

Федеральное агентство связи  
Ордена трудового Красного Знамени федеральное государственное  
бюджетное  
образовательное учреждение высшего образования  
«Московский технический университет связи и информатики»

Отчет по лабораторной работе  
«ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ И ПРИЕМЫ ХЕШИРОВАНИЯ»  
по дисциплине «Информационная безопасность»  
Вариант 1

Выполнил: студент группы БВТ1904

Абакаров Гасан Гаджирабаданович

Проверила:

Магомедова Дженнет Исламутдиновна

**Цель работы:** получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

**Ход работы:**

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу шифрования методом контрольных сумм.
3. Составить программу шифрования методом хеширования с применением гаммирования.
4. Составить отчет по проделанной работе.
5. Защитить работу.

**Постановка задачи:**

Составить программу шифрования методом контрольных сумм и методом хеширования с применением гаммирования.

**Вариант 1**

Пусть  $a = 17$ ,  $b = 11$ ,  $c = \text{MaxVal} + 1 = 256$ ,  $t_0 = 172$ . Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (KSumm) и методом хеширования с применением гаммирования (SummKodBukvOtkr):

- а)  $P = '0123456789'$ , KSumm = ?, SummKodBukvOtkr – ?;
- б)  $P = '9876543210'$ , KSumm = ?, SummKodBukvOtkr – ?;
- в)  $P = '1000005'$ , KSumm = ?, SummKodBukvOtkr – ?;
- г)  $P = '1500000'$ , KSumm = ?, SummKodBukvOtkr – ?

**Листинг программы:**

```
# шифрование методом контрольных сумм
def KSumm(P, MaxVal):
    v=0
    for i in P:
        v+=i
        if v>MaxVal:
            v-=MaxVal
            v-=1
    return v
```

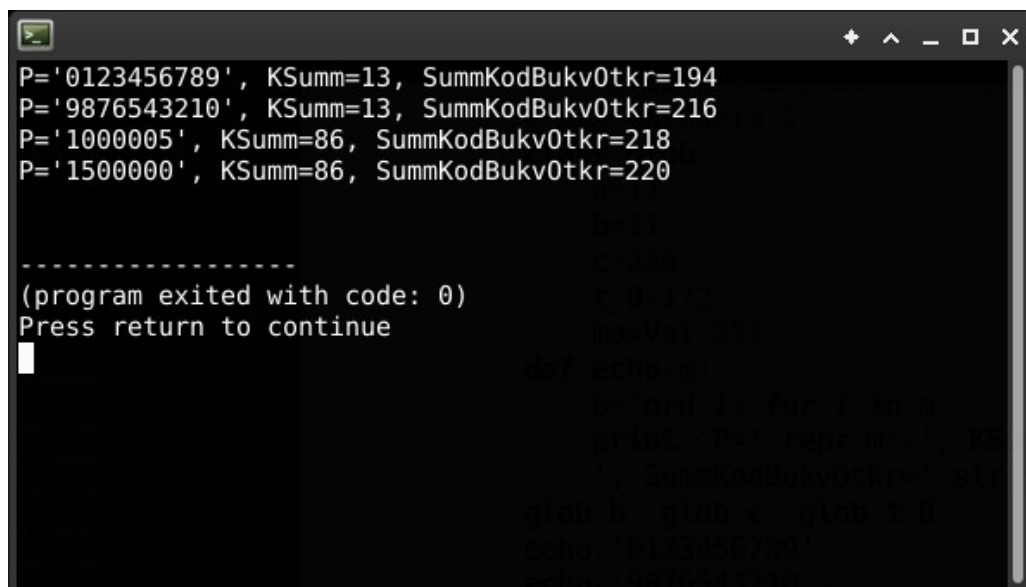
```

# шифрование методом хеширования с применением гаммирования
def SummKodBukvOtkr(P, MaxVal, a, b, c, t):
    p=[]
    for i in P:
        t=(a*t+b)%c
        p.append(i^t)
    return KSumm(p, MaxVal)

# функция выводит в консоль контрольные суммы
# для нескольких сообщений методом контрольных сумм (KSumm)
# и методом хеширования с применением гаммирования (SummKodBukvOtkr)
# для варианта 1
class glob:
    a=17
    b=11
    c=256
    t_0=172
    maxVal=255
def echo(m):
    b=[ord(i) for i in m]
    print('P='+repr(m)+' , KSumm='+str(KSumm(b, glob.maxVal))+
        ' , SummKodBukvOtkr='+str(SummKodBukvOtkr(b, glob.maxVal glob.a,
glob.b, glob.c, glob.t_0)))
echo('0123456789')
echo('9876543210')
echo('1000005')
echo('1500000')

```

### Результат выполнения программы:



```

P='0123456789', KSumm=13, SummKodBukvOtkr=194
P='9876543210', KSumm=13, SummKodBukvOtkr=216
P='1000005', KSumm=86, SummKodBukvOtkr=218
P='1500000', KSumm=86, SummKodBukvOtkr=220

-----
(program exited with code: 0)
Press return to continue

```

### **Контрольные вопросы**

1. Назвать три функции ЭЦП.
2. Перечислить этапы формирования ЭЦП.
3. Что шифруется при применении ЭЦП?
4. Что называется хеш-значением документа?
5. Что называется хеш-функцией?
6. Что называется сворачиванием (хешированием) документа?
7. В чем заключается метод контрольных сумм?
8. Перечислить этапы метода хеширования с применением гаммирования.
9. Недостаток метода контрольных сумм.

### **Ответы:**

1. Электронная цифровая подпись (ЭЦП) обычно выполняет три функции: 1) функцию авторизации — подтверждение того, что подписавшийся действительно является тем, за кого мы его принимаем; 2) обеспечение того, что подписавшийся не может отказаться от документа, который он подписал; 3) подтверждение того, что отправитель подписал именно тот документ, который отправил, а не какой-либо иной.

2. В упрощенном виде ЭЦП формируется следующим образом.

1. Корреспондент X по специальному алгоритму обрабатывает документ, предназначенный для отправки адресату Y. В результате применения этого алгоритма, вырабатывается некоторый параметр, характеризующий документ в целом.
2. Затем X с помощью секретной части ключа шифрует полученный параметр. Полученный таким образом шифр является ЭЦП корреспондента X.
3. Корреспондент X отправляет адресату Y документ и свою электронную цифровую подпись.
4. Адресат Y реализует на полученном документе тот же алгоритм, которым пользовался корреспондент X.
5. Затем Y дешифрует электронную цифровую подпись, полученную от X, пользуясь открытой частью ключа, предоставленной ему корреспондентом X.
6. Адресат Y сравнивает значение параметра, полученного на четвертом этапе, с расшифрованным значением ЭЦП. Если эти значения совпадают, то подпись подлинная и документ при передаче не был изменен.

3. При применении ЭЦП шифруется только некоторая интегральная характеристика этого документа (параметр).

4. Хеш-значение документа - это интегральный параметра документа

5. Хеш-функция — алгоритм получения интегрального параметра

6. Хешированием, или сворачиванием документа называется процесс получения хеш значения с помощью хеш функции

7. Метод контрольных сумм — это метод получения интегрального параметра путем сложения всех чисел (кодов символов), соответствующих тексту. Если сумма превышает максимальное значение, то результатом будет остаток от деления суммы на максимальное значение.

8. Этапы метода хеширования с применением гаммирования:

Пусть исходный документ представляется в виде последовательности  $n$ -битовых двоичных слов:  $X_1, X_2, \dots, X_p$ .

Выработаем последовательность псевдослучайных чисел  $t_i$  по рекуррентной формуле

$$T_{i+1} = (a \cdot T_i + b) \bmod c, \text{ где}$$

$$i = 0, 1, \dots, p - 1; a, b, T_0 \text{ — заданные числа;}$$

$$p \text{ — количество символов в тексте, } c = 2^n,$$

Затем вырабатывается новая последовательность чисел

$$Y_1 = X_1 \oplus T_1, Y_2 = X_2 \oplus T_2, \dots, Y_p = X_p \oplus T_p.$$

Полученная последовательность целых чисел суммируется по модулю  $\text{MaxVal} + 1$

9. Недостатки метода контрольных сумм заключается в том, что можно произвольным образом изменить порядок символов в документе или изменить отдельные символы и подогнать остальные так, чтобы контрольная сумма оставалась неизменной