Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт информационных и электронных систем
Кафедра прикладной математики и информатики

УТВЕРЖДАЮ
Директор ИЭИС
С.И. Эминов
«___» _____ 2017г.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебный модуль по направлению подготовки
01.03.02 – прикладная математика и информатика

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Принято на заседании
Ученого совета ИЭИС
Протокол №29 от 23.03 2017 г.
зам. директора института
_____ С.И. ЭМИНОВ

Разработал
Доцент кафедры ПМИ
_____ Т.В. Жгун
«20» февраля 2017 г.

Принято на заседании кафедры ПМИ
Протокол №7 от 01.03 2017 г.
Заведующий кафедрой ПМИ
_____ А.В. Колногоров

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине (модулю) Методы защиты информации
для направления подготовки
01.03.02 – Прикладная математика и информатика

Модуль, раздел (в соответствии с РП)	ФОС		
	Вид оценочного средства	Количество вариантов заданий	Контролируемые компетенции (или их части)
1.2 Традиционное шифрование: классические методы.	ДЗ №1	25	ОПК2, ОПК4, ПК5,
1.2 Традиционное шифрование: классические методы	собеседование (защита ЛР№1)	25	ОПК2, ОПК4, ПК5,
1.3Алгоритмы симметричного шифрования	собеседование (защита ЛР№2)	25	ОПК2, ОПК4, ПК5,
1,4Асимметричные системы шифрования	ДЗ №2	25	ОПК2, ОПК4, ПК5,
1,4Асимметричные системы шифрования	собеседование (защита ЛР№3	25	ОПК2, ОПК4, ПК5,
1,4Асимметричные системы шифрования	собеседование (защита ЛР№4	25	ОПК2, ОПК4, ПК5,
1.5. Хэш-функции и аутентификация 1.6 Цифровая подпись	собеседование (защита ЛР№5)	25	ОПК2, ОПК4, ПК5,
Экзамен		25	ОПК2, ОПК4, ПК5,

Характеристика оценочного средства № 1

ДОМАШНЕЕ ЗАДАНИЕ № 1

2.1 Общие сведения об оценочном средстве

Домашнее задание (ДЗ1) является одним из средств текущего контроля в освоении учебного модуля «Методы защиты информации». Домашнее задание является средством проверки и оценки знаний студентов по освоенному материалу, а также умений применять полученные знания для решения поставленных задач.

В рамках освоения УМ «Методы защиты информации» ДЗ1 выдаётся индивидуально каждому студенту. Студенты выполняют задания поэтапно в письменном виде и/или с помощью компьютера. В случае неудовлетворительной оценки студенту даётся неделя на исправление ошибок.

Во время проверки выполненной работы оценивается способность студента умение применять полученные в ходе лекционных и практических занятий знания и умения. Максимальное количество баллов, которые может получить студент за домашнее задание, равно 35 баллам.

2.2 Параметры оценки ДЗ1

Условия оценки домашнего задания	
Предлагаемое количество задач	4
Последовательность выборки задач	вариант, соответствующий списочному номеру студента в группе
Критерии оценки:	
20 баллов максимум	полнота решения
15 балла максимум	логичность изложения решения
5 балл максимум	аккуратность
«удовлетворительно»	21 – 29 баллов – испытывает трудности при выполнении заданий
«хорошо»	30– 35 баллов – допускает неточности при выполнении заданий
«отлично»	36 – 40 баллов – демонстрирует четкое и безошибочное выполнение заданий

Характеристика оценочного средства №2

ДОМАШНЕЕ ЗАДАНИЕ № 2

4.1 Общие сведения об оценочном средстве

Домашнее задание (ДЗ2) является одним из средств текущего контроля в освоении учебного модуля «Методы защиты информации». Домашнее задание является средством проверки и оценки знаний студентов по освоенному материалу, а также умений применять полученные знания для решения поставленных задач.

В рамках освоения УМ «Методы защиты информации» ДЗ2 выдаётся индивидуально каждому студенту. Студенты выполняют задания в письменном виде к 10 неделе семестра. В случае неудовлетворительной оценки студенту даётся неделя на исправление ошибок.

Во время проверки выполненной работы оценивается способность студента найти правильный ответ на поставленный вопрос, умение применять полученные в ходе лекций и практик знания и умения. Максимальное количество баллов, которые может получить студент за домашнее задание, равно 35 баллам.

4.2 Параметры оценки ДЗ2

Условия оценки домашнего задания	
Предлагаемое количество задач	4
Последовательность выборки задач	вариант, соответствующий списочному номеру студента в группе
Критерии оценки:	
20 баллов максимум	полнота решения
15 балла максимум	логичность изложения решения
5 балл максимум	аккуратность
«удовлетворительно»	21 – 29 баллов – испытывает трудности при выполнении заданий
«хорошо»	30– 35 баллов – допускает неточности при выполнении заданий
«отлично»	36 – 40 баллов – демонстрирует четкое и безошибочное выполнение заданий

Характеристика оценочного средства №3

СОБЕСЕДОВАНИЕ В СООТВЕТСТВИИ С ПАСПОРТОМ ФОС

3.1 Общие сведения об оценочном средстве

Собеседование является одним из средств текущего контроля в освоении учебного модуля «Методы защиты информации». Собеседование используется для проверки и оценивания знаний, умений и навыков студентов после выполнения каждой лабораторной работы.

Контрольные собеседования проводятся в форме индивидуального устного опроса студентов. Вопросы ставит преподаватель по своему усмотрению, охватывая все основное содержание тем, выносимых на контрольное собеседование. Во время проведения собеседования оценивается способность студента правильно сформулировать ответ, умение выражать свою точку зрения по данному вопросу, ориентироваться в терминологии и применять полученные в ходе лекций, практических и лабораторных работ знания. Список возможных вопросов для собеседования по лабораторным работам находится в Приложении Е к рабочей программе модуля

3.2 Параметры проведения собеседования

Таблица 2 – Параметры оценочного средства (собеседование по лабораторной работе)

Предел длительности контроля	не более 20 мин на одну работу
Предлагаемое количество вопросов	по 4 вопроса на занятие
Критерии оценки:	Максимально 24балла
«5» 21-24 баллов	ЛР правильно выполнена, на защите демонстрирует полноту и аргументированность ответов
«4» 17-20балла	ЛР правильно выполнена, на защите не все ответы достаточно аргументированы.
«3» 12-16 балла	ЛР правильно выполнена, на защите испытывает затруднения при ответе на некоторые вопросы.

Критерии оценивания лабораторной работы:

- правильность выполнения ЛР – 5 балла максимум;
- уверенное владение терминологией на защите – 5 балла максимум;
- полнота ответа на защите – 5 балла максимум;
- аргументированность ответа – 5 балла максимум;
- правильность оформления отчета – 4 балл.

Характеристика оценочного средства №4

Экзамен

6.1 Общие сведения об оценочном средстве

Экзамен т является видом итогового контроля и оценки знаний, умений и навыков, уровня сформированности компетенций студента при освоении учебного УМ «Методы защиты информации».

Задания билетов достаточно полно отображают планируемую содержательную структуру изучаемого и контролируемого материала, дают возможность ранжировать студентов по уровням подготовленности: чем меньше пробелов в ответах обучаемого, тем лучше структура его знаний; чем выше его балл, тем выше качество его подготовленности.

Билеты формируется индивидуально для каждого студента. Пример билета в Приложении Е к рабочей программе.

6.3 Параметры оценки теста

Таблица 6 – Параметры оценочного средства (экзамен)

Предел длительности контроля	не более 60 минут на ответ
Предлагаемое количество вопросов	3
Критерии оценки:	
«5-если	45-50 – Демонстрирует всестороннее и глубокое знание материала модуля
«4», если	35-44 – Допускает неточности при демонстрации знаний
«3», если	25-34 – Испытывает трудности при демонстрации знаний

– Критерии оценивания экзамена:

- уверенное владение терминологией – 10 баллов максимум;
- глубина знаний по теме вопроса – 10 баллов максимум;
- полнота ответа – 10 баллов максимум;
- логическая связность – 10 баллов максимум;
- аргументированность ответа – 10 балла максимум

Приложение 1

Банк заданий для оценочного средства №2 «Экзамен»

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1
по курсу Методы защиты информации

1.Найти порядок элемента x в поле *GF(27),* построенному по модулю многочлена $p(x)=x^3+x^2+1$, вычислить в этом поле $\frac{6-8*4}{45-85}*5$.

2.Выполнить 2 итерации ГОСТ. P = 0 0 0 . . . 0 1 1 K = 1 1 0 . . . 0 0 0. S-блоки известны. Считаем, что на каждом шаге S- матрицы одинаковы и последние 4 строки совпадают с 4 первыми.

$$S=\begin{pmatrix}14&13&2&11&8&3&10&6&12&5&9&0\\0&13&7&14&2&11&4&6&12&15&9&3\\4&11&13&14&8&6&2&1&10&15&9&12\\1&15&8&2&4&9&12&7&5&10&3&6\end{pmatrix}$$

3. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2
по курсу Методы защиты информации

1.Построить поле $GF(2^4)$, используя

- неприводимый многочлен 4 степени над $GF(2)$,
- неприводимый многочлен 2 степени $GF(4)$.

2.Выполнить 2 итерации сети Фейстеля. На входе P = 3 4 =0 1 1 1 0 0 –6 бит. Расширение до 8 бит (P1). Ключ на входе 10 бит, после сжатия (P2) – 8 бит. Нелинейное преобразование задается матрицами S0 и S1. K = 00000000101, P1 = (1234665), P2 = (1234678)

$$S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&2&1&0\end{pmatrix}\quad S1=\begin{pmatrix}1&0&2&3\\2&0&1&3\\3&0&1&2\\2&1&0&3\end{pmatrix}$$

3.Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3
по курсу Методы защиты информации

1. .Построить поле $GF(9)$. Найти порядки элементов в этом поле.

2. Выработка ключа в S –DES. 

3. Хэш-функции и их применение. Хеш-функция MD2

.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 4
по курсу Методы защиты информации

1. Решить в $GF(3^2)$ систему $\begin{cases} 2x+2y=3 \\ x+2y=2 \end{cases}$

2. Зашифровать сообщение, используя AES - упрощенный метод. Открытый текст и ключ – 4*4 бита. 

.3. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5
по курсу Методы защиты информации

1. . Решить в $GF\left(2^3\right)$ систему $\begin{cases} 2x+y=3 \\ x+2y=1 \end{cases}$

2. Выработать секретный ключ по алгоритму Диффи-Хеллмана с абонентом В, который задумал секретное число 3. Открытый ключ (17, q), где q – примитивный элемент поля GF(17).

3. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 6
по курсу Методы защиты информации

1. Вычислить дискретные логарифмы элементов поля GF(7).

2. Зашифровать сообщение с помощью алгоритма RSA. Открытый ключ отправителя (667, 17). M=2.

3. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 7
по курсу Методы защиты информации

1. Построить поле $GF(2^5)$, вычислить в этом поле $\frac{5-7*4}{51-35}$*4-2.

2. Подписать сообщение с помощью алгоритма RSA. Открытый ключ отправителя (377, 55), открытый ключ получателя (551, 13). M=4.

3. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 8
по курсу Методы защиты информации

1. . Решить диофантовы уравнения

$$\begin{cases} 13x-4y=1 \\ 5x-17y=1 \end{cases}$$

2. Подписать сообщение с помощью алгоритма Эль-Гамаля.. P=23, q –примитивный элемент поля GF(23). Известна h(M)=m=6. M=11.

3. Теория сложности вычислений. Классификация алгоритмов

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 9
по курсу Методы защиты информации

1. . Двумя способами решить сравнения

$$3x \equiv 1 \bmod 4$$
$$5x \equiv 1 \bmod 7$$

2. Найти порядок элемента x в поле *GF(27),* построенному по модулю многочлена $p(x) = x^3 + x^2 + 2$, вычислить в этом поле $\frac{6-8*4}{45-75} * 5$.

3. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 10
по курсу Методы защиты информации

1.Построить поле $GF(2^4)$, используя

- неприводимый многочлен 4 степени над $GF(2)$,
- неприводимый многочлен 2 степени $GF(4)$.

2. . Выполнить 2 итерации ГОСТ. P = 0 0 0 . . . 0 1 1.K = 1 1 0 . . . 0 0 0.
S-блоки известны. Считаем, что на каждом шаге S- матрицы одинаковы и последние 4 строки совпадают с 4 первыми.

$$S = \begin{pmatrix} 14 & 11 & 12 & 15 & 8 & 3 & 10 & 6 & 13 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 11 & 14 & 8 & 13 & 6 & 2 & 1 & 12 & 7 & 10 & 1 & 5 & 15 & 9 & 3 \\ 15 & 5 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{pmatrix}$$

3. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.

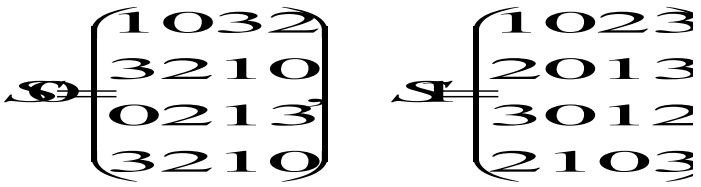
Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 11
по курсу Методы защиты информации

1. Решить в $GF(3^2)$ систему $\begin{cases} 2x+y=3 \\ x+2y=2 \end{cases}$

2.Выполнить 2 итерации сети Фейстеля. На входе P = 3 4 =0 1 1 1 0 0 –6 бит. Расширение до 8 бит (P1). Ключ на входе 10 бит, после сжатия (P2) – 8 бит. K = 00000000101, P1 = (1 2 3 4 6 1 6), P2 = (1 2 3 4 10 9 8 7). Нелинейное преобразование задаётся матрицами



4. Криптосистема Эль-Гамаля.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 12
по курсу Методы защиты информации

1. Решить в $GF(2^3)$ систему $\begin{cases} 2x+y=3 \\ x+2y=2 \end{cases}$

2. Выработка ключа в S –DES.  .

3. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.
4.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 13
по курсу Методы защиты информации

1.Найти порядок элемента x в поле *GF(27),* построенному по модулю многочлена $p(x)=x^3+x^2+1$, вычислить в этом поле $\frac{6-8*4}{45-85}*5$.

2.Выполнить 2 итерации ГОСТ. P = 0 0 0 . . . 0 1 1 K = 1 1 0 . . . 0 0 0. S-блоки известны. Считаем, что на каждом шаге S- матрицы одинаковы и последние 4 строки совпадают с 4 первыми.

$$S=\begin{pmatrix} 14 & 11 & 12 & 13 & 8 & 3 & 10 & 6 & 9 & 15 & 0 & 7 & 4 & 2 & 5 & 1 \\ 0 & 13 & 7 & 14 & 4 & 12 & 2 & 11 & 8 & 6 & 10 & 1 & 9 & 15 & 3 & 5 \\ 4 & 11 & 1 & 8 & 14 & 6 & 2 & 13 & 10 & 12 & 15 & 3 & 7 & 5 & 9 & 0 \\ 1 & 15 & 8 & 2 & 4 & 9 & 12 & 7 & 5 & 13 & 3 & 11 & 14 & 10 & 6 & 0 \end{pmatrix}$$

3. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №14
по курсу Методы защиты информации

1.Построить поле $GF(2^4)$, используя

- неприводимый многочлен 4 степени над $GF(2)$,
- неприводимый многочлен 2 степени $GF(4)$.

2.Выполнить 2 итерации сети Фейстеля. На входе P = 3 4 =0 1 1 1 0 0 –6 бит. Расширение до 8 бит (P1). Ключ на входе 10 бит, после сжатия (P2) – 8 бит. Нелинейное преобразование задается матрицами S0 и S1. K = 00000000101, P1 = (1234665), P2 = (1234678)

$$S0=\begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix} \quad S1=\begin{pmatrix} 1 & 0 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

3.Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 15
по курсу Методы защиты информации

1. .Построить поле $GF(9)$. Найти порядки элементов в этом поле.

2. Выработка ключа в S –DES. 

3. Хэш-функции и их применение. Хеш-функция MD2

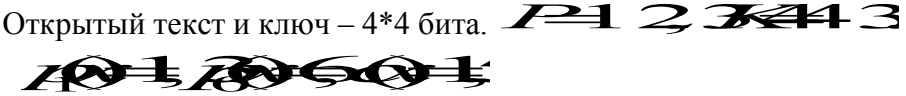
.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 16
по курсу Методы защиты информации

1. Решить в $GF(3^2)$ систему $\begin{cases} 2x+2y=3 \\ x+2y=2 \end{cases}$

2. Зашифровать сообщение, используя AES - упрощенный метод.
Открытый текст и ключ – 4*4 бита. 

.3. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 17
по курсу Методы защиты информации

1. . Решить в $GF\left(2^3\right)$ систему $\begin{cases} 2x+y=3 \\ x+2y=1 \end{cases}$

2. Выработать секретный ключ по алгоритму Диффи-Хеллмана с абонентом В, который задумал секретное число 3. Открытый ключ (17, q), где q – примитивный элемент поля GF(17).

3. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 19
по курсу Методы защиты информации

1. Вычислить дискретные логарифмы элементов поля GF(7).

2. Зашифровать сообщение с помощью алгоритма RSA. Открытый ключ отправителя (667, 17). M=2.

3. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 20
по курсу Методы защиты информации

1. Построить поле $GF\left(2^5\right)$, вычислить в этом поле $\frac{5-7*4}{51-35}$ *4-2.

2. Подписать сообщение с помощью алгоритма RSA. Открытый ключ отправителя (377, 55), открытый ключ получателя (551, 13). M=4.

3. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 21
по курсу Методы защиты информации

1. . Решить диофантовы уравнения

$$\begin{cases} 13x-4y=1 \\ 5x-17y=1 \end{cases}$$

2. Подписать сообщение с помощью алгоритма Эль-Гамаля.. P=23, q –примитивный элемент поля GF(23). Известна h(M)=m=6. M=11.

3. Теория сложности вычислений. Классификация алгоритмов

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 22
по курсу Методы защиты информации

1. . Двумя способами решить сравнения

$$3x \equiv 1 \bmod 4$$
$$59x \equiv 1 \bmod 7$$

2. Найти порядок элемента x в поле $GF(27)$, построенному по модулю многочлена $p(x) = x^3 + x^2 + 2$, вычислить в этом поле $\frac{6-8*4}{45-75} * 5$.

3. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 23
по курсу Методы защиты информации

1.Построить поле $GF(2^4)$, используя

- неприводимый многочлен 4 степени над $GF(2)$,
- неприводимый многочлен 2 степени $GF(4)$.

2. Выполнить 2 итерации ГОСТ. P = 0 0 0 . . . 0 1 1.K = 1 1 0 . . . 0 0 0.
S-блоки известны. Считаем, что на каждом шаге S- матрицы одинаковы и последние 4 строки совпадают с 4 первыми.

$$S = \begin{pmatrix} 14 & 11 & 12 & 15 & 8 & 3 & 10 & 6 & 13 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 11 & 14 & 8 & 13 & 6 & 2 & 1 & 12 & 7 & 10 & 1 & 5 & 15 & 9 & 3 \\ 1 & 15 & 13 & 8 & 10 & 3 & 7 & 4 & 12 & 5 & 6 & 11 & 0 & 14 & 9 & 2 \end{pmatrix}$$

3 Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.

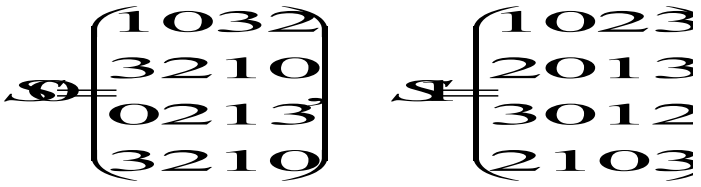
Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 24
по курсу Методы защиты информации

1. Решить в $GF(3^2)$ систему $\begin{cases} 2x+y=3 \\ x+2y=2 \end{cases}$

2.Выполнить 2 итерации сети Фейстеля. На входе P = 3 4 =0 1 1 1 0 0 –6 бит. Расширение до 8 бит (P1). Ключ на входе 10 бит, после сжатия (P2) – 8 бит. K = 00000000101, P1 = (1 2 3 4 6 1 6), P2 = (1 2 3 4 10 9 8 7). Нелинейное преобразование задаётся матрицами



5. Криптосистема Эль-Гамаля.

Зав. кафедрой ПМИ А.В. Колногоров

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 25
по курсу Методы защиты информации

1. Решить в $GF(2^3)$ систему $\begin{cases} 2x+y=3 \\ x+2y=2 \end{cases}$

2. Выработка ключа в S –DES.  .

3. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.

Зав. кафедрой ПМИ А.В. Колногоров