Алгоритм реализации известных методов шифрования в электронной цифровой подписи

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Овчинников Б.А.

Половеня С.И. – к.т.н., доцент

Постоянный интенсивный рост использования мобильных устройств связи определяет потребность в наличии мобильной электронной цифровой подписи. Ранее мы привыкли видеть ЭЦП пользователя на компьютере, переносном устройстве или записанной на удостоверении личности. Теперь ЭЦП пользователя будет привязана к его sim-карте. Хранение ЭЦП на SIM-карте делает процедуру подписи электронных документов удобной и простой: пользователь не ограничен доступом к компьютеру, документ может быть подписан в любое время и в любом месте. Единственные необходимые для этого условия – наличие SIM-карты с поддержкой SIMiD и устройства с функцией отправки и получения SMS (как смартфона, так и самого простого мобильного телефона). Процесс подписания электронного документа представляет собой отправку специальных зашифрованных сообщений – бинарных SMS – и подтверждается вводом PIN-кода услуги SIMiD. Приложение ЭЦП на SIM реализует сервис идентификации и аутентификации владельца SIM с использованием сертификата открытого ключа. После завершения аутентификации приложение ЭЦП на SIM устанавливает защищенное соединение с сервером авторизации с использованием криптографических алгоритмов СТБ 34.101.45., RSA , DSA , ECDSA. Наиболее успешные – это алгоритмы на основе эллиптических кривых СТБ 34.101.45 и ECDSA.

Алгоритм генерации и проверки электронной цифровой подписи на основе эллиптических кривых представлен на рисунке 1:

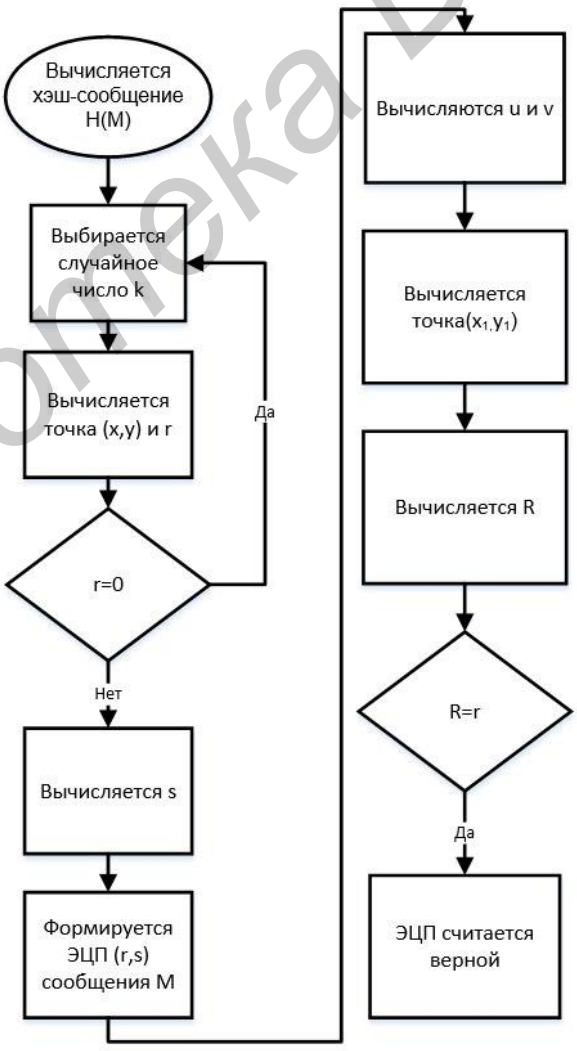

Рис. 1 – Алгоритм ЭЦП на основе эллиптических кривых

Пояснение алгоритма представленного на рисунке 1 :
Генерация ЭЦП (пользователь А подписывает сообщение M):

- вычисляется хэш-собщения $H(M)$;
- выбирается случайное целое число k, взаимно простое с n (то есть не имеющее других общих с n делителей, кроме 1; поскольку n является простым числом по определению, данное условие выполняется автоматически), $1 < k < n - 1$;
- вычисляется точка $(x, y) = kP$ и $r = x \bmod n$.В случае если $r = 0$, повторяетсявыбор k;
- вычисляется $s = k^{-1}(H(M) + rd) \bmod n$;
- цифровой подписью сообщения M является пара чисел (r, s). Проверка ЭЦП (пользователь В проверяет ЭЦП пользователя А под сообщением M):
- если $r = 0$, то полученная ЭЦП неверна;
- вычисляется хэш-сообщения $H(M)$;
- вычисляются $u = s^{-1}H(M) \bmod n$ и $v = s^{-1}r \bmod n$;
- вычисляется точка $(x_1, y_1) = uP + vQ$;
- вычисляется $R = x_1 \bmod n$;
- ЭЦП считается верной, если $R = r$.

Основные достоинства заключаются в том, что параметры эллиптической кривой, личный и открытый ключи могут быть использованы для контроля целостности и подлинности, но и для обеспечения конфиденциальности защищаемой информации. В стандарте определяются алгоритмы транспорта ключа, предназначенные для защищённой передачи ключей и других секретных данных между двумя сторонами. Так же достоинство состоит в том , что по сравнению с системами на основе RSA они обеспечивают существенно более высокую стойкость при равной трудоёмкости.

Список использованных источников:

1. Государственный стандарт Республики Беларусь – СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых.
2. Горбатов В.С., Полянская О.Ю. – Основы технологии PKI – 2011.