Министерство образования Республики Беларусь

Учреждение образования БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

Отчёт по лабораторной работе №7

По теме «Криптография с использованием эллиптических кривых»

Выполнили: студент гр. 053501 Кривецкий Р. А.

Проверил: ассистент кафедры информатики Лещенко Е. А.

Минск 2023

**СОДЕРЖАНИЕ**

[1 Теоретические сведения 3](#_Toc148061125)

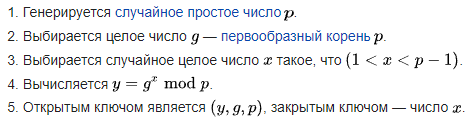
[2 Программная реализация 5](#_Toc148061126)

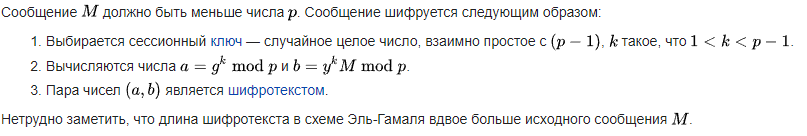
[Заключение 6](#_Toc148061127)

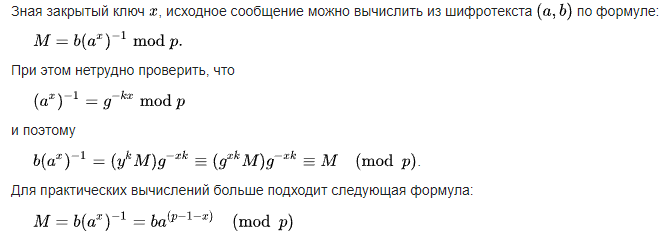
[Приложение А(обязательное) Листинг программного кода 7](#_Toc148061128)

# 1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).







Алгоритм работы схемы Эль-Гамаля представлен на рисунке 1.1.

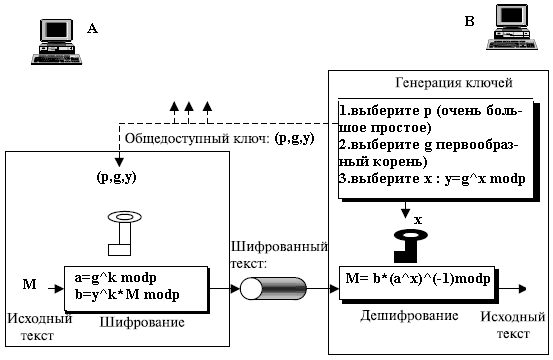


Рисунок 1.1 – Алгоритм работы схемы Эль-Гамаля

Блок-схема алгоритма шифрования и дешифрования для аналога алгоритма Эль-Гамаля на основе эллиптических прямых представлен на рисунке 1.2.

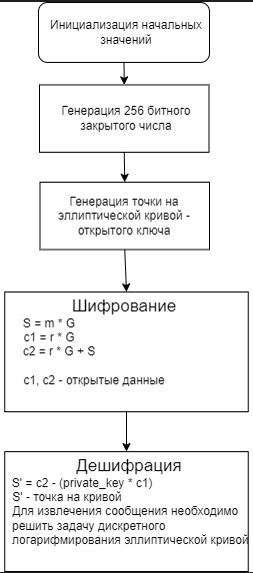


Рисунок 1.2– Аналог алгоритма Эль-Гамаля

на основе эллиптических прямых

**2 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ**

Необходимо реализовать схему шифрования (дешифрования) для аналога алгоритма Эль-Гамаля на основе эллиптических кривых. Программное средство реализовано на языке программирования Python. Демонстрация работы показана на рисунке 2.1

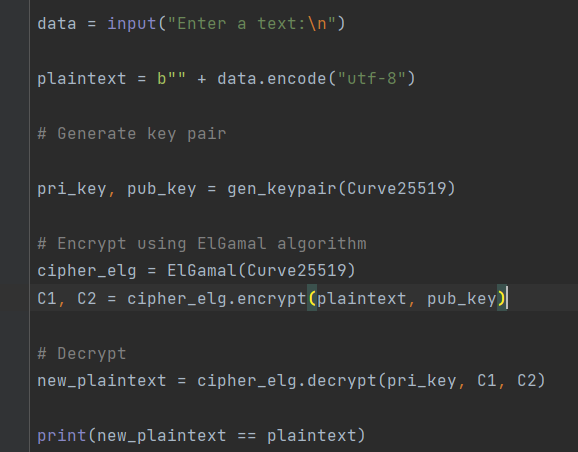


Рисунок 2.1 — Демонстрация работы

# ЗАКЛЮЧЕНИЕ

В заключение, алгоритм Эль-Гамаля на основе эллиптических кривых (ECElGamal) представляет собой эффективный и безопасный криптографический протокол для шифрования данных с использованием эллиптических кривых.

ECElGamal обеспечивает высокий уровень безопасности, основанный на сложности решения дискретного логарифма на эллиптической кривой. Выбор подходящей кривой и правильная реализация ключевых параметров важны для обеспечения стойкости к атакам.

Протокол обеспечивает конфиденциальность передаваемых данных, так как даже при наличии открытого ключа сложно восстановить исходное сообщение без соответствующего закрытого ключа.

Алгоритм широко используется в сфере криптографии, особенно в контексте обеспечения безопасности передачи данных в различных приложениях, включая протоколы обмена ключами и шифрование данных.

Важно правильно выбирать параметры кривой и другие ключевые параметры для обеспечения стойкости и эффективности алгоритма.

Реализация ECElGamal требует внимания к деталям, и использование библиотек, поддерживающих эллиптические кривые, может значительно облегчить этот процесс.

В целом, алгоритм Эль-Гамаля на эллиптических кривых представляет собой мощный инструмент для обеспечения безопасной передачи и защиты данных, особенно в сфере криптографии с открытым ключом.

# ПРИЛОЖЕНИЕ А

(**обязательное)**

**Листинг программного кода**

Файл main.py

from ecc.curve import Curve25519

from ecc.key import gen\_keypair

from ecc.cipher import ElGamal

data = input("Enter a text:\n")

plaintext = b"" + data.encode("utf-8")

# Generate key pair

pri\_key, pub\_key = gen\_keypair(Curve25519)

# Encrypt using ElGamal algorithm

cipher\_elg = ElGamal(Curve25519)

C1, C2 = cipher\_elg.encrypt(plaintext, pub\_key)

# Decrypt

new\_plaintext = cipher\_elg.decrypt(pri\_key, C1, C2)

print(new\_plaintext == plaintext)