Шифрование DES

Случайные числа

1, 2, 3, 5, 7, 2, 5, ...

7, 7, 7, 7, ...

Что можно считать случайными числами?

Виды случайных чисел

- настоящие случайные числа (очень сложно реализовать, используются редко);
- псевдослучайные числа (равномерно распределены в отличие от настоящих, которые распределены по нормальному закону);
- квазислучайные числа (имеют гарантировано равномерное распределение, более надежные).

Тест на k-распределение случайности (спектральный тест)

12345678 - можем взять какую-то последовательность, которая будет иметь нормальное распределение (в данном случае - k = 5).

Алгоритмы получения случайных чисел

1. Алгоритм Фон Неймана

1234

0**52**9

2**70**4 (52^2)

4**90**0 (70^2)

8**10**0 (90^2)

0**10**0 (10^2)

0**10**0 (10^2)

2. Метод перемешивания (метод сдвига)

1234

2341 + 4123 = ...

3. На числах Фибоначчи

0, 1, 1, 2, 3, 5, 8, 13, 21, 34

0, 1, 1, 2, 3, 5, 8, 3, 1, 4

4. Линейный конгруэнтный генератор

R(n + 1) = (A * R(n) + C) mod M

A = 430, C = 2531, M = 11979

5. Вихрь Мерсена

Есть 624 32-битных числа, берем одно из середины, складываем с первым (сдвинутым на один байт) и полученное значение добавляем в конец (первое удаляем).

Симметричные алгоритмы шифрования

Процедуры шифрования и расшифровки симметричны друг другу (используется один и тот же ключ)

Используют два подхода к шифрованию (используются не один раз, а циклически):

- перестановки (линейные преобразования);
- подстановки (нелинейные преобразования).

Функция Фейстеля: перестановка + подстановка.

Data Encryption Standard (DES)

Использует ключ длиной 56 бит => перебор такого ключа довольно трудоемкий.

Каждый бит зашифрованного сообщения является функцией бит всего текста.

Улучшенный алгоритм: **Triple DES** (длина ключа - 192 бит).

C = Ek3(Dk2(Ek1(M)))

M' = Dk1(Ek2(Dk3(C)))

Лабораторная работа 3

Реализовать алгоритм DES.

Лекция 3
Лекция 5