МИНЦИФРЫ РФ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский Технический Университет Связи и Информатики»

Кафедра информационной безопасности

**ЛАБОРАТОРНАЯ РАБОТА №4**

**по основам информационной безопасности**

**«Электронно-цифровая подпись и приёмы хэширования»**

Выполнил Скрипников Андрей Олегович  
БВТ2201

Москва 2021

**Цель работы:** овладеть практическими навыками закрытия информации электронно-цифровой подписью и приёмами хэширования, рассмотреть хэширование методом контрольных сумм и методом наложения кодов - гаммированием.

**Индивидуальное задание:**

Вариант 9. Составить программу шифрования методом контрольных сумм и методом хэширования с применением гаммирования.

a = 23; b = 19; c = MaxVal + 1 = 256,t = 235

**Исходный код программы:**





**Результат выполнения программы:**



**Контрольные вопросы:**

* *Назвать три функции ЭЦП*  
  1) Функция авторизации подписавшегося;  
  2) Гарантия того, что подписавшийся не откажется от подписанного документа;  
  3) Подтверждение подлинности документа.
* *Перечислить этапы формирования ЭЦП*1) Отправитель X по специальному алгоритму обрабатывает документ, предназначенный для адресата Y. Вырабатывается некий параметр, характеризующий документ в целом;  
  2) X с помощью своего секретного ключа шифрует полученный параметр - итоговый шифр и является ЭЦП отправителя X;  
  3) X отправляет Y документ и свою ЭЦП  
  4) Y реализует на полученном документе тот же алгоритм, которым пользовался X;  
  5) Y дешифрует ЭЦП X, пользуясь открытым (публичным) ключом X;  
  6) Y сравнивает значение параметра, полученного в пункте 4, с расшифрованным значением ЭЦП. Значения должны совпадать, если документ и/или ЭЦП не были изменены.
* *Что шифруется при применении ЭЦП?*  
  Хэш-сумма файла.
* *Что называется хэш-значением документа?*  
  Значение интегрального параметра документа.
* *Что называется хэш-функцией?*Хэш-функция преобразует исходные данные в некоторый меньший массив данных; результат выполнения хэш-функции с двумя случайными наборами входных данных с высокой вероятностью должен быть различным. Сложность алгоритма такой функции должна обеспечить невозможность изменения осмысленного исходных данных с сохранением того же результата. Также алгоритм функции реализуется так, что по результату невозможно однозначно восстановить исходные данные.
* *Что называется сворачиванием (хэшированием) документа?*Вычислением результата используемой хэш-функции для данных, содержащихся в документе.
* *В чём заключается метод контрольных сумм?*Складываются все коды символов в документе. Если значение какого-либо кода превышает максимальное допустимое значение, то берётся значение K mod (MaxVal + 1).
* *Перечислить этапы метода хэширования с применением гаммирования*1) Каждый символ представляется в виде восьмибитного двоичного слова;  
  2) По рекуррентной формуле создаётся последовательность псевдослучайных чисел;  
  3) Значение каждого символа складывается по модулю 2 с соответствующим значением в последовательности псевдослучайных чисел;  
  4) Полученные числа переводятся в десятичную систему счисления;  
  5) Полученная последовательность суммируется по модулю MaxVal + 1.
* *Недостаток метода контрольных сумм*Можно произвольным образом изменить порядок следования символов в файле, и при этом контрольная сумма останется прежней.