Тема

Программная реализация вычисления и проверки электронной подписи по алгоритму ElGamal.

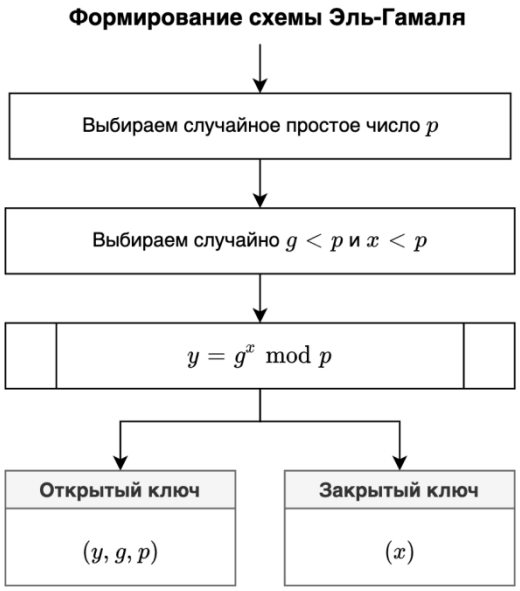
Описание алгоритма

На вход подаётся сообщение M.
На выходе подпись и секретный ключ.

Для формирования электронной подписи нужно сформировать схему Эль-Гамаля (Шаг1), далее по документу M формируется его подпись и закрытый ключ (Шаг2). Последним действием является проверка (Шаг3).

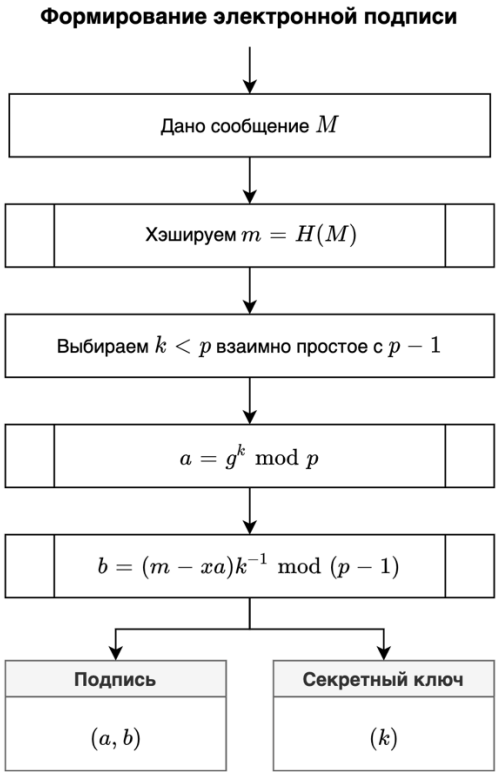
Шаг1

На вход подаётся информация о выборе длины ключей. Далее все нужные данные генерируются случайным образом и сохраняются в файл.
На выходе получаем открытый ключ и закрытый ключ, которые сохраняем в файлах. Закрытый ключ шифруется.



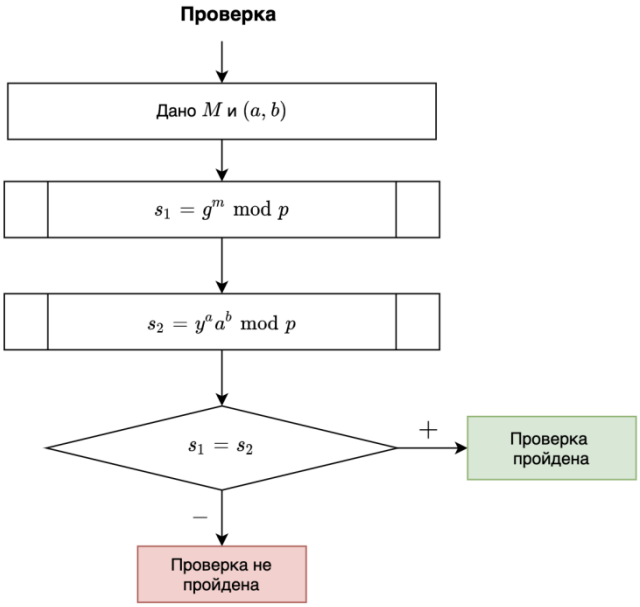
Шаг2

На вход подаётся документ M, далее после завершения алгоритма выходными параметрами являются подпись и секретный ключ.



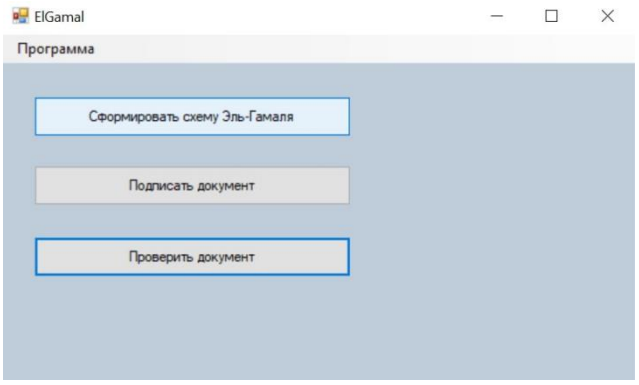
Шаг3

На вход подается документ M и его подпись, которая извлекается из хранилище (файл, формата xml). На выходе получаем статус проверки: пройден/не пройден.

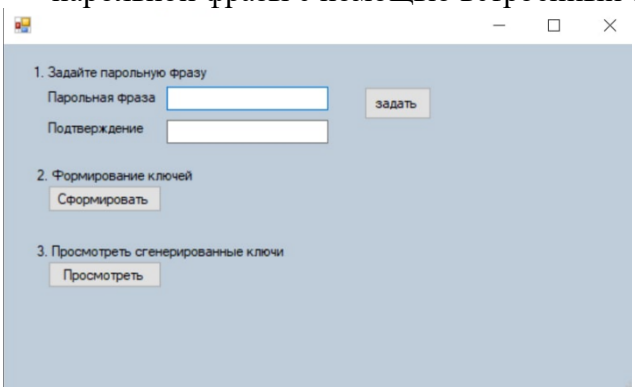


Архитектура

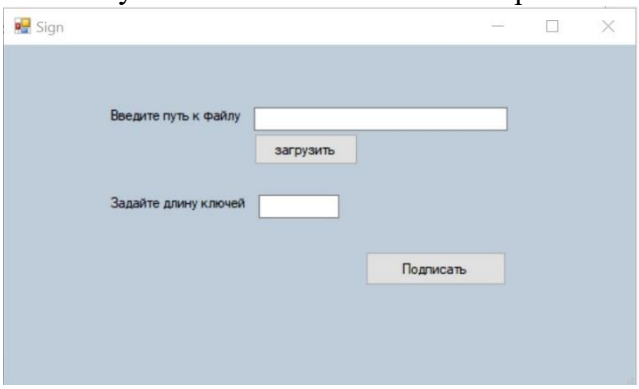
1. Главный экран
    1) Формирование схемы (Шаг1 из алгоритма).
    2) Подписать документ.
    3) Проверить документ.



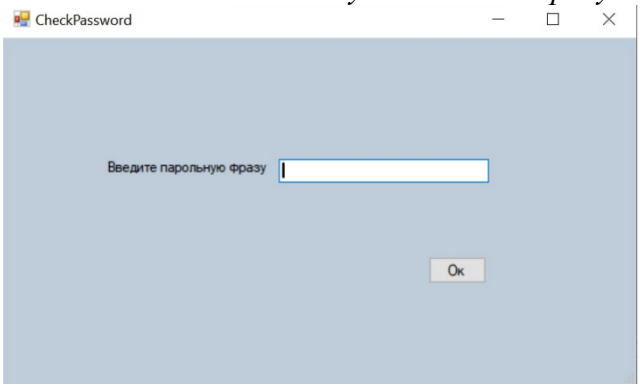
2. Формирование схемы – диалоговое окно.
   1) Нужно задать парольную фразу, с помощью которой будет шифроваться закрытый ключ.
   2) Генерируем открытый и закрытый ключи, которые сохраняются в файлах. Причем закрытый ключ хранится в зашифрованном виде, шифрование происходит с помощью одиночной подстановки по ключу, а хэширование парольной фразы с помощью встроенный средств c#.



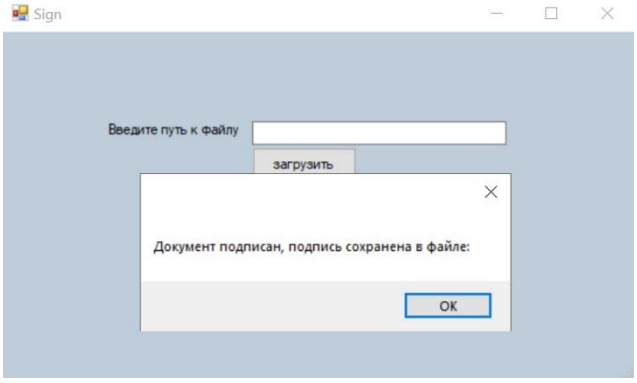
3. Подписание документа – диалоговое окно.
   Используется Шаг2 из описания алгоритма.



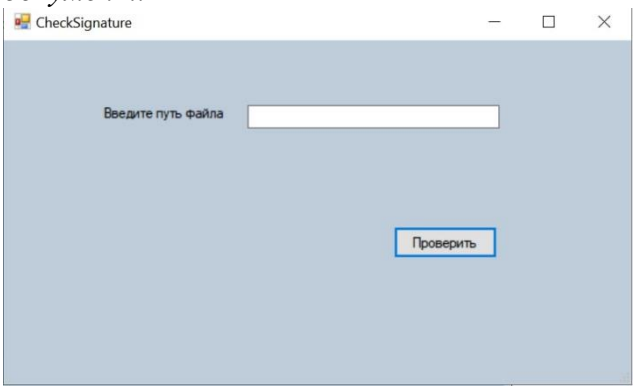
После нажатия на кнопку подписать требуется ввести парольную фразу.



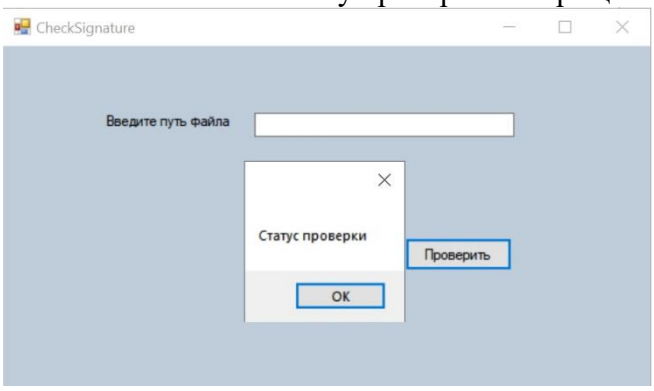
После подписания приходит оповещение о названии файла, в котором сохранена подпись. Фактически это будут два целых числа (a, b). *Подпись документа и путь к документу сохраняются в хранилище (файл в формате xml).*



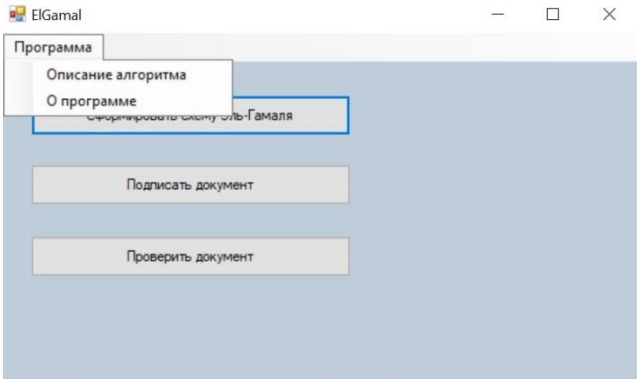
4. Проверка документа – диалоговое окно.
Проверка происходит по Шагу3 из описания алгоритма. На вход подается документ.



После нажатия на кнопку проверки возвращается статус.



5. Меню главного экрана.
В меню можно прочитать описание алгоритма и открыть окно “О программе”.



Открытые архитектурные вопросы:

1. Длина ключей должна задаваться при их генерации, а не при подписании документа (п. 3 архитектуры)
2. Неясно, где будет хранится подпись. Может в том же каталоге, что и подписанный документ?
3. Неясно, откуда будет взята подпись при проверке подписанного документа. Возможно, стоит добавить подпись к файлу.