защита информации методами криптографии, стеганографии и обфускации», гл. 5, пп. 5.1-5.3,
* Рабочие методические материалы: Лабораторный практикум, ч. 2, теоретическая часть к лабораторной работе №5 (все – на Diskstation , в известном фолдере).

Из данной темы на коллоквиум будут вынесены вопросы:

* Сеть Фейстела,
* Понятие, цель, характеристика и реализация «лавинного эффекта»,
* Схема реализации одного раунда алгоритма DES (см. рис. 5.5 практикума).

Домашнее задание:

1.Записать двоичное представление чисел: день рожд.| месяц рождения,

Например, 24 марта: 24 – 11000, 3 – 11, двоичное представлении: 1100011.

2. Подсчитать кол-во символов (n) в двоичном числе. В нашем примере *n*=6.

3. Выполнить сложение 6 разных пар чисел (а и b) длиной n двоичных разрядов по модулю 2n, складываемые числа должны удовлетворять условиям: 2 пары чисел в сумме дают число с < 2n, 2 пары чисел дают число с= 2n, 2 пары ­ - дают число > 2n.

Примеры вычислений см. в п. 5.1.3 Практикума.

Все домашние задания старосты сдают лектору на первой лекции после карантина.

П.Урбанович