Крайние сроки сдачи лабораторных работ.

Лабораторная работа № 1 – 31 марта.

Лабораторная работа № 2 – 30 апреля.

Лабораторная работа № 3 – 31 мая.

Для получения зачета необходимо сдать все лабораторные работы и ответить на вопросы на коллоквиуме.

Лабораторная работа № 1.

см. Варианты 1.1 – 1.8.

Лабораторная работа № 2.

см. Варианты 2.1 – 2.8.

Лабораторная работа № 3.

При помощи функций криптографической библиотеки .NET реализуйте гибридную криптосистему, включающую:

1) генерацию ключевой пары RSA;
2) шифрование и расшифрование документа симметричным криптоалгоритмом;
3) шифрование и расшифрование сеансового ключа симметричного алгоритма при помощи ключей RSA;
4) формирование и проверку цифровой подписи документа.

Полученный шифротекст, открытые ключи должны сохраняться и передаваться через файлы.

Для каждой лабораторной работы должен быть подготовлен отчет. Структура отчета:

1. Титульный лист.
2. Формулировка задания.
3. Описание метода решения.
4. Примеры кода программ.
5. Тестовые данные.

Вариант 1.1.

Напишите программу шифрования и расшифрования алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, число e должно генерироваться после вычисления p и q;
2) шифрование данных (целого числа);
3) расшифрование шифртекста (целого числа).

Вариант 1.2.

Напишите программу шифрования и расшифрования алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, при этом число e задается пользователем;
2) шифрование данных (целого числа);
3) расшифрование шифртекста (целого числа).

Вариант 1.3.

Напишите программу формирования цифровой подписи алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, число e должно генерироваться после вычисления p и q;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).

Вариант 1.4.

Напишите программу формирования цифровой подписи алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, при этом число e задается пользователем;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).

Вариант 1.5.

Напишите программу шифрования и расшифрования алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Для ускорения вычислений использовать китайскую теорему об остатках. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, число e должно генерироваться после вычисления p и q;
2) шифрование данных (целого числа);
3) расшифрование шифртекста (целого числа).

Вариант 1.6.

Напишите программу шифрования и расшифрования алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в

мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Для ускорения вычислений использовать китайскую теорему об остатках. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, при этом число e задается пользователем;
2) шифрование данных (целого числа);
3) расшифрование шифртекста (целого числа).

Вариант 1.7.

Напишите программу формирования цифровой подписи алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Для ускорения вычислений использовать китайскую теорему об остатках. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, число e должно генерироваться после вычисления p и q;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).

Вариант 1.8.

Напишите программу формирования цифровой подписи алгоритмом RSA. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Для ускорения вычислений использовать китайскую теорему об остатках. Выполняемые функции программы:

1) генерация пары открытый/закрытый ключ, при этом число e задается пользователем;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).

Вариант 2.1.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;
3) получение общего ключа.

Вариант 2.2.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Использовать «надежные» простые числа. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;
3) получение общего ключа.

Вариант 2.3.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Использовать подгруппы меньшего размера. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;
3) получение общего ключа.

Вариант 2.4.

Реализуйте криптосистему Эль-Гамаля. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация чисел p, g, x, k;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).

Вариант 2.5.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;

3) получение общего ключа.

Вариант 2.6.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Использовать «надежные» простые числа. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;
3) получение общего ключа.

Вариант 2.7.

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Использовать подгруппы меньшего размера. Выполняемые функции программы:

1) генерация чисел p, g, x, y;
2) имитация обмена данными между пользователями;
3) получение общего ключа.

Вариант 2.8.

Реализуйте криптосистему Эль-Гамаля. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Выполняемые функции программы:

1) генерация чисел p, g, x, k;
2) получения цифровой подписи для сообщения (целого числа);
3) проверки цифровой подписи для данного сообщения (целого числа).