

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Каждая буква алфавита была заменена на другую букву. При этом разные буквы были заменены разными. Расшифруйте фразу, позволяющую запомнить расположение планет солнечной системы (здесь Плутон считается планетой):

ЧАЮША ПСЭЙМЙМЕ ЯК ЧКНО, БПЙЭТНША ОПЙНШЦП Ц ШКИЙУ ЦЭКШЙМС.

2. Даты рождения учеников хранились на сервере школы. Для каждого ученика его дата рождения была представлена числом  $t$ , которое вычислялось по формуле  $t = 31(m-1) + (d-1)$ , где  $m$  – номер месяца,  $d$  – порядковый день месяца. (Например, если  $t = 65$ , то  $m = 3$  и  $d = 4$ , то есть этот ученик родился 4-го марта.) Затем было решено сведения о датах рождения зашифровать. Вместо числа  $t$  на сервере теперь хранится число  $x$  такое, что число  $a^x$  при делении на 373 дает остаток  $t$ , где  $a$  – секретное (но одинаковое для всех учеников) натуральное число. Известно, что Мария родилась 28-го марта, Александр – 31-го января. Известно также, что число  $a^{372}$  при делении на 373 дает остаток 1. Найдите дату рождения Павла.

Ученик	$x$
Мария	31
Александр	12
Павел	189

3. На прямой заданы два отрезка, длины которых равны  $2016^{2015} - 1$  и  $2016^{2018} - 1$ . Осуществляя построения только на этой прямой (т.е. без использования точек вне прямой), с помощью циркуля постройте отрезок длины 2015.
4. Для зашифрования сообщения на русском языке, знаки препинания в котором опущены, а слова отделены друг от друга знаком пробела (-), используется двухблочный шифратор. Первый блок шифратора заменяет буквы сообщения и пробелы (-) на числа в соответствии с таблицей, построенной на основе ключевого слова. Сначала записывается ключевое слово, потом знак пробела (-), потом остальной алфавит в естественном порядке за исключением букв, входящих в ключевое слово (при этом считается, что  $E = \text{Ё}$ ). Например, если ключевое слово *привет*, то первый блок будет осуществлять замену в соответствии со следующей таблицей:

П	Р	И	В	Е	Т	-	А	Б	Г	Д	Ж	З	Й	К	Л	М	Н	О	С	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Второй блок получает на входе числа из первого блока и осуществляет усложнение шифрованного сообщения по следующему правилу. Первое число он оставляет без изменений, а к каждому следующему прибавляет число, равное произведению числа 33 и остатка от деления на три предыдущего числа. Слово *тайное* на предложенном ключе будет зашифровано в сообщение 5 73 46 50 84 4 (см. таблицу). Прочитайте сообщение, зашифрованное этим шифратором на другом ключе, если известно, что в сообщении встречается слово *здесь*:

Текст	Т	А	Й	Н	О	Е
1й блок	5	7	13	17	18	4
Остаток	2	1	1	2	0	1
2й блок	5	73	46	50	84	4

30 5 84 6 16 51 10 42 5 72 19 51 14 66 11 66 5 95 70 65 72 4 38 86 66 17 83 94 49 39 17 84 6 17 84 24 29 97 39 11 74 75 4 62 72 1 37 42 6 14 84 25 47 78 6 4 42 20 94

5. Про составленный из цифр 20-значный пароль  $(a_1, a_2, \dots, a_{20})$  известно следующее: 1) сумма первых 5 цифр  $a_1 + \dots + a_5$  делится на 5, 2) сумма первых 10 цифр  $a_1 + \dots + a_{10}$  делится на 10 и 3) сумма всех цифр пароля  $a_1 + \dots + a_{20}$  делится на 20. Сколько таких паролей?
6. Для безопасной передачи по сети на мобильный телефон секретного ключа (СК), представляющего собой набор из 3-х цифр  $p_1 p_2 p_3$ , этот ключ предварительно зашифровывается следующим образом. Формируется четырехзначное число  $m = 1 p_1 p_2 p_3$ , и вычисляется зашифрованный ключ (ЗК)  $c$  по формуле  $c = r_n(m^3)$ , где  $r_n(z)$  – остаток от деления числа  $z$  на  $n$ . Это значение  $c$  и пересылается по сети. При получении числа  $c$  на телефоне подсчитывается число  $M = r_n(c^d)$ . Причем натуральное число  $d$  выбрано так, что для любого

**XXVI Межрегиональная олимпиада школьников по математике и криптографии**

натурального числа  $z$  выполняется равенство  $r_n(z^{3d}) = r_n(z)$ . Если найденное  $M$  не является четырехзначным числом, первая цифра в котором 1, телефон выдаёт сообщение об ошибке. Злоумышленник перехватил ЗК  $c = 18299$  и предпринял попытку передачи на телефон новых чисел вида  $r_n(s \cdot c)$ . При  $s = 100^3$  была получена ошибка, а при  $s = 89^3$  и  $s = 1728$  ошибки не возникло. Определите СК, если  $n = 20203$ .