Тема 5. Потоковые шифры

Практическая часть

Составить компьютерную программу (на любом языке программирования), которая реализует потоковый шифр. Программа должна выполнять следующие действия (этапы работы).

- 1. *Создание ключа*. Ключ **КЕУ** представляет собой перестановку массива целых чисел от 0 до 255.
- 2. Инициализация генератора случайных чисел. Генератор случайных чисел **GEN** представляет собой массив целых чисел от 0 до 255. В качестве исходного его состояния необходимо взять случайный ключ, полученный в пункте (1). Далее состояние генератора инициализируется, то есть преобразуется по следующему правилу:
 - + j := 0;
 - перебрать в цикле все значения і в диапазоне от 0 до 255, и на каждой итерации выполняя операции:
 - j := (j + GEN[i] + KEY[i]) mod 256;
 - поменять местами GEN[i] и GEN[j];
- 3. Получение гаммы. Сообщение MESSAGE, которое передаёт по каналу связи отправитель, представляет собой байтовую последовательность. Количество состояний одного байта 256. Гамма GAMMA представляет собой массив чисел, взятых из диапазона от 0 до 255 (соответствуют возможным состояниям байтов сообщения). Длина гаммы равна длине сообщения (в байтах). Чтобы построить гамму, необходимо выполнить следующие действия.
 - пусть k индекс буквы сообщения; перебрать все k в количестве, равном длине сообщения (в байтах), и на каждой итерации выполняя операции:

```
i := 0;
j := 0;
i := (i + 1) mod 256;
j := (j + GEN[i]) mod 256;
поменять местами GEN[i] и GEN[j];
t := (GEN[i] + GEN[j]) mod 256,
GAMMA[k] := GEN[t];
```

- 4. *Шифрование сообщения*. К каждому байту сообщения применить операцию **XOR** с соответствующим байтом гаммы.
 - перебрать в цикле все значения k количеством, равным длине сообщения (в байтах), и на каждой итерации выполняя операции:
 - MESSAGE[k] := MESSAGE [k] XOR GAMMA[k];
- 5. *Расшифрование сообщения*. К каждому байту сообщения применить операцию **XOR** с соответствующим байтом гаммы.

ЗАМЕЧАНИЕ: если сообщение, которое нужно зашифровать, является последовательностью символов юникода, на каждый из которых тратится два байта информации, то необходимо перед шифрованием разрезать 16-битное представление кода символа на два 8-битных, и только после этого вести шифрование.

Так, в строчках ниже можно видеть пример того, как реализуется указанный подход

```
# === подготовительная часть === #
import random
# генерация случайной перестановки списка _l
def get_random_permutation(_l: list) -> list:
     _p = _l[:]
     len_list = len(_l)
     seed = 2 * len_list
     for n in range(seed):
          i = random.randint(0, len_list - 1)
j = random.randint(0, len_list - 1)
          if (i != j) and (_p[i] != _p[j]):
              _{p[i]}, _{p[j]} = _{p[j]}, _{p[i]}
     return
# печать длинного списка с пояснением (показываются первые п элементов)
def print_long_list(_msg, _l: list, _n: int):
    print(_msg, end=': ')
    print('[', end='')
     for _ in _l[:_n]:
     print(_, end=', ')
print('...]')
# инициализация генератора случайных чисел
def initialization(_gen: list, _key: list) -> list:
     _gen_temp = _gen[:]
     _j = 0
     for _i in range(256):
         _j = (_j + _gen_temp[_i] + _key[_i]) % 256
_gen_temp[_i], _gen_temp[_j] = _gen_temp[_j], _gen_temp[_i]
     return _gen_temp
# преобразование символа в последовательность нулей и единиц
def char_to_bits(_c: str, _positions: int) -> str:
    return bin(ord(_c))[2:].zfill(_positions)
# преобразование числа в последовательность нулей и единиц
def num_to_bitstr(_num: int, _positions: int) -> str:
    return bin(_num)[2:].zfill(_positions)
# преобразование последовательности нулей и единиц в число
def from_bits_to_number(_s: str) -> int:
     _string = _s[::-1]
     num = 0
     for _i in range(len(_string)):
         _num += int(_string[_i]) * (2 ** _i)
     return _num
# получение списка разбитых кодов юникода на две части
def from_unicode_to_ascii(_s: str) -> list:
     _lst = []
     for _elem in _s:
         _lst.append(char_to_bits(_elem, 16)[:8])
_lst.append(char_to_bits(_elem, 16)[8:])
     return [from_bits_to_number(_elem) for _elem in _lst]
# получение гаммы
def make_gamma(_gen: list, _message: list) -> list:
     _{gamma} = []
     _gen_temp = _gen[:]
     _i, _j = 0, 0
     for _k in range(len(_message)):
          _{i} = (_{i} + 1) \% 256
         _{j} = (_{j} + _{gen_{i}}) % 256
         _gen_temp[_i], _gen_temp[_j] = _gen_temp[_j], _gen_temp[_i]
_t = (_gen_temp[_i] + _gen_temp[_j]) % 256
          _gamma.append(_gen_temp[_t])
     return _gamma
# шифрование списка байт-чисел
def chifering(_message: list, _gamma: list) -> list:
     return [(_message[_i] ^ _gamma[_i]) for _i in range(len(_message))]
```

```
# показ сообщения в символьном виде
def symbolise(_l: list) -> str:
    _s = ""
    _i = 0
    while _i < len(_l):</pre>
         _s += chr(from_bits_to_number(num_to_bitstr(_l[_i], 8) + num_to_bitstr(_l[_i + 1], 8)))
         _i += 2
    return s
# === подготовительная часть === #
# === основная часть === #
# получение начального ключа
key = get_random_permutation(list(range(256)))
print_long_list("Ключ", key, 10)
# инициализация генератора случайных чисел
gen = key[:]
gen = initialization(gen, key)
print_long_list("Инициализированный генератор случайных чисел", gen, 10)
# задание сообшения
message = "Hello, world!"
print("Сообщение: " + message)
# коды юникода символов сообщения
print_long_list("Коды юникода символов сообщения", [ord(letter) for letter in message], 10)
# сисок чисел, соответствующих байтам символов юникода
splitted_message = from_unicode_to_ascii(message)
print_long_list("Пары байтов сообщения", splitted_message, 10)
# гамма
gamma = make_gamma(gen, splitted_message)
print_long_list("Гамма", gamma, 10)
# шифрование сообщения
chifred_message = chifering(splitted_message, gamma)
print_long_list("Зашифрованное сообщение (список)", chifred_message, 10)
# показ сообщения в символьном виде
symbolised_message = symbolise(chifred_message)
print("Шифрованное сообщение (символы юникода): " + symbolised_message)
# расшифрование сообщения
desplitted_message = from_unicode_to_ascii(symbolised_message)
dechifred_message = chifering(desplitted_message, gamma)
print_long_list("Расшифрованное сообщение (список)", dechifred_message, 10)
print("Расшифрованное сообщение (символы юникода): " + symbolise(dechifred_message))
# === основная часть === #
Результат работы программы:
Ключ: [41, 152, 254, 26, 38, 173, 98, 197, 56, 147, ...]
Инициализированный генератор случайных чисел: [92, 130, 61, 146, 120, 211, 134, 197, 101, 140, ...]
Сообщение: Hello, world!
Коды юникода символов сообщения: [72, 101, 108, 108, 111, 44, 32, 119, 111, 114, ...]
Пары байтов сообщения: [0, 72, 0, 101, 0, 108, 0, 108, 0, 111, ...]
Гамма: [167, 110, 162, 244, 254, 166, 45, 7, 195, 166, ...]
Зашифрованное сообщение (список): [167, 38, 162, 145, 254, 202, 45, 107, 195, 201, ...]
Шифрованное сообщение (символы юникода): Ӈ박ᆁ쏉训侃ᡂ좰篌淅숗
Расшифрованное сообщение (список): [0, 72, 0, 101, 0, 108, 0, 108, 0, 111, ...]
Расшифрованное сообщение (символы юникода): Hello, world!
```