МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 1

1. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.
2. Группы, кольца, поля. Классы вычетов по модулю.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 2

1. Модулярные шифры. Шифры Вижинера. Автоматический и бегущий выбор ключа.
2. Первообразные корни и их свойства. Дискретные логарифмы.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 3

1. Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота.
2. Греко-китайская теорема об остатках и ее применения.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 4

1. Шифр Файстеля. Структура шифра. Алгоритм дешифрования. Диффузия и конфузия.
2. Малая теорема Ферма. Теорема Эйлера.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 5

1. DES: алгоритмы шифрования и дешифрования. Надежность. Криптоанализ.
2. Возведение в степень с использованием метода последовательного возведения в квадрат.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 6

1. Режимы работы DES. Сцепление блоков.
2. Теорема о корнях $x^2 = 1 \mod p$ для нечетного простого p. Рандомизация проверки простоты (WITNESS). Числа Кармайкла.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 7

1. Тройной DES.
2. Схема обмена ключами Диффи-Хеллмана с использованием дискретных логарифмов.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 8

1. Двойной DES.
2. Схема обмена ключами Эль Гамаля с использованием дискретных логарифмов.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 9

1. Оценка криптостойкости с применением теории информации. Совершенно криптостойкие системы.
2. Протокол взаимной аутентификации.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 10

1. Криптосистемы, базирующиеся на задаче о рюкзаке.
2. Алгоритм Евклида. Расширенный алгоритм Евклида для вычисления мультипликативного обратного.
3. Задача.

Зав. кафедрой _____

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
Школа _____
ООП _____
шифр, название направления подготовки (специальности)
Дисциплина _____
Форма обучения _____
Семестр осенний 2011 - 2012 учебного года
Реализующая кафедра _____

Экзаменационный билет № 11

1. Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
2. RSA: основные элементы криптосистемы. Шифрование и дешифрование.
3. Задача.

Зав. кафедрой _____

Задачи

1. Используется система Хилла с матрицей 2×2. Наиболее встречающиеся в криптотексте диграммы RH и NI (в исходном тексте TH и HE). Восстановить матрицу.

2. Какова разница между криптопреобразованиями Плейфейера, реализуемыми с помощью матрицы 5×5 и 3×9 (кроме разницы в длине алфавита)?

3. M зашифровано с помощью RSA (n, e - открытый ключ). Известно, что M имеет с n общий делитель. Как можно использовать этот факт для криптоанализа (определения закрытого ключа d)? Какова вероятность того, что $\gcd(M, n) \neq 1$ при случайном выборе M, если p и q имеют k бит в двоичном представлении?

4. Дана схема

   - случайно выбирается E;
   - случайно выбираются простые числа P и Q: $(P-1)(Q-1)-1$ делится на E;
   - $N = PQ$;
   - $D = [(P-1)(Q-1)(E-1)+1]/E$.

   P, Q, E, D используются так же, как p, q, e, d в RSA. Является ли эта схема эквивалентной RSA?

5. Пусть $n = pqr$ (p, q, r – простые числа, $ed = 1 \mod \varphi(n)$). Каковы преимущества и недостатки аналогичной RSA системы по сравнению с оригинальной?

6. Пусть p, q, n, e – параметры RSA (p, q – простые числа, $n = pq$, e - экспонента шифрования). Доказать, что существует ровно $\gcd(p-1, e-1)\gcd(q-1, e-1)$ неподвижных точек M с $\gcd(M, n) = 1$. (Использовать тот факт, что для простого p и $r \in Z$ число элементов $x \in Z_p^*$, для которых $x^r = 1 \mod p$ равно $\gcd(r, p-1)$.)

7. Решить систему, используя греко-китайскую теорему об остатках:

$$x \equiv 2 (\mod 17) \quad (1)$$
$$x \equiv 3 (\mod 9) \quad (2)$$
$$x \equiv 4 (\mod 14) \quad (3)$$

8. Решить систему, используя греко-китайскую теорему об остатках:

$$43x \equiv 9 (\mod 99) \tag{4}$$
$$42x \equiv 31 (\mod 107) \tag{5}$$

9. Решить систему, используя греко-китайскую теорему об остатках:

$$x \equiv 12 (\mod 25) \tag{6}$$
$$x \equiv 19 (\mod 26) \tag{7}$$
$$x \equiv 7 (\mod 27) \tag{8}$$

10. Решить систему:

$$7x \equiv 9 (\mod 11) \tag{9}$$
$$9x \equiv 11 (\mod 7) \tag{10}$$
$$11x \equiv 7 (\mod 9) \tag{11}$$

11. Решить систему:

$$2x \equiv 7 (\mod 5) \tag{12}$$
$$3x \equiv 5 (\mod 8) \tag{13}$$
$$5x \equiv 9 (\mod 12) \tag{14}$$

12. Найти количество решений сравнения $x^n = 1 \mod m$.

13. Найти количество решений сравнения $x^n = -1 \mod m$.

14. Найти наименьшее натуральное число, которое при делении на 3, 4, 5, 6 дает в остатке соответственно 2, 3, 4, 5.

15. Найти все натуральные числа, которые не превосходят 1000 и при делении на 3, 5, 7, 11 дают в остатке соответственно 2, 3, 5, 6.

16. Пусть p, q, n – параметры RSA (p, q – простые числа, $n = pq$). Определим

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

Тогда

$$a^{\lambda(n)} = 1 \mod n, \forall a \in Z_n^*.$$

Как можно эффективно дешифровать $C = M^e \mod n$ с использованием $\lambda(n)$?

17. Известно, что сообщение COFFEE зашифровано с использованием шифра Хилла $c = Km$ в виде M$TXVB. При этом используется алфавит, содержащий 29 символов 0-28 (в исходном тексте A-Z представлены числами 0-25, $ - 26, % - 27, # - 28), и K имеет размерность 2×2. Найти K.

18. Проверить, что 641 делит $2^{2^5} + 1$ (следовательно, $2^{2^n} + 1$ не является простым для всех n).

19. Предположим, что вместо RSA используется схема, при которой $n = pqr$, где p, q, r – большие простые натуральные числа, а экспоненты шифрования и дешифрования удовлетворяют соотношению $ed = 1 \mod \varphi(n)$. Каковы плюсы и минусы по сравнению с традиционной RSA?

20. Пусть $x, y, z \in B^n$, $k_1, k_2 \in K$, $f : K \times B^n \to B^n$, а $\Pi : (B^n)^3 \to (B^n)^3$ и $\Theta : (B^n)^3 \to (B^n)^3$ задаются соотношениями $\Pi(x, y, z) = (x + f(k_1, y), y + f(k_2, y), z)$ и $\Theta(x, y, z) = (y, z, x)$.

    Доказать, что

    - Π^4 – тождественная функция,
    - Π^4 – биекция на $(B^n)^3$,
    - Θ^3 – тождественная функция.

    Для криптосистемы $\Pi_3\Theta\Pi_2\Theta\Pi_1$, где Π_j использует пару ключей $(k_1^{(j)}, k_2^{(j)})$, $j = 1, 2, 3$, найти обратное преобразование.

21. Рассмотрим криптосистему типа DES с 3 раундами, входом (L, R) и выходом (L', R'), ключами K_1, K_2, K_3, где $L, R, L', R', K_0, K_1, K_2 \in B^{32}$:

$$L_1 = L \quad R_1 = L + R + K_0 \tag{15}$$
$$L_2 = L_1 \quad R_2 = L_1 + R_1 + K_1 \tag{16}$$
$$L_3 = L_2 \quad R_3 = L_2 + R_2 + K_2 \tag{17}$$
$$L' = L_3 \quad R' = R_3 \tag{18}$$

    Предположим, что криптоаналитик имеет в своем распоряжении пару исходный текст $M = (L, R)$ и соответствующий ему шифр $C = (L', R')$. Как провести криптоатаку (выписать соотношения, которые позволяют восстановить исходное сообщение $m = (l, r)$ через шифр $c = (l', r')$ с использованием L, R, L', R')?

22. Вычислить корень седьмой степени из 23 в Z_{77}^*, используя функцию Эйлера и метод последовательного возведения в квадрат (соответствующий корень равен $23^{7^{-1} \bmod \varphi(77)} \bmod 77$).

23. Предположим, что Alice и Bob используют для RSA один модуль n, но разные экспоненты шифрования e^A и e^B, где e^A и e^B взаимно простые. Charlie посылает одно и то же сообщение m в виде кодов $c_A = m^{e_A} \bmod n$ для Alice и $c_B = m^{e_B} \bmod n$ для Bob. Предположим, что Eve перехватывает оба кода c_A и c_B. Как Eve может восстановить m?