Министерство образования и науки РФ

ФГОУ СПО «Хабаровский машиностроительный техникум

ПЛАН-КОНСПЕКТ

урока по дисциплине **«Основы безопасности компьютерных сетей»**

на тему: **«Криптосистемы шифрования данных RSA и Эль Гамаля»**

Разработала преподаватель: **Ермолко Г.С.**

Хабаровск
2012

Тема: **«Криптосистемы шифрования данных RSA и Эль Гамаля»**

Вид занятия: урок-КВН (практическая работа).

Оборудование: ПК, интерактивная доска.

Цель занятия: Повторить и закрепить материал по темам «Криптосистемы шифрования данных RSA и Эль Гамаля»

Образовательный компонент цели:

- Исследование асимметричных криптосистем на примере криптоалгоритмов RSA и Эль Гамаля.
- Систематизация знаний на уровне понимания, применения и анализа.

Развивающий компонент цели:

- Развитие умения работать в группе.
- Развитие дисциплинированности.

Воспитательный компонент цели:

- Воспитание уважение к мнению других, способствовать выработке собственного мнения.
- Воспитание интеллектуальных способностей студента.

Познавательный компонент цели:

- Активизация пройденного материала по теме «Криптография».

План занятия:

1) Организационный момент.(5 мин.)
2) Актуализация знаний. (20 мин.)
3) Закрепление пройденного материала (50 мин.).
4) Подведение итогов. (10 мин.)
5) Домашнее задание (5 мин.)

ХОД ЗАНЯТИЯ

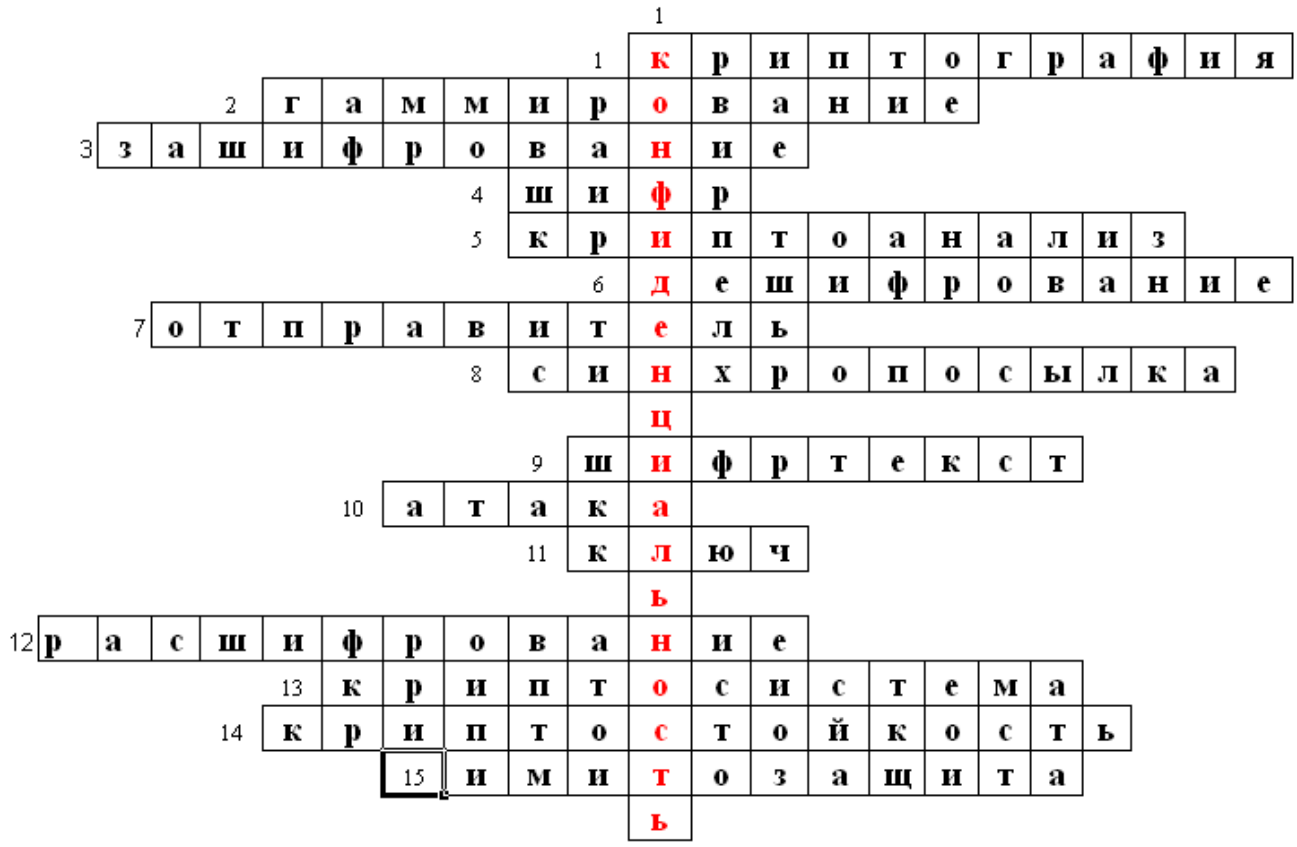
I. Организационный момент

Сообщение студентам цели и структуры занятия. Формирование команд. Выбор капитана команды.

II. Актуализация знаний

Студентам предлагается отгадать кроссворд. За каждый правильный ответ команде присуждается 1 балл.

Кроссворд



По вертикали:

1. Свойство информации быть доступной только ограниченному кругу пользователей.

По горизонтали:

1. Раздел прикладной математики, изучающей методы преобразования информации в целях сокрытия ее содержания.
2. Процесс наложения по определенному закону гаммы шифра на открытые данные.
3. Процесс маскировки сообщения способом, позволяющим скрыть ее суть.
4. Совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных.
5. Раздел прикладной математики, изучающий методы, алгоритмы, программные и аппаратные средства анализа криптосистем с целью извлечения конфиденциальных данных.
6. Нарушение конфиденциальности шифртекста, достигнутое методами криптоанализа.
7. Субъект, посылающий сообщение.

8. Исходные открытые параметры алгоритма криптографического преобразования.

9. Зашифрованное сообщение.

10. Реализация угрозы безопасности для криптосистемы.

11. Сменный элемент шифра, применяемый для зашифрования отдельного сообщения.

12. Процесс преобразования шифртекста в открытый текст.

13. Система, реализованная программно, аппаратно или программно-аппаратно и осуществляющая криптографические преобразования информации.

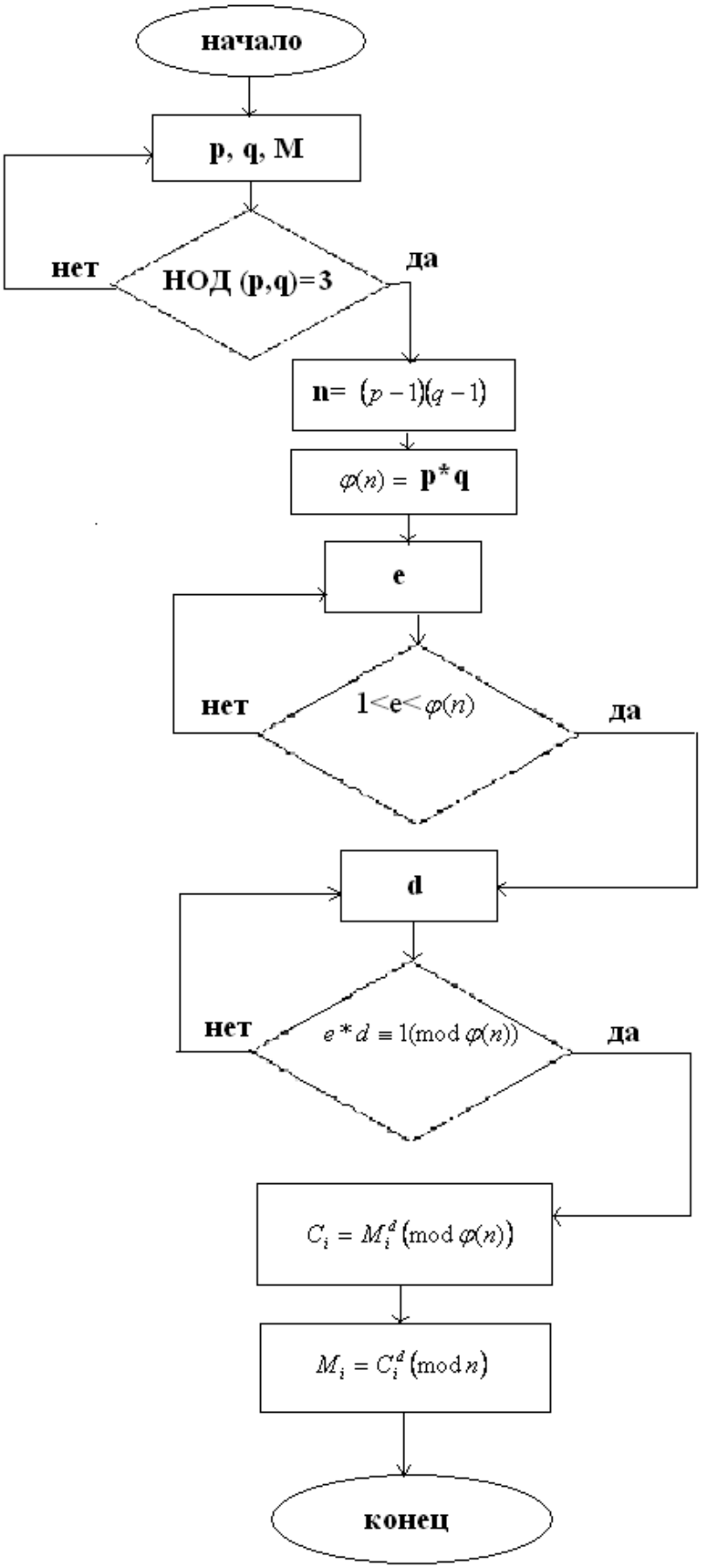
14. Способность шифра противостоять попыткам его расшифрования.

15. Защита получателя от навязывания ложной информации.

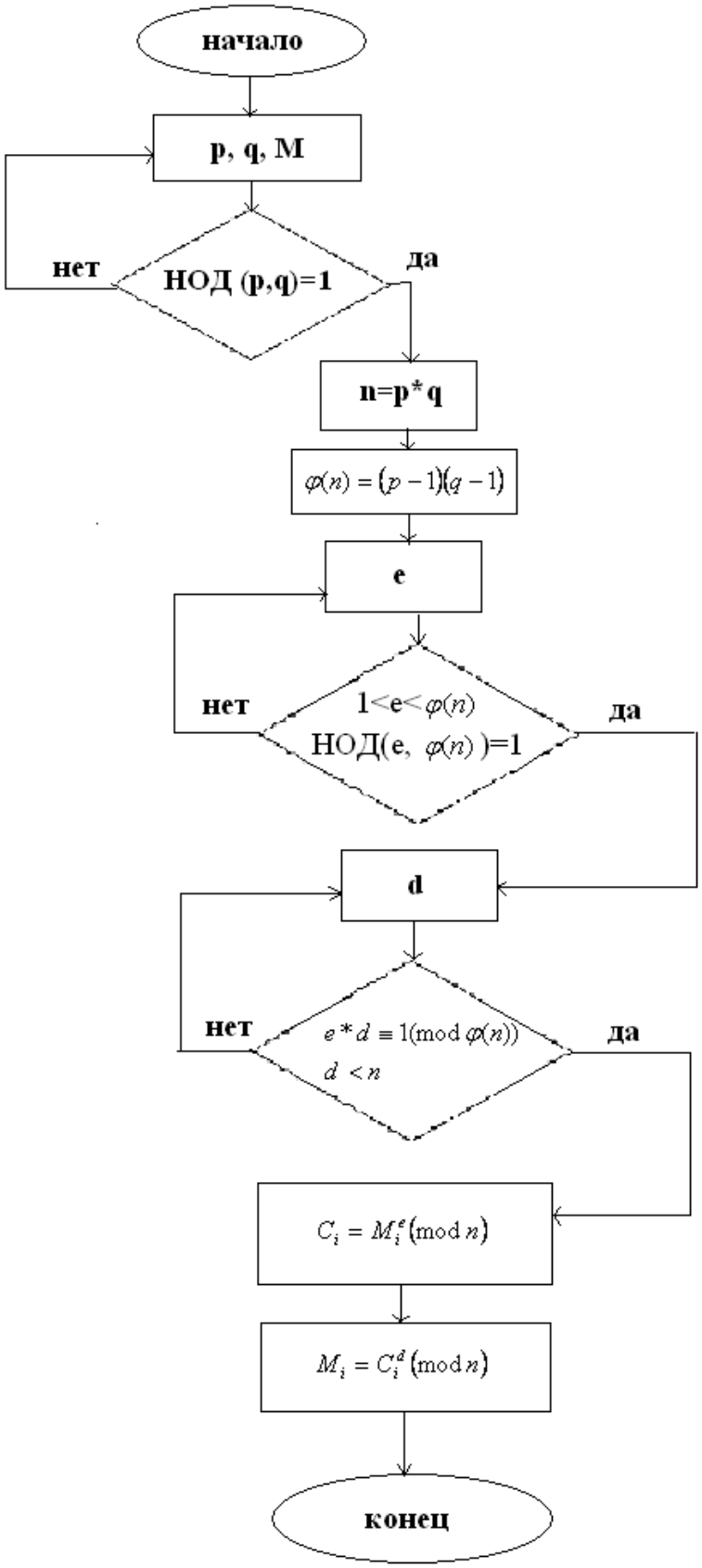
III. Закрепление пройденного материала

1. Студентам предлагается найти ошибки в методике зашифрования и расшифрования данных (представленной в виде блок-схемы) криптоалгоритмом шифрования данных RSA.

Блок-схема зашифрования и расшифрования данных криптоалгоритмом шифрования данных RSA (с ошибками)



Блок-схема зашифрования и расшифрования данных криптоалгоритмом шифрования данных RSA (без ошибок)



2. Проверить ЭЦП алгоритма шифрования RSA. Задание оценивается по пятибалльной шкале, взависимости от полноты и правильности выполнения.

Задание для 1 команды:

$n = 33$

$e = 3$

$S = 22$

$H_0 = 6$

Сообщение: 11, 12, 31, 24 (ключ)

Ответ: ЭЦП достоверна

Задание для 2 команды:

$n = 33$

$e = 3$

$S = 3$

$H_0 = 6$

Сообщение: 25, 9, 21, 17 (шифр)

Ответ: ЭЦП достоверна

3.Студентам предлагается расшифровать слова, с заданными параметрами шифрования используя алгоритм шифрования Эль Гамаля. Задание оценивается по пятибалльной шкале, взависимости от полноты и правильности выполнения.

Задание для 1 команды:

$a = 6$

$x = 1$

$p = 11$

Сообщение: 8, 10, 9, 11

Ответ: диск

Задание для 2 команды:

$a = 6$

$x = 1$

$p = 11$

Сообщение: 1, 6, 5, 4

Ответ: байт

IV. Подведение итогов.

Выставление оценок.

V. Домашнее задание.

Продумать способы формирования ЭЦП криптоалгоритма Эль Гамаля.

Список используемой литературы

1. Р.Р. Хамидуллин, И.А. Бригаднов, А.В. Морозов «Методы и средства защиты компьютерной информации»: учеб. Пособие. – СПб.:СЗТУ, 2005
2. Электронный учебник «Иллюстрированный самоучитель по защите информации»
3. Электронный учебник «Иллюстрированный самоучитель по защите в Интернет»
4. Электронный учебник «Иллюстрированный самоучитель по разработке безопасности»
5. Электронный учебник «Иллюстрированный самоучитель по теории операционных систем»