ДМ-2. Задачі до лекції 8.

Теорія чисел і криптографія: застосування конгруенцій; класична криптографія

Задачі

Блок 1. Застосування конгруенцій.

1. Яку область пам'яті буде присвоєно геш-функцією $h(k) = k \bmod 97$ для реєстрації страховою компанією клієнта з таким номером соцзабезпечення

а) 183211232
б) 220195744
в) 987255335

2. Автомобільний паркінг має 31 місце, які занумеровано від 0 до 30. Користувачам призначається місце за допомогою геш-функції $h(k) = k \bmod 31$, де k – номерний знак. Які місця буде призначено відвідувачам з номерними знаками 317, 918, 007, 100, 111, 310? Що робити, коли призначене для парковки місце зайнято?

3. Яку послідовність псевдовипадкових чисел генерує лінійний конгруентний генератор $x_{n+1} = (3x_n + 2) \bmod 13$, якщо початкове значення $x_0 = 1$?

4. Яку послідовність псевдовипадкових чисел генерує лінійний конгруентний генератор $x_{n+1} = (4x_n + 1) \bmod 7$, якщо початкове значення $x_0 = 3$?

5. *Степеневий генератор* – це метод для генерування псевдовипадкових чисел. Для використання степеневого генератора вибирають параметри p і d, де p – просте, d – додатне ціле, таке, $p \nmid d$; також вибирають початкове значення x_0. Псевдовипадкові числа x_1, x_2, x_3, ... генерують за рекурентною формулою $x_{n+1} = x_n^d \bmod p$. Знайти послідовність псевдовипадкових чисел, генеровану степеневим генератором з $p = 7$, $d = 3$ і початковим значенням $x_0 = 2$.

6. Знайти послідовність псевдовипадкових чисел, генеровану степеневим генератором з $p = 11$, $d = 2$ і початковим значенням $x_0 = 3$.

7. Припустімо, що ми отримали з каналу зв'язку наведені нижче бітові рядки, де останній біт – паритетний. У яких рядках *напевно* є помилка?

а) 00000111111
б) 10101010101
в) 11111100000
г) 10111101111

8. Перші дев'ять розрядів в коді ISBN-10 європейської версії п'ятого видання книги Kenneth H. Rosen *Discrete Mathematics and Its Applications* такі: 0-07-119881. Знайти перевірочний розряд цього коду.

9. Код ISBN-10 шостого видання книги *Elementary Number Theory and Its Applications* такий 0-321-500Q1-8, де Q – розряд. Знайти значення Q.

10. Тринадцяти бітний код ISBN-13 сьомого видання книги Kenneth H. Rosen *Discrete Mathematics and Its Applications* має такі перші дванадцять розрядів: 978-0-07-338309. Знайти перевірочний розряд цього коду.

11. Поштовий сервіс США (**United States Postal Service, USPS**) під час пересилання коштів для ідентифікації використовує 11-розрядний код $x_1x_2\ldots x_{11.}$ Перші 10 розрядів ідентифікують грошовий переказ; x_{11} перевірочний розряд, $x_{11} = x_1 + x_2 \ \ldots + x_{10}$ **mod** 9.

Знайти перевірочний розряд USPS грошового переказу, якщо перші десять розрядів такі:

а) 7555618873
б) 6966133421
в) 8018927435
г) 3289744134

12. Одна з цифр у кожному з наступних ідентифікаційних номерів USPS затерта. Чи можна відновити затерту цифру, позначену Q, у кожному з наступних номерів?

а) 493212Q0688
б) 850Q9103858
в) 2Q941007734
г) 66687Q03201

13. Одна з цифр у кожному з наступних ідентифікаційних номерів USPS затерта. Чи можна відновити затерту цифру, позначену Q, у кожному з наступних номерів?

а) Q1223139784
б) 6702120Q988
в) 27Q41007734
г) 213279932Q1

14. Визначити перевірочний розряд для коду UPC (Universal Product Code), якщо перші 11 розрядів такі:

а) 73232184434;
б) 63623991346;
в) 04587320720;
г) 93764323341.

15. Перевірте, чи є кожний із рядків 12 цифр коректним UPC кодом.

а) 036000291452;
б) 012345678903;
в) 782421843014;
г) 726412175425.

16. Періодичні видання ідентифікують за допомогою **International Standard Serial Number (ISSN)**. Код ISSN містить два блоки по чотири цифри кожний. Остання цифра другого блоку – перевірочна. Перевірочну цифру обчислюють за допомогою конгруенції

$$d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}.$$

Коли $d_8 \equiv 10 \pmod{11}$, ми використовуємо букву X для репрезентації d_8 у коді.

Для кожних із наведених нижче початкових цифр коду ISSN визначити перевірочну цифру (яка може бути буквою X).

а) 1570-868;
б) 1553-734;
в) 1089-708;
г) 1383-811.

17. Чи є наведені нижче восьмицифрові коди коректними кодами ISSN?

а) 1059-1027;
б) 0002-9890;
в) 1530-8669;
г) 1007-120X.

Блок 2. Класична криптографія.

Таблиця 1.

Латинська абетка

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Таблиця 2.

Українська абетка

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

1. Зашифрувати повідомлення DO NOT PASS GO за допомогою шифру зсуву чи афінного шифру:

а) $f(p) = (p + 3)$ **mod** 26 (шифр Цезаря);
б) $f(p) = (p + 13)$ **mod** 26;
в) $f(p) = (3p + 7)$ **mod** 26.

2. Зашифрувати повідомлення WATCH YOUR STEP за допомогою шифру зсуву чи афінного шифру:

а) $f(p) = (p + 14)$ **mod** 26;
б) $f(p) = (14p + 21)$ **mod** 26;
в) $f(p) = (-7p + 1)$ **mod** 26.

3. Зашифрувати повідомлення ЗУСТРІЧ ВІДМІНЕНО за допомогою шифру зсуву чи афінного шифру:

а) $f(p) = (p + 14)$ **mod** 33;
б) $f(p) = (14p + 21)$ **mod** 33;
в) $f(p) = (-7p + 1)$ **mod** 33.

4. Чому в задачах **1** і **2** використано операції за модулем 26, а в задачі **3** – за модулем 33?

5. Розшифрувати повідомлення, зашифроване за допомогою шифру зсуву $f(p) = (p + 10)$ **mod** 26:

а) CEBBOXNOB XYG;
б) LO WI PBSOXN;
в) DSWO PYB PEX.

6. Розшифрувати повідомлення, зашифроване за допомогою шифру зсуву $f(p) = (p + 12)$ **mod** 33:

а) КЇРЦЇ СЇНЇЕЇ;
б) ЩОАЮЬНУКЩЇ СВАБЯУЕ.

7*. Нехай рядок англомовного тексту зашифровано за допомогою шифру зсуву

$$f(p) = (p + k) \textbf{ mod } 26:$$

DY CVOOZ ZOBMRKXMO DY NBOKW.

Дешифрувати це повідомлення.

8. Зашифрувати повідомлення ORANGE з використанням шифру Віженера з ключем RED.

9. Зашифрувати повідомлення SNOWFALL з використанням шифру Віженера з ключем BLUE.

10. Криптотекст OIKYWVVHBX отримано як результат шифрування певного повідомлення за допомогою шифру Віженера з ключем НОТ. Яке це повідомлення?

11. Зашифрувати повідомлення СНІГОПАД з використанням шифру Віженера з ключем РІК.

12. Криптотекст УМАИМДГЖШЇТЩ отримано як результат шифрування певного повідомлення за допомогою шифру Віженера з ключем СТУДЕНТ. Яке це повідомлення?