ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

(МТУСИ)



Кафедра Информационной безопасности

Лабораторная работа №4

Выполнили студенты группы БВТ1904:

Игнатов Д.В.

Баскаева М.А.

Игнатенко Я.И.

Проверила:

Магомедова Д.И.­

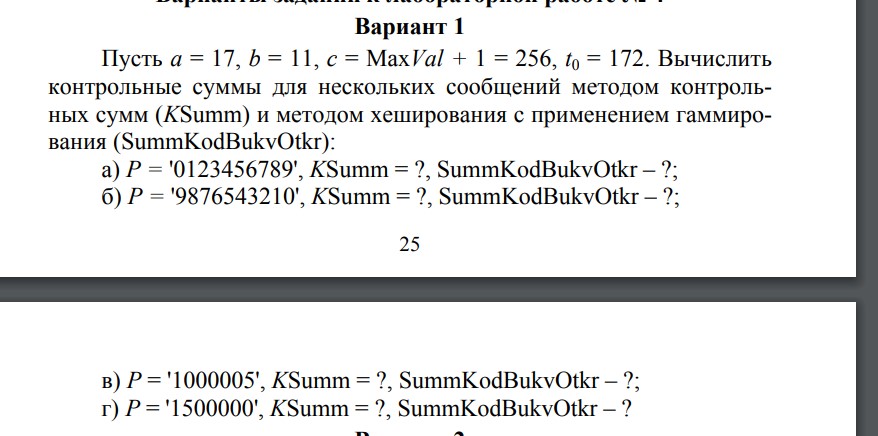
*Москва,2020*

**Цель работы**

Овладеть практическими навыками закрытия информации электронно-цифровой подписью и приемами хеширования, рассмотрение хеширования методом контрольных сумм и методом наложения кодов — гаммированием.

**Постановка задачи**

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



**Листинг программы**

int a = 17, b = 11, c = 256, t0 = 172;

char[] str = str\_tb.Text.ToCharArray();

int summ = 0;

int summk = 0;

char[] t = new char[str.Length];

for (int i = 0; i < str.Length; i++) {

summ += str[i];

summk += str[i] ^ (t0 = (a \* t0 + b) % c);

}

KSumm\_lb.Text = Convert.ToString(summ % c);

SummKod\_lb.Text = Convert.ToString(summk % c);

**Результаты выполнения программы**

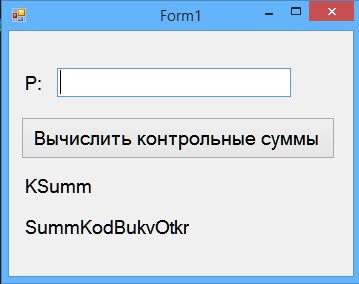


Рис 1. Финальный вид программы

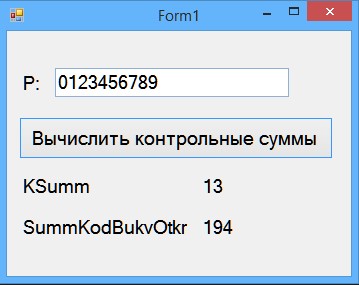


Рис 2. Вычисление контрольных сумм фразы «0123456789»

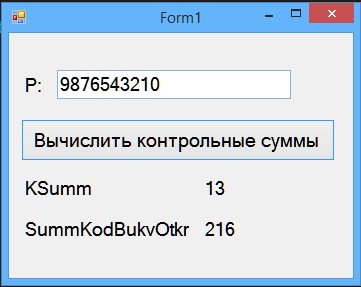


Рис 3. Вычисление контрольных сумм фразы «9876543210»

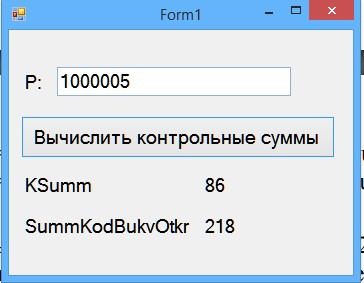


Рис 4. Вычисление контрольных сумм фразы «1000005»

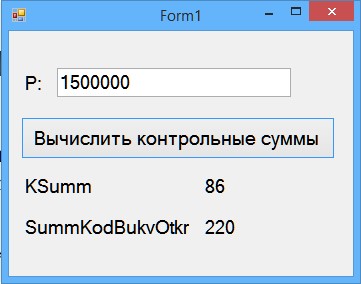


Рис 5. Вычисление контрольных сумм фразы «1500000»

**Контрольные вопросы**

**1) Назвать три функции ЭЦП.**

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) Перечислить этапы формирования ЭЦП.**

1. Корреспондент Х по специальному алгоритму обрабатывает документ, предназначенный для отправки адресату Y. В результате применения этого алгоритма, вырабатывается некоторый параметр, характеризующий документ в целом. Объем памяти, занимаемый выработанным параметром, значительно меньше, чем объем всего документа (1, 2, 4 байта).

2. Затем Х с помощью секретной части ключа шифрует полученный параметр. Полученный таким образом шифр является ЭЦП корреспондента X.

3. Корреспондент Х 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. Окончательно 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. В противном случае — либо документ искажен, либо подпись подделана, либо и то и другое.

**3) Что шифруется при применении ЭЦП?**

Применение ЭЦП не предполагает обязательного засекречивания (шифрования) самого передаваемого документа. Шифруется только некоторая интегральная характеристика этого документа. Если документ при передаче по каналу связи будет изменен злоумышленником, то, естественно, изменится и его интегральная характеристика, а это сразу заметит адресат при расшифровании ЭЦП. В связи с этим встает вопрос, каким должен быть алгоритм получения интегральной характеристики документа (не слишком большого параметра, характеризующего документ в целом)

**4)** **Что называется хеш-значением документа?**

Значение интегрального параметра называют хеш-значением документа

**5)** **Что называется хеш-функцией?**

Способ (алгоритм) получения хеш-значения называется хеш функцией.

**6)** **Что называется сворачиванием (хешированием) документа?**

Получение хеш-значения с помощью хеш-функции называют сворачиванием (хешированием) текста документа в более короткий текст (интегральный параметр)

**7)** **В чем заключается метод контрольных сумм?**

Под контрольной суммой понимается некоторое значение, рассчитанное путем сложения всех чисел (кодов символов), соответствующих данному тексту. Если сумма всех таких чисел K превышает максимально допустимое значение (МахVаl), заданное заранее, то величина контрольной суммы полагается равной остатку от деления полученной суммы на максимально возможное значение контрольной суммы, увеличенное на единицу

**8)** **Перечислить этапы метода хеширования с применением гаммирования**.

Пусть каждому символу документа (открытого текста) соответствует восьмибитовое двоичное слово Хi. Таким образом, исходный документ представляется в виде последовательности восьмибитовых двоичных слов: Х1, Х2 , …, Хр. Затем выработаем последовательность псевдослучайных чисел ti по рекуррентной формуле ti+1 = (а ⋅ ti + b) mod c, (6) где i = 0, 1, …, р – 1; а, b, t0 — заданные числа; р — количество символов в тексте. При с = 2n . Если взять n = 8, то двоичные представления чисел ti не будут превышать восьми двоичных знаков. Далее каждое число ti представим в виде восьмибитового двоичного слова. Получаем последовательность двоичных слов: Т1, Т2, ..., Tp. Двоичные числа Хi и Ti, сложим поразрядно по модулю 2. Получим новую последовательность двоичных слов: Y1 = X1 ⊕ T1, Y2 = X2 ⊕ T2, ..., Yp = Xp ⊕ Tp. Каждое двоичное слово, рассматриваемое как двоичное число, переведем в десятичную систему, при этом получим последовательность чисел: y1, y2, …, yp. Полученная последовательность целых чисел суммируется по модулю МахVal + 1 (если п = 8, то МахVal = 255).

**9)** **Недостаток метода контрольных сумм**.

Недостаток метода контрольных сумм (в обоих вариантах) заключается в том, что хотя несовпадение значений этих сумм служит верным признаком того, что документ подвергся изменению, но равенство значений еще не дает гарантии, что информация осталась неизменной. Можно произвольным образом изменить порядок следования букв, цифр или слов и фраз в документе, при этом контрольная сумма сохранит прежнее значение. Так предложениям «казнить нельзя, помиловать» и «казнить, нельзя помиловать» соответствуют одни и те же контрольные суммы, а их содержание прямо противоположное. И что еще хуже — можно изменить отдельные числа в документе и подогнать остальные так, что контрольная сумма останется той же самой. Например, вместо суммы в 1 000 005 рублей написать 1 500 000 рублей и получить ни за что половину миллиона рублей

**Заключение**

Итак, опираясь на результаты тестирования, можно сделать вывод что я овладел практическими навыками закрытия информации электронно-цифровой подписью и приемами хеширования, рассмотрел хеширования методом контрольных сумм и методом наложения кодов — гаммированием.