Лабораторная работа №. 4

Блочные шифры. Алгоритм DES

Задание 1. Изучайте учебно-методические материалы, размещенные на ELSE:

- *C4. Cifruri bloc*
- *DES-FIPS-46*
- *DES-FIPS-46-3*
- *Theory of Data Encryption Standard (DES)*
- *ASCII Character Set*
- *DES eng*
- *DES RO*

Задание 2. Разработайте программу на одном из языков программирования для реализации некоторого элемента алгоритма DES. Номер задания *no_task* будет выбран в соответствии с порядковым номером *n* ученика в списке группы, по формуле: *no_task* = *n* mod 11. Для каждого задания на экран будут выведены используемые таблицы и все промежуточные шаги. Программа должна позволить ввести данные либо от клавиатуры, либо сгенерировать их случайным образом.
Внимание! При защите работы будут заданы вопросы по функционированию всего алгоритма!!!

Lista de sarcini

2.1. Будучи задан ключ алгоритма DES (8 символов), определить K +.
2.2. Будучи задан $K+$ в алгоритме DES, определить C_i и D_i для заданного i.
2.3. В алгоритме *DES* задан $K+$. Определить раундовый ключ K_i для заданного i.
2.4. В алгоритме *DES* задано сообщение (8 символов). Вычислить L_1.
2.5. В алгоритме *DES* задан $K+$. Вычислить все 16 раундовых ключей K_i.
2.6. В алгоритме *DES* в раунде i известны K_i и R_{i-1}. Вычислить
$$B_1B_2B_3B_4B_5B_6B_7B_8$$
2.7. В алгоритме *DES* задан $B_1B_2B_3B_4B_5B_6B_7B_8$
Вычислить
$$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$
2.8. Вычислить R_i для раунда k алгоритма *DES*, если известны L_{k-1} и результат применения ящиков-*S*.
2.9. В раунде i алгоритма *DES* было получено $K_i + E(R_{i-1}) = ...$ (48 бит)
Вычислить $S_j(B_j)$ для заданного j.

2.10. В раунде *i* алгоритма *DES* известно L_{i-1}= ... (32 biți) и:

$$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$

Вычислить R_i.

2.11. При шифровании некоторого блока бит алгоритмом *DES* было получено

$$L_{16} = \text{... (32 бит)}$$
$$R_{16} = \text{... (32 бит)}$$

Вычислить зашифрованный блок сообщения в шестнадцатеричном представлении.

Примечание: **Кто не сможет разработать приложение – имеет возможность выбрать следующее альтернативное задание (максимальная оценка 9):**

- **зашифровать блок *i* сообщения *m* алгоритмом *DES* с ключом *k*, учитывая укороченный вариант, состоящий из одного раунда (окончательная перестановка будет выполнена в конце раунда 1);**
- **зашифрованное сообщение будет представлено в шестнадцатеричном формате;**
- **индекс *i* битового блока, и ключ *k* будут запрошены у преподавателя.**

m *= The Data Encryption Standard (DES) specifies two FIPS approved cryptographic algorithms as required by FIPS 140-1. When used in conjunction with American National Standards Institute (ANSI) X9.52 standard, this publication provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.*