ӘДЕБИЕТТЕР

1. Диффи У., Хеллман М. Э. Защищенность и имитостойкость: Введение в криптографию //ТИИЭР. – 1979. – 67. - №3. - С.71-103.
2. Задирака В. К., Абдикаликов К. А. Элементы современной криптографии и методы защиты банковской информации. Алматы. Респ. Изд. Кабинет. 1999. 337 с.
3. Абдикаликов К. А. Традиционные симметричные криптосистемы. – Актобе.: АГУ им. К. Жубанова, 2003. – 66 с.
4. Diffie W., Hellman M. New directions in cryptography //IEEE Trans. on Informat.Theory. – 1976. – Vol 22. – P. 644-654.
5. Rivest R. L., Shamir A, and Adleman. A method for obtaining digital signatures and public – key cryptosystems // Comm. ACM. – 1978. – 21. – P.120-126.
6. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. – 1985. Vol. It – 31. - №.4.
7. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М: Мир, 1996. – 318 с.
8. Герасименко В., Размахнин М. К. Криптографические методы в автоматизированных системах // Зарубежная радиоэлектроника. – 1982. - №8. -С. 97-123.
9. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
10. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
11. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
12. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему. – С. Петербург.: «Мир и Семья», «Интерлайн», 1998. – 256 с.
13. Конхейм А. Г. Основы криптографии: Пер. с англ. – М.: Мир, 1987. – 412 с.
14. Малый тематический выпуск «Защита информации» //ТИИЭР. – 1988. – 76. № 5. – С.24-125.
15. Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993. – 216 с.

16. Рублинецкий В. И. Введение в компьютерную криптологию. Харьков.: ОКО, 1997. – 128 с.

17. Сравнение практических схем цифровой подписи //Передача информации: Экспресс-информация. – 1993. - №6. – С.19-27.

18. Абдикаликова Н. И. Современные симметричные криптосистемы. – Актобе: Ред. Изд. Отдел АГУ К. Жубанова, 2001. – 64с.

19.Тимошенко А. А. Защита информации в системах «Клиент - Банк » //Безопасность информации. – 1995. - № 5. – С.39-44.

20.Уолкер Б. Дж., Блейн Я. Ф. Безопасность ЭВМ и организация их защиты. – М.: Связь, 1980. – 142 с.

21. Хоффман Л. Дж. Современные методы защиты информации. – М.: Сов. радио, 1980. – 264 с.

22. Шеннон К. Э. Теория связи в секретных системах. В работах по теории информации и кибернетики. – М.: ил.,1963. -830 с.

23. Гайкович В. Ю., Ершов Д. В. Основы безопасности информационных технологий. – М.: ЦБ РФ, МИФИ, 1995. – 94с.

24. Давыдовский А. И., Дорошкевич П. В. Защита информации в вычислительных сетях // Зарубежная радиоэлектроника. – 1989. - №12. – С. 60-70.

25. Бияшев Р. Г., Диев С. И., Размахнин М. К. Основные направления развития и совершенствования криптографического закрытия информации// Зарубежная радиоэлектроника. – 1989. - №12. -С. 76-91.

26. Задирака В. К. Теория вычисления преобразования Фурье. – Киев.: Наукова думка, 1983. – 216 с.

27. Задирака В. К., Мельникова С. С. Быстрое умножение многоразрядных чисел с использованием БПФ //Кибернетика и системный анализ. – 1996. -№3. -С.63-68.

28. Кнут Д. Е. Искусство программирования для ЭВМ. Т.2. - М.: Мир, 1977. – 724 с.

29. Коваленко Н. И., Никитин А. И., Пилипчак С. И., Фаль А. М. Стандарты по защите информации, требующие использования криптографических методов //Безопасность информации. – 1996. - №3(6). - С.18-23.

30. Брикелл Э. Ф., Одлижко Э. М. Крипоанализ: Обзор новейших результато //ТИИЭР. – 1988. – 76. №5. - С.75-93.

31. Кудин А. М. Анализ современных методов формирования ключей с использованием принципов асимметричной криптографии. //Безопасность информации. – 1996. - №4(7). - С. 6 -10.

32. Лагутин В. С., Петраков А. В. Утечка и защита информации в телефонных каналах. – М.: Энергоатомиздат, 1996. – 296 с.

33. Месси Дж. Л. Введение в современную криптологию //ТИИЭР. – 1988. – 76. № 5. – С.24-42.

34. Введение в криптографию /Под общ. ред. В. В. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 278 с.

35. Моисеенков И. Э. Американская классификация и принципы оценивания безопасности компьютерных систем // Компьютер Пресс. – 1992. -№2. – С. 61-68. - №3. -С. 47-54.

36. Моисеенков И.Э. Основы безопасности компьютерных систем // Компьютер Пресс. – 1991. - №10. - С. 19-24.

37. Рябко Б. Я. Просто реализуемая идеальнаякриптографическая система // Проблемы передачи информации. – 2000. – Т.36, №1. - С. 90-104.

38. Охрименко С. А. Защита от компьютерных вирусов. - Кишинев.: Штеминица, 1991. – 102с.

39. Першиков В. И., Савенков В. М. Толковый словарь по информатике. 2-е изд., доп. - М.: Финансы и статистика, 1995. - 544 с.

40. Райвест Л. Р. Многоуровневая криптография //Защита информации. «Конфидент». – 1997. - №1. - С. 65-70.

41. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. М.: Мир, 1984. - Т1. -527с.

42. Спановский В. А. Безопасность обмена банковскими сообщениями в SWIFT //Защита информации. - 1992. -№1. -С.185-193.

43. Смид М. Э., Бранстед Д. К. Стандарт шифрования данных: Прошлое и будущее //ТИИЭР. - 1988. - 76. №5. - С.43-53.

44. Сяо D., Керр D., Медник С. Защита ЭВМ. – М.: Мир, 1982. - 263 с.

45. Тайли Э. Безопасность персонального компьютера: Пер. с анг. – М: ООО «Попурри», 1997. – 480 с.

46. Уилкинсон Дж. Х. Алгебраическая проблема собственных чисел. - М.: Наука , 1970. - 564 с.

47. Уильямс Х. Проверка чисел на простоту с помощью вычислительных машин // Кибернет. сб., нов. серия.М.: Мир, - 1986, - № 33. -С.31-50.

48. Чмора А. Л. Практическая криптостойкость RSA: оценки и прогнозы // Мир связи. - 1997,-№ 10. – С. 56-61.

49. Фаль А. М. Алгоритм шифрования по ГОСТу 28147-89 и способы применения блочных шифров //Безопасность информации. - 1995. - № 3. -С. 8-11.

50. Хэйт Т. Размышления об электронных платежах //Сети и системы связи. – 1996. - №4. - С. 118-121.

51. Шенхаге А., Штрассен В. Быстрое умножение больших чисел //Кибернет. сб. -1973. -вып.10. -С. 87-98.

1-ҚОСЫМША. САНДАР ТЕОРИЯСЫНЫҢ ЭЛЕМЕНТТЕРІ

1. Бүтін сандар сақинасы және олардың бөлінгіштігі. Қалдықпен бөлу теоремасы

1.1. Бүтін сандар сақинасы

Натурал сандар жиынында алу амалы орындала бермейді, яғни $a + x = b$ теңдеуінің шешімі N -де жатпауы мүмкін.

Тек, $b > a$болса ғана $x = b - a$ шешімі табылады. $b - a$ натурал сандардың айырымы деп айтылады. Натурал сандар үшін алу амалы орындалатын жиын құрайық. Оны Z деп таңбалайық. Сонымен бүтін сандар жиыны деп екі натурал санның айырымы түрінде жазылатын сандар жиынын белгілейік:

$$Z = \{\alpha, \beta, \gamma, \dots\}$$

мұндағы

$$\alpha \leftarrow (a, b), \quad \beta \leftarrow (c, d) \text{ т.с.с}$$

a, b, c, d- натурал сандар

Басқаша айтақанда $\alpha = a - b \overset{Df}{\leftarrow} (a, b), \quad \beta = (c - d) \overset{Df}{\leftarrow} (c, d)$

Df- «анықтама бойынша» деп оқылады.

Z жиынында қосу, көбейту амалдарын енгізейік.

Анықтама 1. $\alpha \sim \beta \Leftrightarrow a + d = b + c$

$\sim$ - эквиваленттілік қатынас.

Келешекте $\alpha \sim \beta$ болса, онда $\alpha = \beta$ деп алайық.

Аксиома 1.

$1^{+}) (a, b) + (c, d) = (a + c, b + d)$

$2^{+}) -(c, d) = (d, c)$

қарама-қарсы элемент.

Теорема 1. Бүтін сандарды қосу коммутативті және ассоциативті, яғни

а) $(a, b) + (c, d) = (c, d) + (a, b)$

б) $[(a, b) + (c, d)] + (k, l) = (a, b) + [(c, d) + (k, l)]$

Дәлелдеуі натурал сандарды қосудың коммутативтілігі мен ассоциативтігінен шығады:

а) $(a, b) + (c, d) = (a + c, b + d)$

$(c, d) + (a, b) = (c + a, d + b)$

$a + c = c + a$, $b + d = d + b$

теңдіктерінен а) ақиқаттығы шығады.

Осы сияқты б) ақиқаттығы дәлелденеді.

Теорема 2. Бүтін сандар жиыны қосу бойынша абельдік группа құрады.

Дәлелдеу. Бүтін сандарды қосу әр кез орындалады және қосу коммутативті, ассоциативті (теорема 1).

Ендеше, группа болу үшін нөл және қарама-қарсы элемент (сан) бар екенін көрсетсек болғаны.

$(0, 0)$ - қосағы нөлді анықтайтындығын тексеру қиын емес. Себебі

$$(a, b) + (0,0) = (a + 0, b + 0) = (a, b)$$

$(0, 0)$ қосағымен (m, m) кез келген қосағы эквивалентті екенін ескерте кетейік. Демек $(0, 0) \sim (m, m) \to 0 \in Z$.

$$(c, d) + [-(c, d)] \overset{2+}{=} (c, d) + (d, c) = (c + d, d + c) = (0, 0)$$

Демек $-(c, d)$ қосағы (c, d) үшін қарама-қарсы.

Бұдан бүтін сандар үшін алу амалы орындалатындығы көрінеді:

$$(c, d) + (x, y) = (a, b),$$

онда

$$(x, y) = (a, b) - (c, d) = (a, b) + [-(c, d)]$$

Аксиома. $2^{\oplus})(a,\ b) \cdot (c,\ d) = (ac + bd,\ ad + bc)$.

Теорема 3. Бүтін сандарды көбейту коммутативті және ассоциативті. Көбейту қосу бойынша дистрибутивті. Яғни,

а) $(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$

б) $[(a, b) \cdot (c, d)] \cdot (k, l) = (a, b) \cdot [(c, d) \cdot (k, l)]$

в) $[(a, b) + (c, d)] \cdot (k, l) = (a, b) \cdot (k, l) + (c, d) \cdot (k, l)$.

Дәлелдеуі натурал сандарды көбейтудің коммутативтілігі, ассоциативтілігінен, дистрибутивтілігінен шығады.

Теорема 4. Бүтін сандар жиыны сақина құрайды.

Дәлелдеуі 3 теоремадан шығады.

1.2. Z сақинасындағы қалдықпен бөлу теоремасы

$Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ бүтін сандар жиыны.

Теорема 5. Кез келген екі бүтін a және $b > 0$ бүтін сандары үшін жалғыз q және r бүтін сандары табылып

$$a = bq + r,\ 0 \le r < q \qquad (1)$$

теңдігі орындалады, мұндағы q толымсыз бөлінді, r оң қалдық деп айтылады.

Дәлелдеу. Алдымен q және r бүтін сандарының табылатынын көрсетейік.

1) Егер $a < b$ болса, онда $a = b \cdot 0 + a$. Демек $q = 0$, $r = a$

(1) – теңдік орындалады.

2) $a > b > 0$ болсын. Онда Архимед аксиомасы бойынша $b \cdot 1,\ b \cdot 2,\ b \cdot 3,\ ...,\ b \cdot q,\ b(q+1),\ ...$ сандарының арасында $bq \le a < b(q+1)$ теңсіздігі орындалатын q табылады.

$a - bq = r$ деп белгілесек, мұндағы $0 \le r < b$.

Бұдан, $a = bq + r$ орындалатынын көреміз.

3) $a < 0$ болсын. Онда $-a > 0$ оң бүтін сан. Онда 1) және 2) жағдайдағы сияқты Архимед аксиомасынан $bq < -a \le b(q+1)$ орындалатын q табылады.

Демек $b(-q) > a \ge b(-q-1)$. Егер $a - b(-q-1) = r$ деп белгілесек, мұндағы $0 \le r < b$. Онда $a = b(-q-1) + r$ орындалып, (1) сияқты теңдік орындалады. Тек q орнына $-q-1$ алынған.

Сонымен, a және b үшін q және r табылатыны дәлелденеді. Енді q және r жалғыз екенін көрсетейік.

Керісінше, (1) теңдікті қанағаттандыратын басқа q_1, r_1 екі саны табылсын.

$$a = bq + r,\ 0 \le r < b \qquad (2)$$
$$a = bq_1 + r_1,\ 0 \le r_1 < b \qquad (3)$$

$r \ne r_1$ болсын, онда не $r > r_1$, не $r < r_1$

$r > r_1$ болсын, онда (1)-ден (2) шегерсек

$b(q_1 - q) = r - r_1$, $r - r_1 > 0$ (3) болғандықтан және $b > 0$, ендеше $q - q_1 > 0$ оң бүтін сан, яғни$q - q_1 \geq 1$. b-ге көбейтсек, $b(q_1 - q_0) > b$. Бұдан (3) $r - r_1 > b$ шығады, ал бұл мүмкін емес, себебі $r < b$, $r_1 < b$.

Мысал.

1) $a = 47$, $b = 6$ болсын, онда $47 = 6 \cdot 7 + 5$, $q = 7$, $r = 5$

2) $a = -29$, $b = 6$ болсын, онда $-29 = 6 \cdot (-5) + 1$, $q = -5$, $r = 1$.

1.3. Бүтін сандардың бөлінгіштігі. Екі санның ең үлкен ортақ бөлгіші және ең кіші ортақ еселігі

Бүтін сандар үшін бөлінгіштік бинарлық қатынасын қарайық.

Анықтама 3. Егер бүтін a және b сандары үшін $a = bc$ теңдігін қанағаттандыратын c бүтін саны табылса, онда a саны b-ға бөлінеді және $a \vdots b$ деп жазады. Мұндағы b-ны a-ның бөлгіші дейді, немесе a саны b-ға еселі сан дейді.

Егер $a = bc$ орындалатын c бүтін саны табылмаса, онда a саны b-ға бөлінбейді дейді және $a \vdots b$ деп жазады.

Бөлінгіштіктің анықтамасынан шығатын қасиеттер:

1º. 1) $a \vdots a$, себебі $a = a \cdot 1$, «$\vdots$» - рефлексивті

2) $a \vdots 1$, себебі $a = 1 \cdot a$

3) $0 \vdots b$, себебі $0 = b \cdot 0$

2º. $\forall a, b, c \in Z$, $a \vdots b \wedge b \vdots c \Rightarrow a \vdots c$, «$\vdots$» - транзитивті.

Дәлелдеу. $a = bq_1 \wedge b = cq_2 \Rightarrow a = cq_1q_2 \Rightarrow a \vdots c$.

3º. $\forall a, b, c \in Z$, $a \vdots c \wedge b \vdots c \Rightarrow (a \pm b) \vdots c$.

Дәлелдеу. $a = cq_1 \wedge b = cq_2$, онда $a + b = c(q_1 + q_2) \Rightarrow (a + b) \vdots c$. $(a - b) \vdots c$ осы сияқты дәлелденеді.

4º. $\forall a, b, c \in Z$, $a \vdots b \Rightarrow ac \vdots b$, сол сияқты $ac \vdots bc$.

Дәлелдеу. $a = bq \Rightarrow ac = b(qc) \Rightarrow ac \vdots b$ осы теңдіктен $ac \vdots bc$ шығады.

5º. $\forall a_1, a_2, ..., a_n \in Z$, $\forall b_1, b_2, ..., b_n \in Z$,

$$a_1 \vdots c, a_2 \vdots c, \ldots, a_n \vdots c \Rightarrow (a_1b_1 + a_2b_2 + \ldots + a_nb_n) \vdots c.$$

Дәлелдеуі. 3º, 4º шығады.

6º. Егер $a \vdots b$ және $b \vdots a$, онда $a = \pm b$

Дәлелдеуі. Шарттан $a = bq$, $b = aq_1 \Rightarrow a = aqq_1 \Rightarrow 1 = qq_1$ бұдан qq_1-бүтін сандардың көбейтіндісі 1- ге тең болу үшін $q = q_1 = \pm 1$ болу керек. Демек $a = b$ не $a = -b$.

Анықтама 4. a және b бүтін сандарының ортақ бөлгіші деп екеуі де бөлінетін d бүтін санын айтады. a және b сандарының ең үлкен ортақ бөлгіші (қысқаша *Е.Ү.О.Б.*) деп басқа ортақ бөлгіштерге бөлінетін ортақ бөлгішін айтады.

Ортақ бөлгішті қысқаша $О.Б.(a,b)$, ең үлкен ортақ бөлгішті $Е.Ү.О.Б.(a,b)$ деп белгілейміз.

Мысалы.

$a=18$, $b=24$, О.Б.$(18,24)=1,2,3,6.$

Е.Ү.О.Б.$(18,24)=6$, себебі $6\vdots 3$, $6\vdots 2$, $6:1$.

Анықтама 5. Егер a және b сандарының $Е.Ү.О.Б.(a,b)=1$ болса, онда оларды өзара жай сандар дейді.

Ескерту. Келешекте $Е.Ү.О.Б.(a,b)$ орнына (a,b), $Е.Ү.О.Б.(a,b)=1$ орнына $(a,b)=1$ жазамыз.

Қасиет 1º. Егер $a\vdots b$, онда $(a,b)=b$.

Дәлелдеусіз түсінікті.

Қасиет 2º. $\forall a,b\in Z$, егер $a=bq+r$ болса, онда $(a,b)=(a,r)$.

Дәлелдеуі. Егер d a мен b-ның ең үлкен ортақ бөлгіші болса, онда $a=bq+r$ теңдігінен d b мен r үшін де ең үлкен ортақ бөлгіш екенін байқау қиын емес.

Ескерту. $Е.Ү.О.Б.(a,b)$ табу үшін 2º - ші қасиетті пайдалануға болады. Мысал $a=2484$, $b=60$.

Қалдықпен бөлу жасап, 2º пайдаланайық.

$2484=60\cdot 41+24\Rightarrow(2484,60)=(60,24)$

$60=24\cdot 2+12\Rightarrow(60,24)=(24,12)$

$$24=12\cdot 2+0\Longrightarrow(24,12)=12.$$

Демек$(2484,60)=12.$

Екі санның ең үлкен ортақ бөлгішін табу үшін Евклид өзінің «Бастама» кітабының VII томында қарапайым алгоритм қолданған. Оны Евклид алгоритмі деп атайды. Бұл әдісті қолданудың мәні 2º қасиетте айтылады.

Евклид алгоритмі.

Қалдықпен бөлу теоремасындағы бөліндіні қалдыққа қайталап бөле берейік.

$$\left.\begin{array}{ll} a = bq + r, & 0 < r < b \\ a = bq_1 + r_1, & 0 < r_1 < r \\ r = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ - - - - - - - - - - & \\ - - - - - - - - - - & \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + 0, & \end{array}\right\} (4)$$

(4) – бөлу процесін Евклид алгоритмі дейді.

Бөлу кезінде қалдықтар 1-ге дейін кемиді, сондықтанда бөлу процесі шекті.

2º қасиеттен $(a,b) = (b,r) = (r,r_1) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n$.

Теорема 6. Егер $(a,b) = d$ болса, онда $a = a,d$, $b = b,d$, $(a_1, b_1) = 1$.

Дәлелдеуі оңай көрініп тұр.

Теорема 7. Егер және бүтін сандарының ең үлкен ортақ бөлгіші d болса, онда u, ϑ деген бүтін сандар табылып, $au = b\vartheta = d$ теңдігі орындалады.

Дәлелдеуі. (4) алгоритміндегі r_n-ді төменнен жоғары көтеріліп a және b арқылы өрнектеу керек.

Дербес жағдай, $d = 1$ болса, $(a,b) = 1$ үшін u, ϑ сандары табылып, $1 = au + b\vartheta$ орындалады.

Анықтама 6. a және b сандарының әрқайсысына бөлінетін санды олардың ортақ еселігі дейді. a және b сандарына еселі сандардың бәрі бөлінетін a мен b-ның ортақ еселігі санын олардың ең кіші ортақ еселігі саны дейді.

Басқаша айтқанда, ең кіші ортақ еселік сан a мен b-ның ортақ еселіктерінің ең кішісі.

a мен b ортақ еселігін *О.Е.* $[a,b]$ деп, ал ең кіші ортақ еселігін $[a,b]$ деп немесе *Е.К.О.Е.* $[a,b]$ деп жазамыз.

Теорема 8. a және b сандарының *Е.Ү.О.Б.* мен *Е.К.О.Е.* арасында $[a,b] = \dfrac{a \cdot b}{(a,b)}$ теңдігі орындалады.

Дәлелдеуі. $M = O.E.[a,b]$ болсын, демек $M \vdots a$, $M \vdots b$.

Ендеше, $M = ak$ болсы, онда $\dfrac{M}{b} = \dfrac{ak}{b}$ бүтін сан болады.