Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование алгоритмов генерации и верификации электронной цифровой подписи

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

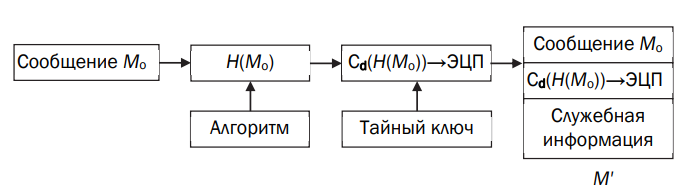
ЭЦП делятся на три типа:

• на основе симметричных систем (с тайным ключом);

• на основе симметричных систем и посредника;

• на основе асимметричных систем (с открытым ключом).

Схема подписания сообщения ЭЦП:



1. **Практическая часть**

**2.1 ЭЦП на основе RSA**

При генерации ЭЦП (по классической схеме) для сообщения

М отправитель последовательно выполняет следующие действия:

• вычисляет хеш (хеш-образ) сообщения М: Н(М);

• вычисляет содержание ЭЦП (собственно ЭЦП S) по хешу

Н(М) с использованием своего закрытого ключа d: S =Сd(Н(М));

• присоединяет (конкатенирует) ЭЦП к сообщению М и некоторой служебной информации, создавая таким образом итоговое

сообщение М';

• посылает сообщение М' получателю;

– получив сообщение М', другая сторона последовательно выполняет следующие действия:

• отделяет цифровую подпись S от сообщения М (для общего

случая применим одинаковые символьные обозначения);

• применяет к сообщению М операцию хеширования, используя ту же функцию, что и отправитель, и получает хеш-образ полученного сообщения;

• используя открытый ключ отправителя, расшифровывает S,

т. е. извлекает из ЭЦП хеш-образ отправленного сообщения;

• проверяет соответствие (равенство) обоих хеш-образов, и если

они совпадают, то отправитель действительно является тем, за кого

себя выдает, а сообщение при передаче не подверглось искажению.

При этом стойкость ЭЦП к подделыванию (криптостойкость)

Реализация метода представлена на рисунке 2.1.

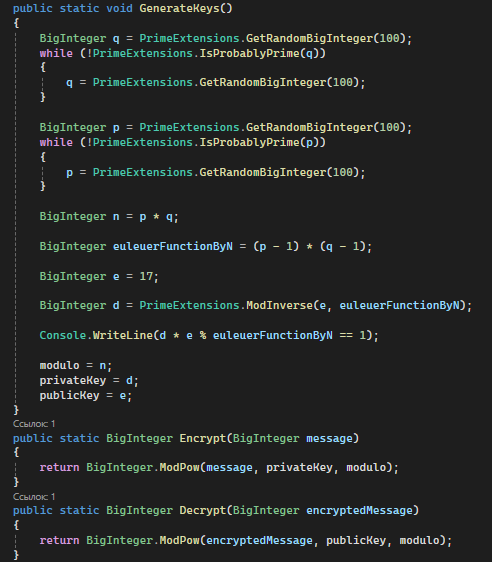


Рисунок 2.1 – ЭЦП на основе RSA

**2.2 ЭЦП на основе DSA**

Общая схема генерации и верификации ЭЦП DSA

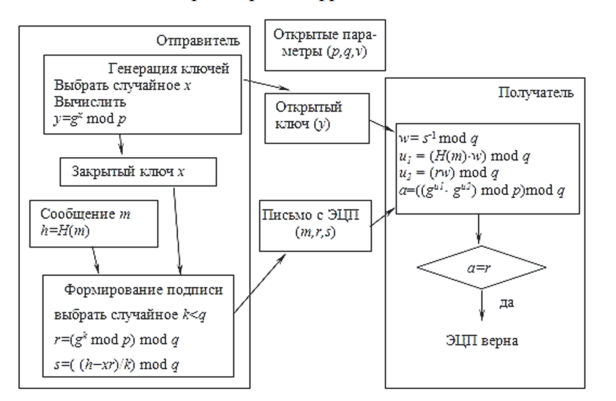


Рисунок 2.2 – Схема DSA

**2.3 ЭЦП на основе Эль-Гамаля**

Для подписи сообщения 𝑀𝑜​ отправитель использует открытый ключ 𝑦*y*, 𝑔*g*, 𝑝*p* и секретный ключ 𝑥*x*. Он выбирает случайное число 𝑘*k*, взаимно простое с 𝑝−1*p*−1, и вычисляет подпись 𝑆={𝑎,𝑏}*S*={*a*,*b*}:

1. 𝑎≡𝑔𝑘mod  𝑝*a*≡*gk*mod*p*
2. Решает уравнение 𝐻(𝑀𝑜)≡(𝑥𝑎+𝑘𝑏)mod  (𝑝−1) для 𝑏

Получателю отправляется сообщение 𝑀′=𝑀𝑜∣∣𝑆. Для верификации подписи вычисляется хеш 𝐻(𝑀𝑝)=ℎ. Подпись считается действительной, если выполняется равенство: 𝑦𝑎⋅𝑎𝑏≡𝑔ℎmod  𝑝

**2.4 ЭЦП на основе Шнорра**

Ключевая информация: 𝑝 – простое число (512-1024 бита), 𝑞 – 160-битное простое число, делитель 𝑝−1*p*−1; 𝑔≠1 такое, что 𝑔^𝑞≡1mod  𝑝. Числа 𝑝, 𝑔, 𝑞 являются открытыми и используются группой пользователей. Выбирается секретный ключ 𝑥<𝑞, вычисляется открытый ключ 𝑦≡𝑔−𝑥mod  𝑝.

Для подписи сообщения 𝑀𝑜​ выбирается случайное число 𝑘(1<𝑘<𝑞), и вычисляется параметр 𝑎≡𝑔𝑘mod  𝑝. Хеш вычисляется от конкатенации сообщения 𝑀𝑜​ и числа 𝑎: ℎ=𝐻(𝑀𝑜∣∣𝑎). Затем вычисляется значение 𝑏≡(𝑘+𝑥ℎ)mod  𝑞. Отправляется 𝑀′=𝑀𝑜∣∣𝑆, где 𝑆={ℎ,𝑏}.

Для проверки подписи получатель вычисляет 𝑋≡𝑔𝑏𝑦ℎmod  𝑝 и проверяет выполнение равенства ℎ=𝐻(𝑀𝑝∣∣𝑋). Подпись достоверна, если равенство выполняется.

Результат выполнения всех алгоритмов представлен на рисунке.

