МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ имени

Кафедра IT - Инжиниринг

**ЛАБОРАТОРНАЯ РАБОТА №6**

По дисциплине «Проектирование микропроцессорных систем»

На тему: Электронная цифровая подпись.

Специальность 7M06103-Вычислительная техника и программное обеспечение

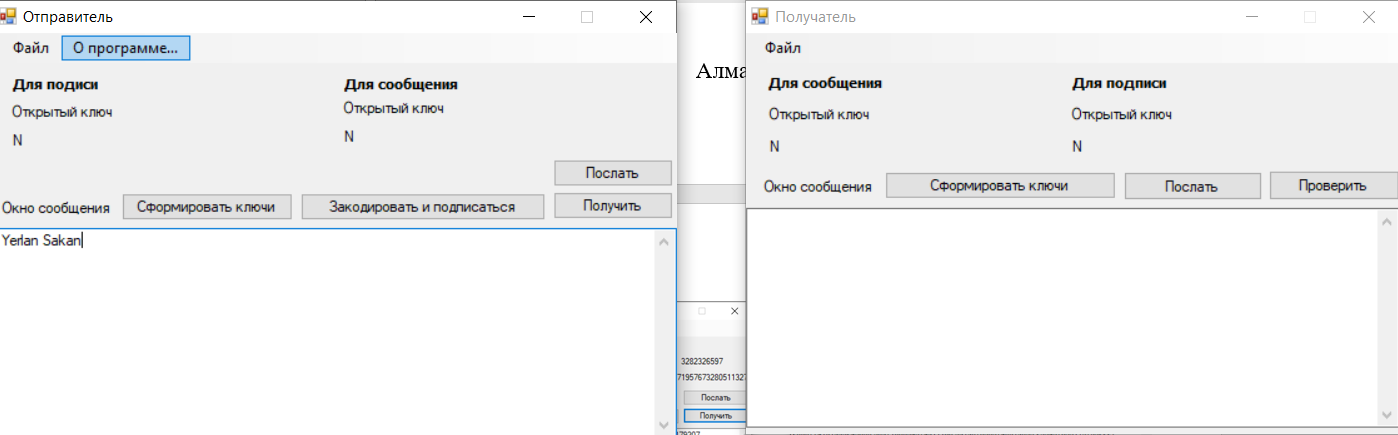
Выполнил Сакан Ерлан Группа МВТн-21-2

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_202\_\_\_г.

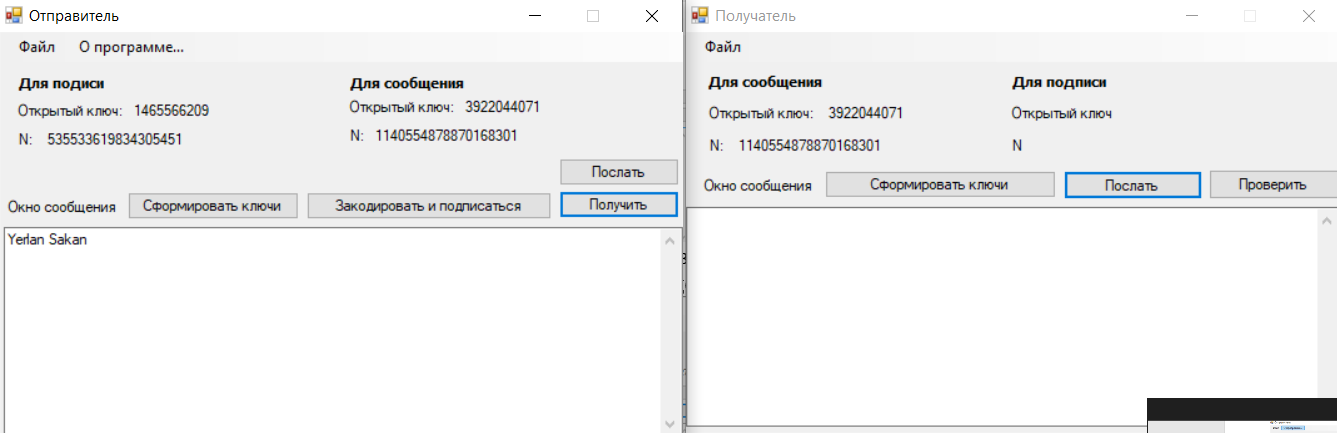
(оценка) (подпись)

Алматы 2022

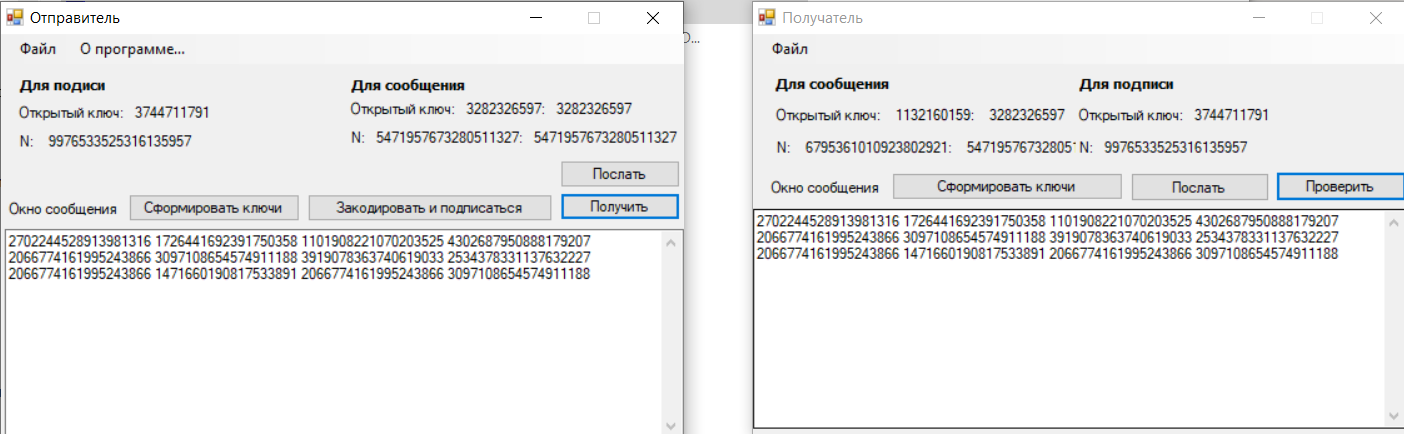
Для начала необходимо сформировать сообщение и открытый ключ подписи



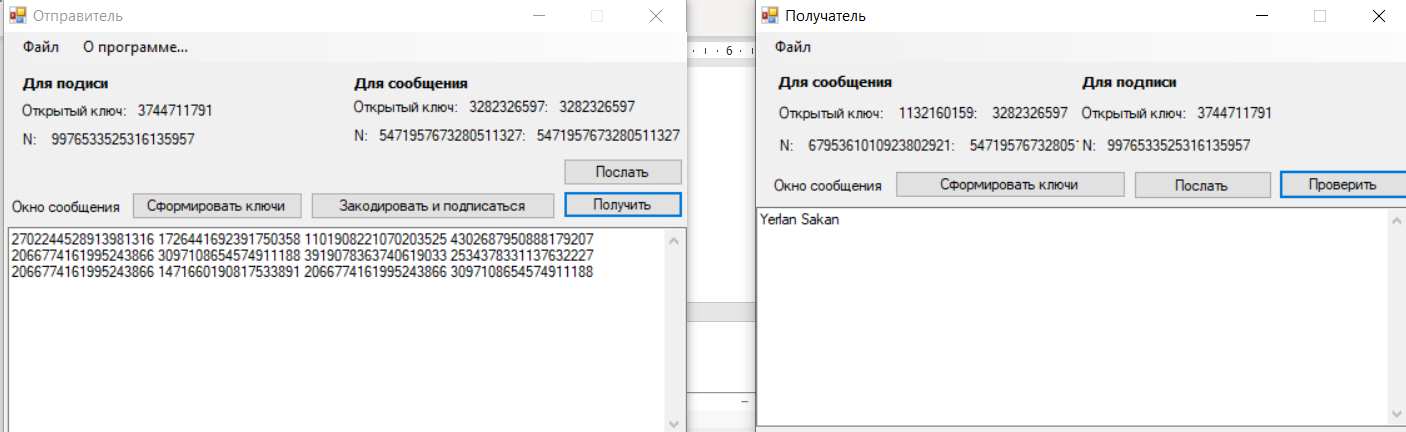
Затем получатель сформировывает свой ключ и отправляет, который мы получаем открытый ключ для сооющения



Далее необходимо его закодировать и послать получателю



Получатель его и “подпись верна”

****

1. В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭЦП?

Хэш-функции применяются для тестирования логических устройств, для быстрого поиска и проверки целостности записей в базах данных. построения систем контроля целостности данных при их передаче или хранении, аутентификация источника данных.

Перечислите стандарты хэш-функций, действующие в Российской Федерации

В основном ГОСТ Р 34.11, начиная с 1994 года – 1994, 2012, 2018

1. Опишите процедуры постановки и проверки ЭЦП

Система ЭЦП включает две процедуры: 1) процедуру постановки подписи; 2) процедуру проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи - открытый ключ отправителя.

Какая информация содержится в ЭЦП?

Данные владельца; уникальный ключ проверки; наименование средства электронной подписи; название удостоверяющего центра.

1. Перечислите стандарты ЭЦП, действующие в Российской Федерации

Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012 (основан на сложности вычисления дискретного логарифма в группе точек эллиптической кривой)

На каких принципах основана криптостойкость современных алгоритмов ЭЦП?

Наиболее известными схемами для создания электронной цифровой подписи являются схемы RSA, Эль-Гамаля (ElGamal), Рабина, Шнорра, Диффи-Лампорта. Применение алгоритма RSA для создания ЭЦП основано на зашифровании сообщения секретным (закрытым) ключом, и расшифровании – открытым.

1. Приведите пример реализации алгоритма ЭЦП (RSA, Эль-Гамаль, DSA)

Действия объекта В:

Берет Р = 3, Q = 11.

Берет модуль N = P × Q = 3 × 11 = 33.

Берет значение функции Эйлера для N = 33: φ(N) = (P-1) × (Q-1) = 2 × 10 = 20.

Берет в качестве открытого ключа Kв произвольное число с учетом условия: 1 < Kв ≤ φ(N), НОД (Kв, φ(N)) = 1, допустим Kв = 7.

Решаем значение секретного ключа κв используя алгоритм Евклида: κв ≡ = 3.

объект В передает объекту А пару чисел (N = 33, Kв = 7).

Действия объекта A:

Показывает шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Допустим буква А представляется как число 1, буква В это 2 и С = 3. Припустим что сообщение С А В можно показать как последовательность числе 321, то есть M1 = 3, M2 = 1, M3 = 2.

Шифрует сообщение, М используя ключ Kв = 7 и N = 33 по формуле: Ci = MiKв (mod N) = Mi7(mod 3).

Получаем:

Ci = 37(mod 33) = 2187 (mod 33) = 9

Ci = 17(mod 33) = 1 (mod 33) = 1

Ci = 27(mod 33) = 128 (mod 33) = 29

Передает объекту В криптограмму: C1, C2, C3 = 9, 1, 29.

Действия объекта B:

Расшифровывает принятую криптограмму C1, C2, C3 используя секретный ключ ≡ = 3 по формуле:Mi = CiKв (mod N) = Ci3 (mod 3)

M1= 93 (mod 33) = 729 (mod 33) =3.

M2 = 13 (mod 33) = 1 (mod 33) =1.

M2 = 293 (mod 33) = 24389 (mod 33) =2.

Объект получил исходное сообщение, которое послал объект A.