Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОССУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОННИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №7

По дисциплине «Методы защиты информации»

По теме «Криптография с использованием эллипти4еских прямых»

Выполнил:

студент гр. 653502

Максименко П.В.

Проверил:

Артемьев В. С.

Минск 2019

1. Постановка зада4и

Написать программу, реализующую схему шифрования алгоритма Диффи-Хеллмана на основе эллипти4еских прямых.

2. Теорети4еская 4асть

Протокол Ди́ффи-Хе́ллмана на эллиптических кривых ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Elliptic curve Diffie–Hellman, ECDH) — [криптографический протокол](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), позволяющий двум сторонам, имеющим пары [открытый/закрытый ключ](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC) на [эллиптических кривых](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%B2%D0%B0%D1%8F), получить общий секретный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), используя незащищённый от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для [формирования нового ключа](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D1%84%D0%BE%D1%80%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0), который затем может использоваться для последующего обмена информацией с помощью алгоритмов [симметричного шифрования](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Это вариация [протокола Диффи-Хеллмана](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0) с использованием [эллиптической криптографии](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F).

3. Блок-схема

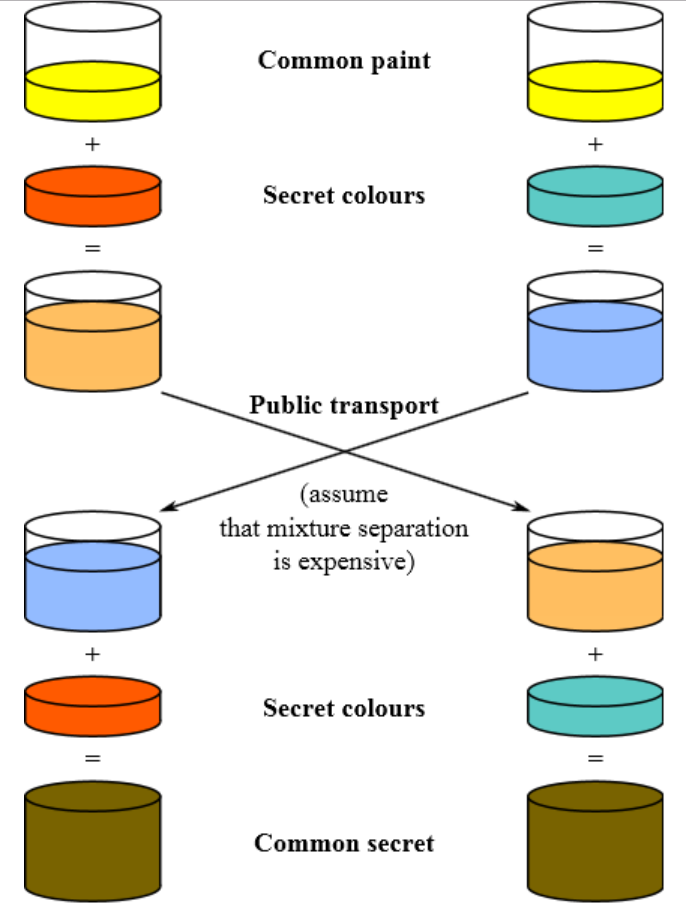


Рис 3.1. Схема работы алгоритма.

4. Ход программы



Рис 4.1. Данные, поступающие на вход



Рис 4.2. Задание клю4ей

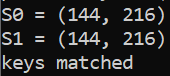


Рис 4.3. Вы4исление и сверка общего секретного клю4а



Рис 4.4. Зашифрованные данные

5. Код программы

int DFP(int inp\_data)

{

std::cout << "input data = " << inp\_data << std::endl;

//F37

//y^2 = x^3 - x + 3;

int N = 42;

int n = 7;

float h = N / n;

int P[2]; // rand

int G[2];

P[0] = 2;

P[1] = 3;

// basic subgroup point create

G[0] = P[0] \* h;

G[1] = P[1] \* h;

int d[2]; // [1, n-1]

int H0[2];

int H1[2];

d[0] = 3;

d[1] = 4;

// public keys creation

H0[0] = d[0] \* G[0];

H0[1] = d[0] \* G[1];

H1[0] = d[1] \* G[0];

H1[1] = d[1] \* G[1];

std::cout << "private keys = " << d[0] << ", " << d[1] << std::endl;

std::cout << "public keys = (" << H0[0] << ", " << H0[1] << "); and ("<< H1[0] << ", " << H1[1] << ")" << std::endl;

// key exchange

int S0[2];

int S1[2];

S0[0] = d[1] \* H0[0];

S0[1] = d[1] \* H0[1];

S1[0] = d[0] \* H1[0];

S1[1] = d[0] \* H1[1];

std::cout << "S0 = (" << S0[0] << ", " << S0[1] << ")" << std::endl;

std::cout << "S1 = (" << S1[0] << ", " << S1[1] << ")" << std::endl;

int flag = 0;

if (S0[0] == S1[0])

{

if (S0[1] == S1[1])

{

std::cout << "keys matched" << std::endl;

}

else

{

flag = 1;

std::cout << "y var was grong" << std::endl;

}

}

else

{

flag = 1;

std::cout << "x var was grong" << std::endl;

}

// encrypt data if S0 == S1

if (flag == 0)

{

return inp\_data + S0[0] - S0[1];

}

else

{

return inp\_data;

}

}

int main()

{

SetConsoleCP(1251);

SetConsoleOutputCP(1251);

// lab7

// DFP on EC

int data = 3274;

int output\_data;

output\_data = DFP(data);

if (output\_data == data)

{

std::cout << "error" << std::endl;

}

else

{

std::cout << "output data = " << output\_data << std::endl;

}

return 0;

}

6. Вывод

В ходе выполнения лабораторной работы был успешно реализован алгоритм Диффи-Хеллмана на основе эллипти4еских прямых.

Были выявлены возможности улу4шения алгоритма. К примеру, вместо использования кривых Вейерштрасса над простыми полями можно использовать кривые Коблица над двои4ными полями, 4то обеспе4ит особо эффективное сложение то4ек и скалярное умножение. Также можно использовать двои4ные кривые и кривые Эдвардса.

Протокол Диффи-Хеллмана отлично противостоит пассивному нападению, но в случае реализации атаки «человек посередине» он не устоит. В самом деле, Атакующий заменяет сообщения переговоров о ключе на свои собственные и таким образом получает два ключа — свой для каждого из законных участников протокола. Далее он может перешифровывать переписку между участниками, своим ключом для каждого, и таким образом ознакомиться с их сообщениями, оставаясь незамеченным.