**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Национальный исследовательский университет «МЭИ»**

Кафедра электрофизики информационных систем

Рытов А.А

Разработка биометрического идентификатора с

электронно-цифровой подписью.

Курсовая работа

Учебно-методическое пособие по курсу

"Цифровые технологии защиты информации"

для студентов, обучающихся по направлению

09.04.01

"Информатика и вычислительная техника".

МОСКВА НИУ МЭИ 2016

УДК 519.

ББК 22.18

Р–954

Подготовлено на кафедре электрофизики информационных систем

Рецензент: канд. техн. наук, проф. Казанцев Ю.А.

**Рытов А.А**

**Разработка биометрического идентификатора с электронно-цифровой подписью:** Курсовая работа– НИУ «МЭИ», 2016. – 12 с.

Курсовая работа включает в себя самостоятельное изучение теоретических и справочных материалов, разработку программных модулей встраивания информации в цифровой объект, разработку одного из трех вариантов ЭЦП на основе эллиптических кривых, отладку программы, создание единого программного модуля на базе Wolfram Mathematica, позволяющего встроить в фотографию студента, с помощью стеганографических методов данные его студенческого билета и получить ЭЦП этого объекта.

Методическое пособие предназначено для студентов, обучающихся по направлению подготовки "Информатика и вычислительная техника".

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Введение

Курсовая работа состоит из двух частей. Первая часть посвящена разработке программного модуля, реализующего электронно-цифровую подпись (ЭЦП) на основе эллиптических кривых (ЭК). В пособии приведены необходимые теоретические данные, базирующиеся на источниках [1,2,3].

Отправной точкой является поиск базовой точки ЭК, порядок которой должен быть простым числом. Выбор осуществляется случайным образом на множестве ЭК, для которых проводится последовательное изменение свободного члена в кубическом уравнении. После того как точка найдена, реализуется один из трех вариантов ЭЦП с пятью разными хэш-функциями.

В качестве биометрического идентификатора выступает цифровая фотография студента заданного размера, в которую средствами цифровой стеганографии [] встраивается часть информации из студенческого билета. Процессы встраивания ЦВЗ основаны на методах замены младшего бита. Эти методы требуют изменения того или иного значащего бита для растрового изображения. Для конкретной реализации выбран формат BMP-24. Таким образом формируется невидимый цифровой водяной знак (ЦВЗ).

На заключительном этапе формируется ЭЦП заполненного фиксированного контейнера – фотографии с ЦВЗ.

Все операции, которые необходимы для выполнения курсовой работы реализуются в системе компьютерной алгебры Wolfram Mathematica 9.0.

1.Элементы эллиптической криптографии.

1.1. Эллиптические кривые. Определение.

Эллиптической кривой ***E*** над полем ***F*** называется гладкая кривая, задаваемая уравнением вида:

(1)

представляющая собой множество точек , удовлетворяющих этому уравнению и содержащая также бесконечно удаленную точку, обозначаемую ***O.***

Приведенное выше аффинное уравнение Вейерштрасса может определяться над любым полем, в том числе полями рациональных и комплексных чисел, однако для криптографических целей предполагается, что коэффициенты и точки кривой принадлежат полю *GF*(*q*) .

В свою очередь *GF*(*q*) – это конечное поле из *q* элементов, где . Число *p* – простое и называется характеристикой поля *GF*(*q*). Если *m*=1, то *GF*(*q*) – это множество целых чисел по модулю *p*.

В том случае, если , уравнение Вейерштрасса можно упростить (с новыми значениями *a,b,c*):

(2)

Если, к тому же, , уравнение можно привести к виду:

(3)

Обе приведенные формы уравнений для эллиптической кривой будут применяться в дальнейшем, при этом следует учитывать, что последнее уравнение формально получается из более общего при коэффициенте .

Для кривой в форме Вейерштрасса условие гладкости выражается в том, чтобы во множестве не должно быть точек, в которых обе частные производные по *x* и по *y* равны 0. То есть два уравнения

не должны удовлетворяться ни в одной точке .

В случае представления эллиптической кривой в виде:

(4)

условие гладкости состоит в требовании, чтобы кубический многочлен справа не имел кратных корней. Это выполняется тогда и только тогда, когда его дискриминант не равен нулю:

. (5)

Эллиптическая кривая может быть задана как с помощью коэффициентов, например *a* и *b*, так и через инвариант.

Инвариантом эллиптической кривой называется величина *J*(*E*), удовлетворяющая тождеству:

(6)

Коэффициенты *a*,*b* эллиптической кривой *Е*, по известному инварианту *J* (*E*), определяются следующим образом:

**Пример 1**.

Для кривой, заданной коэффициентами *a* = 7 и *b* = 1 над полем *GF*(11) и величиной дискриминанта d

,

инвариант определяется как:



При заданном инварианте, определение коэффициентов эллиптической кривой может быть выполнено следующим образом:



1.2. Число точек эллиптической кривой.

Эллиптическая кривая над конечным полем имеет конечную группу точек. Порядок этой группы называют порядком эллиптической кривой.

В то же время существует понятие порядка точки *P* эллиптической кривой – это наименьшее число *k* такое, что произведение *k·P* = *O*. По теореме Лагранжа порядок точки делит порядок эллиптической кривой.

Для небольших полей определение числа точек ЭК может быть выполнено в результате прямого решения уравнения, описывающего эллиптическую кривую.

**Пример 2.**

Для эллиптической кривой над полем *GF*(11) точки этой кривой могут быть найдены с помощью функции ] :

.

Этот же результат можно представить в виде более удобном для дальнейших операций :

.

Длина полученного списка с учетом точки в бесконечности – порядок кривой – составляет : *N*ЭК = Length[g1] + 1=15.

В том случае, когда эллиптическая кривая описывается как над полем *GF*(*p*) и *p >* 2 , порядок кривой определяется по следующей формуле:

(7)

, где - символ Лежандра. При простом *p* значение символа Лежандра совпадает со значением символа Якоби.

**Пример 3**.

Для кривой над полем *GF*(11)

*N*ЭК = p+1+Sum[JacobiSymbol[x^3-5 x + 3,p],{x,0,p-1}] = 15.

Однако, вычисление порядка эллиптической кривой не всегда просто или даже возможно []. Общая формула для вычисления порядка произвольной кривой неизвестна. Неизвестно даже, можно ли за полиномиальное время найти кривую данного порядка.

Оценка порядка эллиптической кривой над полем *GF*(*p*) определяется по теореме Хассе:

(8)

Пример 4.

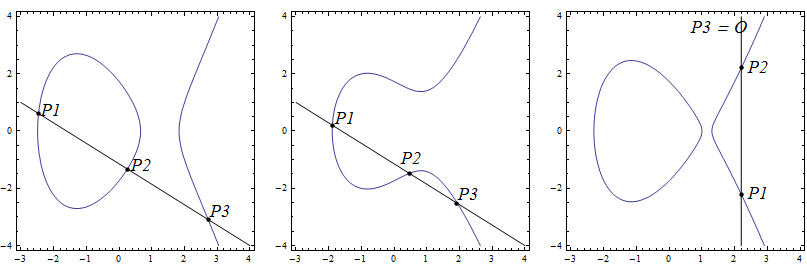
Для кривой над полем *GF*( *p* = 11)

1.3. Сложение точек эллиптической кривой.

Причиной интереса к эллиптическим кривым служит операция сложения, которая может быть на них определена и является основой для построения односторонних функций. Относительно операции сложения точка в бесконечности ***O E*** служит нулем, а множество ***E*** обладает структурой аддитивной группы.

Для определения сложения на ***E*** используется то свойство, что любая прямая, пересекающая эллиптическую кривую в двух точках, пересекает её трижды. Точка касания считается за две точки и точка ***O*** в бесконечности – это точка пересечения всех "вертикальных" прямых.

На рис. 1 приведены три случая ,в которых прямая пересекает эллиптическую кривую над полем действительных чисел с отрицательным дискриминантом (а), с положительным дискриминантом (б), а также (в) пересечение с вертикальной прямой – здесь третья точка пересечения – ***О*** в бесконечности.



а) б) в)

Рис.1. Эллиптическая кривая над полем действительных чисел с отрицательным дискриминантом (а), с положительным дискриминантом (б), а также (в) пересечение с вертикальной прямой.

1.3.1. Геометрия эллиптических кривых.

Если заданы две различные точки на эллиптической кривой ***E***:  и причем обе точки не в бесконечности , то прямая ***L*** проходящая через эти точки задается уравнением:

.

В том случае, если , то по определению третьей точкой пересечения будет ***О***.

Для поля, порядок которого , координаты третьей точки точки пересечения могут быть определены как:

и

Точки и могут совпадать  , тогда ***L*** – касательная к эллиптической кривой и её наклон совпадает с производной в точке .:

Третья точка пересечения прямой ***L*** и кривой ***E*** также имеет координаты .

Пусть точка – это точка эллиптической кривой, тогда определим противополжную точку:

.

Точка ***О*** в бесконечности интерпретируется как точка пересечения всех вертикальных прямых, противоположна самой себе и является нейтральным элементом по сложению.

Для того, чтобы сложить точки и , когда обе они не лежат в бесконечности, нужно выполнить следующие два шага:

1. вычислить прямую, проходящую через и (или, в случае ,касательную прямую, проходящую через ), и найти третью точку пересечения с ***E***; пусть это будет ;
2. найти сумму , определяемую равенством .

1.3.2. Законы сложения точек эллиптической кривой.

Пусть  **–** точка на эллиптической кривой ***E*** , а ***О*** точка в бесконечности. Тогда положим:

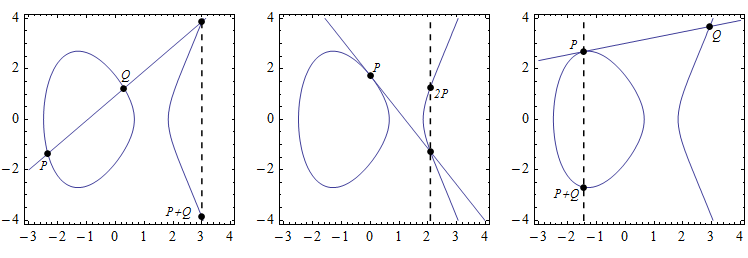
.

Далее, пусть и **,** две точки на ***E***, обе отличные от ***О***.

Тогда сумма определяется равенствами:

1. **,** если , здесь  **-** третья точка пересеченияс ***E*** прямой ***L***, проходящей через и **.**
2. **,** если и касательная, проходящая через **,** единична, здесь данной касательной.
3. если и проходящая через касательная двойная.
4. **,** если **.**

Три наиболее типичных случая, а именно , 1), 2) и 3) (илюстрация для поля действительных чисел приведены на рис.2.



а) б) в)

Рис. 2. Сложение точек ЭК – а) , б) удвоение точки пересечения по касательной, в) сложение точек с инфлекцией.

Сложение двух точек эллиптической кривой может быть выполнено с помощью программного модуля – функции пользователя ,

где должны быть заданы следующие формальные параметры:

p – порядок поля;

a, b, c – коэффициенты, описывающие кривую вида

P\_List, Q\_List – списки координат точек и **.**



здесь в бесконечности {O} прописная буква O английского алфавита.

Например, для того чтобы сложить две точки и **,** принадлежащие кривой над полем ***p*** = 11 выполним следующие действия:



В результате получаем точку также принадлежащую эллиптической кривой .

1.3.3. Умножение точки ЭК на целое число.

Пользуясь операцией сложения точек на кривой, можно естественным образом определить операцию умножения точки на произвольное целое число ***k***:

. (9)

Таким образом модуль умножения точки ЭК на целое число легко реализовать в виде циклического сложения точки с самой собой на основе функции .

Эффективные алгоритмы вычисления приведены в [].

Необходимо отметить [], что множество точек эллиптической кривой вместе с точкой в бесконечности и операцией сложения, описанной выше, является абелевой группой.

Одним из вариантов реализации операции умножения при является применение рекурсивных вычислений [], однако в этом случае максимальное значение ограничено глубиной рекурсии.

Пример. Умножение точки кривой над полем ***p*** = 11 на число .



В выходном списке первый результат- это умножение точкина , далее удвоение и т.д.

При результатом умножения является **,** то есть точка имеет порядок равный 5, в соответствии с определением порядка точки ЭК (наименьшее число такое, что произведение ).

Модуль умножения на основе рекурсии рекомендуется применять при малых для отладки основного модуля умножения.

1.4. Построение односторонней функции на основе эллиптической кривой.

Пусть ***E -*** эллиптическая кривая и - точка на этой кривой.

Выберем целое число , где -порядок эллиптической кривой.

В качестве **прямой** функции выберем произведение .

Для его вычисления по оптимальному алгоритму потребуется не более операций сложения.

**Обратная задача**:

По заданной эллиптической кривой ***,***

Точке и произведению

**Найти**  .

В настоящее время все известные алгоритмы решения этой задачи требуют экспоненциального времени.

1.5. Протоколы электронной цифровой подписи на основе эллиптических кривых.

Электронная цифровая подпись (ЭЦП) для сообщения является числом, зависящим от самого сообщения и от некоторого секретного, известного только подписывающему субъекту ключа. При этом предполагается, что она должна быть легко проверяемой и что осуществить проверку подписи должен иметь возможность каждый без получения доступа к секретному ключу.

Введем следующие обозначения:

**–** сообщение, для которого формируется ЭЦП;

**-** значение хеш-функции для документа ;

**–** эллиптическая кривая;

**–** базовая точка открытого ключа;

**-** порядок точки **;**

**-** секретный ключ подписывающего сообщение участника;

**-** открытый ключ.

1.5.1. Схема Nyberg-Rueppel электронной подписи

с использованием группы точек эллиптической кривой.

Алгоритм генерации подписи:

1. Образовать случайную битовую строку и вычислить **.**
2. Используя -компоненту точки *R* как целое число, вычислить:

Пара является подписью для документа , такого, что***.***

Базовая точка умножается на случайное число *,* и получается точка ,

-компонента этой точки также является случайным числом.

Прибавление этой точки к хеш-значению по модулю (порядка точки *)* эффективно маскирует это хеш-значение.

Алгоритм верификации подписи:

Для проверки, что является корректным хеш-значением, выполняется следующий алгоритм:

1. Вычислить***;***
2. используя -компоненту , вычислить
3. если полученное значение совпадает с хеш-значением , то последнее удостоверяется:

Этап верификации позволяет восстановить это замаскированное хеш-значение, не допуская никакой утечки информации, которая позволила бы активному криптоаналитику изменить документ и хеш-значение так, чтобы измененный документ воспринимался бы как корректный.

1.5.2. Алгоритм ECDSA электронной подписи с использованием группы точек эллиптической кривой.

Алгоритм генерации подписи :

1.Выбираем случайное целое число  и вычисляем

2.Вычисляем

3**.** Вычисляем

4. Формируем цифровую подпись , где

Верификация цифровой подписи:

1. Получить авторизованную копию открытого ключа **,**

а также ***m' , P ,*** {***r' ,с'***}, ***q..***

2. Проверить, что илежат в интервале . .

3. Вычислить и **.**

4. Определить и **.**

5. Вычислить и сравнить – компоненту точки с полученной по открытому каналу составляющей электронной подписи .

1.5.3. Алгоритм ГОСТ Р 3410 - 2001 электронной подписи

с использованием группы точек эллиптической кривой .

Алгоритм генерации подписи :

1.Выбираем случайную битовую строку  и

вычисляем **.**

2.Вычисляем ***,***

3. Формируем цифровую подпись , где

Верификация цифровой подписи:

1. 1. Получить авторизованную копию открытого ключа **,**

а также ***.***

2. Проверить, что илежат в интервале .

3. Вычислить и

4. Определить и ***.***

5. Вычислить и сравнить – компоненту точки с полученной по открытому каналу составляющей электронной подписи .

2. Встраивание идентификационной информации в цифровой объект.

2.1. Модель процесса встраивания ЦВЗ.



Рис 3. Модель процесса встраивания цифрового водяного знака.

В общем случае исходными данными для процесса встраивания ЦВЗ в фиксированный контейнер являются:

* исходное изображение ;
* множество всех возможных точек размещения ЦВЗ;
* ключ, в виде некоторой псевдослучайной последовательности;
* цифровой водяной знак – встраиваемая информация.

Выбор стего пути основывается на анализе возможностей размещения ЦВЗ в заданном контейнере, сопоставлении этих возможностей с ключом, методом встраивания и требований защиты ЦВЗ от статистических атак. Возможна дополнительная коррекция стего пути, учитывающая особенности исходного контейнера, в результате которой получается рабочая реализация стего-пути .

В свою очередь ЦВЗ – информация, чаще всего, должна быть представлена в виде двоичного кода в котором необходимо предусмотреть возможность декодирования и восстановления ЦВЗ, а также может быть дополнена введением избыточности и необходимой служебной информации.

Встраивание каждого бита информации в элемент стего-пути осущетвляется в соответствии с реализацией того или иного стеганографического метода. Так же в зависимости от метода встраивания, предварительно заполненный контейнер и исходный контейнер могут быть объединены с вероятностным признаком в конечный результат встраивания ЦВЗ:

. (10)

2.2. Цветовые модели

В растровом изображении каждому пикселу соответствует значение, задающее его цвет.Система представления цветов называется цветовой моделью.

Цветовые модели обычно разработаны так, чтобы использовать достоинства устройств отображения конкретного типа.

В большинстве цветных мониторов для каждого пиксела используются три люминофора (красный, зеленый и синий) или три светоизлучателя. Настраивая яркости отдельных люминофоров, можно управлять цветом пиксела.

Когда яркость всех трех люминофоров минимальна, пиксел выглядит черным.

При максимальной яркости пиксел выглядит белым.

Наиболее общепринятая цветовая модель, применяемая в компьютерных программах, известна как RGB (Red-Green-Blue - Красный-Зеленый-Синий).

Модель RGB отражает работу компьютерных дисплеев.

В модели RGB цвета получаются сложением трех компонентов, которые представляют относительные яркости красного, зеленого и синего цветов.

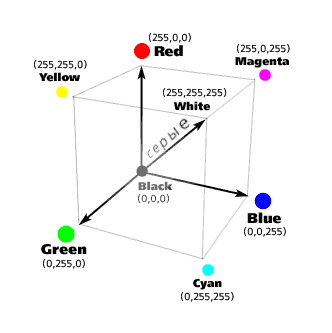


Рис 4. Цветовая модель RGB.

2.3. Неформатные методы сокрытия в графических изображениях – пространственная область. Методы замены.

2.3.1. Метод замены наименьшего значащего бита (НЗБ).

Данный метод обычно работает с растровыми изображениями, которые представлены в формате без сжатия (например, GIF и BMP**).**

Основным его недостатком является сильная чувствительность к малейшим искажениям контейнера.

Для ослабления этой чувствительности часто применяют помехоустойчивое кодирование.

В простейшем случае проводится замена НЗБ всех последовательно расположенных пикселей изображения.

Однако, так как длина секретного сообщения обычно меньше количества пикселей изображения, то после его внедрения в контейнере будут присутствовать две области с различными статистическими свойствами (область, в которой незначащие биты были изменены, и область, в которой они не менялись).

Это может быть легко обнаружено с помощью статистических тестов.

Для создания эквивалентного изменения вероятности всего контейнера секретное сообщение обычно дополняют случайными битами так, чтобы его длина в битах была равна количеству пикселей в исходном изображении.

2.3.2. Метод случайного интервала.

Заключается в последовательном случайном распределении битов секретного сообщения по контейнеру , в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Эта методика наиболее эффективна при использовании потоковых контейнеров (видео).

2.3.3. Метод псевдослучайной перестановки.

Данный метод может применяться для контейнеров произвольного доступа.

Суть метода заключается в том, что генератор псевдослучайных чисел производит последовательность индексов и сохраняет -й бит сообщения в пикселе с индексом .

Однако в этом случае один индекс может появиться в последовательности более одного раза, т.е. может произойти "пересечение" — искажение уже встроенного бита.

Если число битов сообщения намного меньше размера изображения , то вероятность пересечения незначительна, и поврежденные биты могут быть восстановлены с помощью корректирующих кодов.

Вероятность, по крайней мере, одного пересечения оценивается как:

(10)

при условии, что **.**

При увеличении иданная вероятность стремится к единице.

Для предотвращения пересечений необходимо сохранять все индексы использованных элементов и перед сокрытием нового пикселя проводить проверку его на повторяемость.

2.3.4. Метод блочного сокрытия

Исходное изображение-контейнер разбивается на непересекающихся блоков произвольной конфигурации и для каждого из них вычисляется бит четности. В каждом блоке проводится сокрытие одного секретного бита **.**

Если бит четности блока не совпадает с секретным битом , то происходит инвертирование одного из НЗБ блока , в результате чего , будет выполняться равенство

Выбор блока может производиться случайно с использованием стегоключа.

Хотя этот метод обладает такой же устойчивостью к искажениям, как и все предыдущие, он имеет ряд преимуществ. Прежде всего, имеется возможность изменять значения такого пикселя в блоке, для которого статистика контейнера изменится минимально.

Кроме того, влияние последствий встраивания секретных данных в контейнер можно уменьшить за счет увеличения размера блока.

2.3.5. Метод квантования изображений.

Метод основан на межпиксельной зависимости, которую можно описать некоторой функцией .

В простейшем случае, можно рассчитать разность между смежными пикселями и задать ее в качестве параметра для функции .

В данном методе сокрытие информации проводится путем корректирования разностного сигнала .

Стегоключ представляет собой таблицу, которая каждому возможному значению ставит в соответствие определенный бит , например:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | -4 | -3 | -2 | -1 | 0 | +1 | +2 | +3 | +4 |
|  | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |

Для сокрытия *i*-го бита сообщения вычисляется . Если не соответствует секретному биту, который необходимо скрыть, то значение заменяется ближайшим , для которого это условие выполняется. При этом корректируются значения интенсивностей пикселей, между которыми вычислялась разница .

Извлечение секретного сообщения осуществляется согласно значению , соответствующему разнице

3. Рабочее задание.

3.1. Разработка программного модуля ЭЦП на основе эллиптической кривой (ЭК).

Задана эллиптическая кривая y2 = x3 + ax2 + bx +( c+i ) над полем GF(p). Коэффициент а=0 для всех вариантов, переменная i – целое 0,

стартовое значение i=0.

Остальные параметры кривой приведены в Табл. 1.

Номер варианта определяется следующим образом: (25\*(Nгр)mod4 + N)mod50,

где Nгр – номер группы (4 или 5), N – номер по списку в группе. Для реализации первой части задания необходимо выполнить следующую последовательность действий:

1. Найти базовую точку P(x,y), принадлежащую ЭК, со следующими параметрами:
   * x – координата задается из условия x Floor[p/2];
   * порядок точки должен быть простым числом, б*о*льшим 2p/3;
   * поиск точки может быть проведен с помощью изменения (инкремента) переменной "i";
   * эллиптическая кривая должна быть гладкой.
2. Разработать программный модуль, реализующий алгоритм ЭЦП и хэш- функцию, согласно варианту в Табл. 1.
3. Провести верификацию программного модуля ЭЦП на текстовом файле, содержащем данные из студенческого билета.

Таблица 1. Варианты индивидуальных заданий.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | b | c + i | p | Алгоритм | Хэш-функция |
| 1 | 31 | 28+i |  | ECDSA | "SHA384" |
| 2 | 29 | 51+i |  | ГОСТ Р 3410-2001 | "SHA256" |
| 3 | 22 | 11+i |  | Nyberg-Rueppel | "SHA" |
| 4 | 40 | 18+i |  | ECDSA | "MD5" |
| 5 | 23 | 15+i |  | ГОСТ Р 3410-2001 | "SHA512" |
| 6 | 7 | 3+i |  | Nyberg-Rueppel | "SHA384" |
| 7 | 15 | 5+i |  | ECDSA | "SHA256" |
| 8 | 30 | 15+i |  | ГОСТ Р 3410-2001 | "SHA" |
| 9 | 60 | 9+i |  | Nyberg-Rueppel | "MD5" |
| 10 | 29 | 1+i |  | ECDSA | "SHA512" |
| 11 | 36 | 4+i |  | ГОСТ Р 3410-2001 | "SHA384" |
| 12 | 120 | 8+i |  | Nyberg-Rueppel | "SHA256" |
| 13 | 101 | 2+i |  | ECDSA | "SHA" |
| 14 | 53 | 4+i |  | ГОСТ Р 3410-2001 | "MD5" |
| 15 | 65 | 30+i |  | Nyberg-Rueppel | "SHA512" |
| 16 | 33 | 11+i |  | ECDSA | "SHA384" |
| 17 | 42 | 5+i |  | ГОСТ Р 3410-2001 | "SHA256" |
| 18 | 60 | 43+i |  | Nyberg-Rueppel | "SHA" |
| 19 | 23 | 7+i |  | ECDSA | "MD5" |
| 20 | 25 | 25+i |  | ГОСТ Р 3410-2001 | "SHA512" |
| 21 | 17 | 24+i |  | Nyberg-Rueppel | "SHA384" |
| 22 | 51 | 57+i |  | ECDSA | "SHA256" |
| 23 | 55 | 22+i |  | ГОСТ Р 3410-2001 | "SHA" |
| 24 | 88 | 18+i |  | Nyberg-Rueppel | "MD5" |
| 25 | 23 | 9+i |  | ГОСТ Р 3410-2001 | "SHA512" |

Продолжение табл. 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | b | c + i | p | Алгоритм | Хэш-функция |
| 26 | 31 | 28+i | 1086133 | ECDSA | "SHA384" |
| 27 | 29 | 51+i | 1086139 | ГОСТ Р 3410-2001 | "SHA256" |
| 28 | 22 | 11+i | 1086149 | Nyberg-Rueppel | "SHA" |
| 29 | 44 | 18+i | 1086161 | ECDSA | "MD5" |
| 30 | 23 | 15+i | 1086179 | ГОСТ Р 3410-2001 | "SHA512" |
| 31 | 7 | 3+i | 1086191 | Nyberg-Rueppel | "SHA384" |
| 32 | 15 | 5+i | 1086193 | ECDSA | "SHA256" |
| 33 | 30 | 15+i | 1086199 | ГОСТ Р 3410-2001 | "SHA" |
| 34 | 60 | 9+i | 1086203 | Nyberg-Rueppel | "MD5" |
| 35 | 150 | 1+i | 1086247 | ECDSA | "SHA512" |
| 36 | 400 | 4+i | 1086251 | ГОСТ Р 3410-2001 | "SHA384" |
| 37 | 180 | 8+i | 1086257 | Nyberg-Rueppel | "SHA256" |
| 38 | 133 | 2+i | 1086259 | ECDSA | "SHA" |
| 39 | 217 | 4+i | 1086263 | ГОСТ Р 3410-2001 | "MD5" |
| 40 | 90 | 30+i | 1086277 | Nyberg-Rueppel | "SHA512" |
| 41 | 170 | 11+i | 1086299 | ECDSA | "SHA384" |
| 42 | 70 | 5+i | 1086301 | ГОСТ Р 3410-2001 | "SHA256" |
| 43 | 60 | 100+i | 1086307 | Nyberg-Rueppel | "SHA" |
| 44 | 140 | 7+i | 1086331 | ECDSA | "MD5" |
| 45 | 120 | 25+i | 1086343 | ГОСТ Р 3410-2001 | "SHA512" |
| 46 | 190 | 30+i | 1086347 | Nyberg-Rueppel | "SHA384" |
| 47 | 111 | 433+i | 1086353 | ECDSA | "SHA256" |
| 48 | 55 | 22+i | 1086361 | ГОСТ Р 3410-2001 | "SHA" |
| 49 | 88 | 18+i | 1086373 | Nyberg-Rueppel | "MD5" |
| 50 | 23 | 9+i | 1086389 | ГОСТ Р 3410-2001 | "SHA512" |

3.2 Встраивание идентификационной информации (основных элементов содержимого студенческого билета) в фиксированный контейнер – фотографию студента.

Для реализации второй части задания необходимо выполнить следующую последовательность действий:

1. Подготовить контейнер-оригинал в формате BMP24: цифровую фотографию с размерами, указанными в Табл. 2.
2. Провести предварительную подготовку встраиваемой информации из Табл. 3, для чего перевести все символы ЦВЗ в двоичную форму и выровнять цифры до размера букв – 11бит/символ с использованием функции PadLeft[\*\*\*,11], сформировать битовую строку предназначенную для встраивания в фотографию.
3. Определить цветовой канал для встраивания информации по следующему правилу: Nmod3= 0 - > R; 1 -> G; 2 -> B.
4. Разработать программный модуль для встраивания ЦВЗ в соответствии с методом и стего-путем, приведенными в Табл. 2.
5. Провести верификацию ЦВЗ путем восстановления встроенных данных по соответствующему алгоритму.
6. Создать ЭЦП для модифицированного контейнера со встроенным ЦВЗ с использованием функции FileHash[].

Таблица 2. Варианты реализации методов встраивания.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вариант, Nmod4+1 | 1 | 2 | 3 | 4 |
| Размер фотографии,  ширина х высота | 240х320 | 240х320 | 240х320 | 240х320 |
| Размер блока, точек | - |  |  | 4х4 |
| Метод встраивания  ЦВЗ | **Метод замены наименьшего значащего бита** | **Метод псевдослучайного интервала** | **Метод псевдослучайной перестановки** | **Метод блочного сокрытия** |
| Стего путь | Последовательно, непрерывно,  по строкам. | Последовательно, непрерывно,  по строкам. | Последовательно по стего пути. | Последовательно, непрерывно, по столбцам |

Таблица 3. ЦВЗ – идентификационные данные

|  |  |
| --- | --- |
| Наименование документа | Студенческий |
| билет |
| Номер документа |  |
| Фамилия |  |
| Имя |  |
| Отчество |  |
| Группа |  |
| Номер по списку в группе |  |
| Дата выдачи |  |
| курс | четвертый |

**СПИСОК ЛИТЕРАТУРЫ**

1. **Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.** Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы.- М.: КомКнига, 2006.-328с.
2. **Тилборг Ван Х.К.Ф.** Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.:Мир,2006,стр.471,ил.
3. **Болотов А.А., Гашков С.Б., Фролов А.Б.** Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых –М.: КомКнига, 2006,стр.280,ил.
4. **Грибунин В.Г., Оков И.Н., Туринцев И.В.** Цифровая стеганография. –М.: СОЛОН-Пресс,2002.- 272 стр.
5. **Аграновский А. В., Балакин А.В., Грибунин В.Г., Сапожников С.А.** Стеганография, цифровые водяные знаки и стегоанализ. – М.: Вузовская книга, 2009. – 220 с.: ил.
6. **Конахович Г.Ф., Пузыренко А.Ю.** Компьютерная стеганография. Теория и практика.-К.: "МК-Пресс", 2006.-288с.,ил.
7. **Миано Дж.** Форматы и алгоритмы сжатия изображений в действии. Учеб.пособ.- М.: Триумф, 2003-336 с.: ил.
8. **Alasdair McAndrew.** Introduction to cryptography with open-source software. - CRC Press, 2011. – 441 p.: pict.

**СОДЕРЖАНИЕ**

1.Элементы эллиптической криптографии.

1.1. Эллиптические кривые. Определение.

1.2. Число точек эллиптической кривой.

1.3. Сложение точек эллиптической кривой.

1.3.1. Геометрия эллиптических кривых.

1.3.2. Законы сложения точек эллиптической кривой.

1.3.3. Умножение точки ЭК на целое число.

1.4. Построение односторонней функции на основе эллиптической кривой.

1.5. Протоколы электронной цифровой подписи на основе эллиптических

кривых.

1.5.1. Схема Nyberg-Rueppel электронной подписи

1.5.2. Алгоритм ECDSA электронной подписи с использованием группы точек эллиптической кривой.

1.5.3. Алгоритм ГОСТ Р 3410 - 2001 электронной подписи

с использованием группы точек эллиптической кривой .

2. Встраивание идентификационной информации в цифровой объект.

2.1. Модель процесса встраивания ЦВЗ.

2.2. Цветовые модели

2.3. Неформатные методы сокрытия в графических изображениях – пространственная область. Методы замены.

2.3.1. Метод замены наименьшего значащего бита (НЗБ).

2.3.2. Метод случайного интервала.

2.3.3. Метод псевдослучайной перестановки.

2.3.4. Метод блочного сокрытия

2.3.5. Метод квантования изображений.

3. Рабочее задание.

3.1. Разработка программного модуля ЭЦП на основе эллиптической кривой (ЭК).

3.2 Встраивание идентификационной информации (основных элементов содержимого студенческого билета) в фиксированный контейнер – фотографию студента.