МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра математики

Составители
Е. А. Николаева
А. В. Чередниченко
Е. В. Гутова

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Методические материалы

Рекомендовано учебно-методической комиссией специальности 10.05.03 Информационная безопасность автоматизированных систем в качестве электронного учебного издания для использования в образовательном процессе

Кемерово 2018

Рецензенты Фадеев Ю. А. – доктор физико-математических наук, профессор кафедры математики ФГБОУ ВО «Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Прокопенко Е. В. – председатель учебно-методической комиссии специальности 10.05.03 Информационная безопасность автоматизированных систем

Николаева Евгения Александровна
Чередниченко Алла Валериевна
Гутова Елена Владимировна
Математические основы криптологии [Электронный ресурс]: методические материалы для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. А. Николаева, А. В. Чередниченко. Е. В. Гутова; КузГТУ. – Электрон. издан. – Кемерово, 2018.

Приведен материал, необходимый для успешного изучения дисциплины.

Назначение издания – помощь обучающимся в получении знаний по дисциплине «Математические основы криптологии» и организовать самостоятельную работу.

Предлагаемые методические указания предназначены для организации практических занятий и самостоятельной работы обучающихся очной формы обучения по курсу «Математические основы криптологии».

Цель работы – помочь студентам при освоении дисциплины «Математические основы криптологии», организация практических занятий и самостоятельной работы.

Практические занятия разбиты по темам согласно рабочей программе, приведены задания для решения на практических занятиях и задания для самостоятельной работы.

Практические занятия и самостоятельная работа студентов очной формы обучения

Раздел 1. Основные сведения о целых числах. *1.1 Деление с остатком, алгоритм Евклида, множители Безу. 1.2 Сравнение по модулю, кольца вычетов. 1.3 Теорема Эйлера. 1.4 Китайская теорема об остатках.*

Практическое занятие:

1. Дайте определение неполного частного и остатка от деления целого числа x на целое число y.

2. Разделить с остатком

а) 115 на 27;

б) 115 на 23;

в) 7 на 8.

3. Дайте определение наибольшего общего делителя (НОД) целых чисел x и y.

4. С помощью алгоритма Евклида найти наибольший общий делитель чисел 3558 и 1856.

5. Дайте определение взаимно простых целых чисел.

6. Являются ли числа 315 и 78 взаимно простыми?

7. Сформулируйте теорему о линейном представлении НОД.

8. Найти какие-либо множители Безу для чисел 81 и 26.

9. Дайте определение отношения сравнимости целых чисел по модулю n.

10. Дайте определение класса вычетов по модулю натурального числа n. Как определяются операции сложения и умножения для классов вычетов?

11. Найти

а) $13+17 \pmod{20}$;

б) $9 \cdot 5 \pmod{14}$;

в) $-3 \pmod{5}$.

12. Дайте определение кольца вычетов по модулю n.

13. Постройте таблицы умножения и сложения в кольце $Z4$. Привести пример ненулевых элементов x, y кольца $Z4$, для которых $xy=0$.

14. Какие элементы кольца Zп называются обратимыми? Какие элементы кольца Zп называются делителями нуля? Может ли обратимый элемент кольца Zп быть делителем нуля? Может ли элемент кольца Zп не быть ни обратимым, ни делителем нуля?

15. Сформулируйте критерий обратимости элемента кольца классов вычетов по модулю п.

16. Найти

а) 3-1 (mod 5);

б) 9-1 (mod 14);

в) 1-1 (mod 118);

17. Решите сравнение

а) 7x = 11 (mod 25);

б) 9x = 3 (mod 10);

в) 6x + 2 = 3 (mod 7).

18. Дайте определение группы.

19. Докажите, что множество обратимых элементов кольца Zп является группой по умножению.

20. Дайте определение функции Эйлера φ(п) Как связано значение φ(п) и группа обратимых элементов кольца Zп?

21. Дайте определение простого числа. Сформулируйте теорему о разложении натурального числа в произведение простых чисел.

22. Разложите на простые множители числа

а) 2100;

б) 429;

в) 2048.

23. Сформулируйте теорему о вычислении функции Эйлера.

24. Найти

а) φ(210);

б) φ(4500);

в) число обратимых элементов в кольце Z2197;

25. Сформулируйте малую теорему Ферма.

26. Сформулируйте теорему Эйлера, обобщающую малую теорему Ферма.

27. Используя, если надо. теорему Эйлера и алгоритм быстрого возведения в степень, найти

а) 3198 (mod 47);

б) 32101 (mod 45);

в) 2199 (mod 38).

28. Зная значения функции φ(п), найти разложения числа п в произведение простых чисел, если известно, что п имеет ровно два простых делителя

а) п = 115937, φ(п) = 115140;

б) п = 30749, φ(п) = 30336.

29. Какие кольца Zп называются полными? Для каких чисел п кольцо Zп является полем?

30. Является ли полем кольцо

а) Z127;

б) Z217;

в) Z111;

г) Z14532.

31. Сформулируйте китайскую теорему об остатках.

32. Решить систему уравнений

$$\begin{cases} x = 3\ (mod\ 8) \\ x = 4\ (mod\ 5) \\ x = 2\ (mod\ 9) \end{cases}$$

Самостоятельная работа:

1. Разделить с остатком

а) –31 на 10;

б) 14 на –5;

в) –18 на –4.

2. С помощью алгоритма Евклида найти наибольший общий делитель чисел 4158 и 1056.

3. Являются ли числа 1315 и 178 взаимно простыми?

4. Найти какие-либо множители Безу для чисел 111 и 26.

5. Найти

а) 4·(6 + 8) + 3·7 (mod 10);

б) 4·9 –5·8 (mod 11);

в) 35 (mod 5);

г) 1725 (mod 18)

6. Постройте таблицы умножения и сложения в кольце Z4. Привести пример ненулевых элементов x, y кольца Z4, для которых x + y = 0.

7. Постройте таблицы умножения и сложения в кольце Z5. Убедиться, что для каждого ненулевого элемента x кольца Z5, существует элемент y, для которого x+y=1.

8. Найти

а) $3 \cdot 4-1 \pmod 7$;

б) $(-3)-1 \pmod 7$;

в) $6-2 \pmod{11}$;

г) $3-3 \pmod 8$

9. Решите сравнение

а) $6x + 2 = 3 \pmod 9$;

б) $6x + 2 = 4 \pmod 9$;

в) $6x + 1 = 4 \pmod 9$

10. Разложите на простые множители числа

а) 2200;

б) 1429;

в) 2248.

11. Найти

а) $\varphi(250)$;

б) $\varphi(500)$;

в) число обратимых элементов в кольце Z2297;

г) $\varphi(p)$, p – простое число;

д) $\varphi(p^n)$, p – простое число, n – натуральное число;

е) $\varphi(p \cdot q)$, p, q – простые числа.

12. Используя, если надо, теорему Эйлера и алгоритм быстрого возведения в степень, найти

а) $3^{198} \pmod 7$;

б) $32^{101} \pmod 4$;

в) $2^{199} \pmod 8$

13. Зная значения функции $\varphi(n)$, найти разложения числа n в произведение простых чисел, если известно, что n имеет ровно два простых делителя

а) $n = 115937$, $\varphi(n) = 115140$;

б) $n = 30749$, $\varphi(n) = 30336$.

14. Является ли полем кольцо

а) Z111;

б) Z14532.

15. Решить систему уравнений

$$\begin{cases} x = 4\ (mod\ 6) \\ x = 4\ (mod\ 49) \\ x = 5\ (mod\ 11) \end{cases}.$$

Раздел 2. Криптосистемы с закрытым ключом. *2.1 Простые подстановочные шифры. 2.2 Периодические шифры. 2.3 Шифр Хилла.*

Практическое занятие:

1. Дайте определение ключа подстановочного шифра.
2. Дайте определение модульного шифра.
3. Зашифруйте слово STUDENT с помощью модулярного шифра f: Z26→Z26; f(x) = 3x+1.
4. Дайте определение периодичного подстановочного шифра с периодом p.
5. Дайте определение периодичного шифра Вижинера.
6. С помощью шифра Вижинера с ключевым словом VIGENERE зашифруйте слово GRYPTOGRAPHY.
7. Дайте определение периодичного шифра Хилла.
8. Дайте определение инволютивной матрицы.
9. Проверьте, что матрица $\begin{pmatrix} 2 & 7 \\ 7 & 24 \end{pmatrix}$ инволютивна над Z26.
10. В криптосистеме Хилла с инволютивной над Z26 матрицей $\begin{pmatrix} 2 & 7 \\ 7 & 24 \end{pmatrix}$ зашифруйте слово STUDENTS. Осуществите проверку, расшифровав полученное сообщение.

Самостоятельная работа:

1. Зашифруйте слово MATHEMATICS с помощью модулярного шифра f: Z26→Z26; f(x) = 3x-4.
2. Зашифруйте слово TABLE с помощью модулярного шифра f: Z26→Z26; f(x) = 2x+6.
3. Зашифруйте слово CRYPTOLOGY с помощью модулярного шифра f: Z26→Z26; f(x) = 3x-4.
4. С помощью шифра Вижинера с ключевым словом CIPHER зашифруйте слово COMPUTER.
5. С помощью шифра Вижинера с ключевым словом WATERMELON зашифруйте слово LOCOMOTIVE.

6. Проверьте, что матрица $\begin{pmatrix} 8 & 3 \\ 3 & 25 \end{pmatrix}$ инволютивна над Z26.

7. В криптосистеме Хилла с инволютивной над Z26 матрицей $\begin{pmatrix} 8 & 3 \\ 3 & 25 \end{pmatrix}$ зашифруйте слово STUDENT.

Раздел 3. Криптосистемы с открытым ключом. *3.1 Элементы теории алгоритмов. 3.2 Криптосистема RSA. 3.3 Криптосистема электронной подписи по протоколу RSA.*

Практическое занятие:

1. Какие алгоритмы называются полиномиальными? Какие алгоритмы называются экспоненциальными? Что такое односторонняя функция? Что такое односторонняя функция с секретом? Как с помощью односторонней функции можно построить криптосистему с открытым ключом?

2. Сформулируйте последовательность действий при шифровании цифрового сообщения в криптосистеме RSA.

3. Сформулируйте последовательность действий при расшифровании цифрового сообщения в криптосистеме RSA.

4. Что называется открытым ключом пользователя в криптосистеме RSA?

5. Что называется закрытым ключом пользователя в криптосистеме RSA?

6. Вычислите закрытый ключ криптосистемы RSA с параметрами p = 47, q = 83, e = 163. Зашифруйте с помощью полученной системы сообщение «123». Выполните проверку, расшифровав закодированное сообщение.

7. Вычислите закрытый ключ криптосистемы RSA с параметрами p = 53, q = 79, e = 97. Зашифруйте с помощью полученной системы сообщение «123». Выполните проверку, расшифровав закодированное сообщение.

8. Опишите последовательность формирования криптосистемы электронной подписи по протоколу RSA.

9. Опишите протокол RSA формирования и проверки электронной подписи.

10. Сформируйте криптосистему электронной подписи для заданных значений параметров P = 37, Q = 73, E = 53, p = 31, q = 43, e = 83. В ответе укажите значения закрытых ключей D и d.

11. Вычислите значение подписи для сообщения т = 151 от клиента А к банку В системе электронной подписи, если известны значения открытых ключей банка В (N, E) = (4399, 83) и клиента А (п, е) = (2923, 109), а так же закрытый ключ клиента (p, d) = (37, 541).

12. В криптосистеме электронной подписи известны открытые ключи банка и клиента: (N, E) = (3713, 71) и (п, е) = (2993, 83). Банк получил подписанное сообщение (m, s) = (1486, 131) от клиента. Сделайте проверку правильности подписи со стороны банка и дайте ответ6 принимать сообщение или не принимать, если известен закрытый ключ банка (P, D) = (41, 1415).

13. В криптосистеме электронной подписи известны открытые ключи банка и клиента: (N, E) = (3713, 71) и (п, е) = (2993, 83). Банк получил подписанное сообщение (m, s) = (517, 139) от клиента. Сделайте проверку правильности подписи со стороны банка и дайте ответ6 принимать сообщение или не принимать, если известен закрытый ключ банка (P, D) = (41, 1415).

Самостоятельная работа:

1. Вычислите закрытый ключ криптосистемы RSA с параметрами p = 7, q = 3, e = 63. Зашифруйте с помощью полученной системы сообщение «112». Выполните проверку, расшифровав закодированное сообщение.

2. Вычислите закрытый ключ криптосистемы RSA с параметрами p = 58, q = 19, e = 83. Зашифруйте с помощью полученной системы сообщение «112». Выполните проверку, расшифровав закодированное сообщение.

3. Сформируйте криптосистему электронной подписи для заданных значений параметров P = 27, Q = 53, E = 83, p = 41, q = 63, e = 13. В ответе укажите значения закрытых ключей D и d.

4. Вычислите значение подписи для сообщения т = 383 от клиента А к банку В системе электронной подписи, если известны значения открытых ключей банка В (N, E) = (1375, 28) и кли-

ента А (п, е) = (1721, 489), а так же закрытый ключ клиента (p, d) = (12, 457).

5. В криптосистеме электронной подписи известны открытые ключи банка и клиента: (N, E) = (713, 51) и (п, е) = (1563, 53). Банк получил подписанное сообщение (m, s) = (4168, 456) от клиента. Сделайте проверку правильности подписи со стороны банка и дайте ответ: принимать сообщение или не принимать, если известен закрытый ключ банка (P, D) = (58, 4515).

6. В криптосистеме электронной подписи известны открытые ключи банка и клиента: (N, E) = (7513, 51) и (п, е) = (8293, 43). Банк получил подписанное сообщение (m, s) = (517, 139) от клиента. Сделайте проверку правильности подписи со стороны банка и дайте ответ6 принимать сообщение или не принимать, если известен закрытый ключ банка (P, D) = (51, 8615).

Самостоятельная работа студентов

Студенты обязаны в объеме часов, отпущенных на самостоятельную работу при изучении данной дисциплины, выполнять следующие виды самостоятельной работы:

- разбор и изучение теоретического материала по учебникам, пособиям и конспектам лекций;
- решение заданий по темам практических занятий;
- подготовка к промежуточному контролю.

К экзамену необходимо выполнить все виды работ.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины «Математические основы криптологии»:

Основная литература

1. Фомичев, В. М. Дискретная математика и криптология: курс лекций[Электронный ресурс]. – Москва : Диалог-МИФИ, 2003. – 397 с. – Режим доступа:

http://biblioclub.ru/index.php?page=book_red&id=89387. – Загл. с экрана. (14.06.2018)

2. Ерусалимский, Я. М. Дискретная математика. Теория и практикум. – Санкт-Петербург : Лань, 2018. – 476 с. – Режим до-

ступа: http://e.lanbook.com/book/106869. – Загл. с экрана. (14.06.2018)

3. Новиков, Ф. А. Дискретная математика для программистов [Текст] : учеб. пособие для вузов / Ф. А. Новиков. – Санкт-Петербург : Питер, 2007. – 364 с.

4. Акимов, О. Е. Дискретная математика: логика, группы, графы [Текст] : [учеб. пособие для вузов] / О. Е. Акимов. – Москва : Лаборатория Базовых Знаний, 2003. – 376 с.

Дополнительная литература

1. Шевелев, Ю. П. Дискретная математика. – Санкт-Петербург : Лань, 2018. – 592 с. – Режим доступа: http://e.lanbook.com/book/107270. – Загл. с экрана. (14.06.2018)

2. Соболева, Т. С. Дискретная математика [Текст] : учебник для студентов вузов / Т. С. Соболева, А. В. Чечкин; под ред. А. В. Чечкина. – Москва : Академия, 2006. – 256 с.

3. Белоусов, А. И. Дискретная математика [Текст] : учебник для студентов втузов / А. И. Белоусов, С. Б. Ткачев; под ред. В. С. Зарубина, А. П. Крищенко. – Москва : МГТУ им. Н. Э. Баумана, 2006. – 744 с.

4. Иванов, Б. Н. Дискретная математика. Алгоритмы и программы [Текст] : учебное пособие для вузов / Б. Н. Иванов. – Москва : Лаборатория Базовых Знаний, 2003. – 288 с.