11. Довести, що за допомогою ASCII можна кодувати 256 символів. (стор. 57).

12. Пояснити, чому "алфавіт", "буквами" якого є пари букв українського алфавіту з доданим символом ␣ , містить 1156 "букв"? (стор. 58).

13. Пояснити, чому правило $\mathcal{L}_{\mathtt{UV}} < \mathcal{L}_{\mathtt{XY}}$ є еквівалентним до лексікографічного порядку? (стор. 58).

14. Проаналізувати спосіб шифрування за допомогою групування по три символи. (стор. 59).

5. Задачі

Задача 1. *Довести, що формули* (3) *та* (4) *дають однаковий результат, якщо $\mathcal{C}_{\mathtt{X}}$ є парним.*

Задача 2. *Зашифрувати* БУКВА *за допомогою мультиплікативного шифру M_{16}.*

Задача 3. *Дешифрувати слово* ИҐЄВЄ, *яке було зашифровано за допомогою мультиплікативного шифру M_{23}.*

Задача 4. *Дешифрувати слово* ЕЦЧЛЧ, *яке спочатку було зашифровано за допомогою шифру M_4, а після цього — за допомогою шифру M_7.*

Задача 5. *Чи можна застосовувати шифр M_a, якщо*

(a) $\mathcal{P}_{\mathtt{С}} = \mathcal{C}_{\mathtt{И}}$?
(b) $\mathcal{P}_{\mathtt{И}} = \mathcal{C}_{\mathtt{С}}$?

Задача 6. *Чи існує M_a шифр, при якому*

a) $\mathcal{P}_{\mathtt{Й}} = \mathcal{C}_{\mathtt{Р}}$; b) $\mathcal{P}_{\mathtt{Г}} = \mathcal{C}_{\mathtt{С}}$; c) $\mathcal{P}_{\mathtt{Е}} = \mathcal{C}_{\mathtt{Є}}$;
d) $\mathcal{P}_{\mathtt{В}} = \mathcal{C}_{\mathtt{Б}}$; e) $\mathcal{P}_{\mathtt{Ж}} = \mathcal{C}_{\mathtt{М}}$; f) $\mathcal{P}_{\mathtt{И}} = \mathcal{C}_{\mathtt{Ж}}$.

Задача 7. *Відомо, що $\mathcal{P}_{\mathtt{О}} = \mathcal{C}_{\mathtt{Х}}$, якщо застосувати шифр M_a. Знайти a.*

Задача 8. *Розглянемо наступну систему шифрування, яка базується на алфавіті з 30 букв. Перед шифруванням кожне повідомлення змінюється так, щоб три обрані букви перейшли у три інші, а саме*

$$\mathtt{К} \to \mathtt{И}, \qquad \mathtt{В} \to \mathtt{І}, \qquad \mathtt{Р} \to \mathtt{Т}.$$

Наприклад,

СЛОВО → СЛОІО

Після такої заміни у повідомленні використовується лише 30 букв українського алфавіту (всі, крім К, В *та* Р*). Змінене повідомлення шифрується за допомогою шифру M_a. Нижче показано процедуру шифрування повідомлення* РЕЧЕННЯ *для шифру M_7:*

повідомлення	Р	Е	Ч	Е	Н	Н	Я
змінене повідомлення	Т	Е	Ч	Е	Н	Н	Я
числовий формат	23	7	28	7	18	18	33
$2 \cdot \mathcal{P}_{\mathtt{X}} \pmod{30}$	11	19	16	19	6	6	21
буквенний формат	И	О	Л	О	Д	Д	Р

Таким чином,

РЕЧЕННЯ → ИОЛОДДР

a) *Яким чином відбувається дешифрація повідомлення для описаного способу?*
b) *Чому шифр M_5 можна вживати для звичайного алфавіту, але небажано для розглянутого способу? З іншого боку, чому M_{11} можна вживати для описаної схеми, а для звичайного алфавіту ні?*
c) *Зашифрувати повідомлення* БУКВА, *використовуючи описану схему.*
d) *Пояснити, чому з точки зору криптоаналізу описана схема є більш стійкою, ніж мультиплікативний шифр для звичайного алфавіту?*

Задача 9. *Нехай $m = (a_1 a_2 \dots a_k)_{10}$, де $a_1, a_2, \dots, a_k$ — це десяткові цифри у десятковому записі числа m. Довести, що $m \equiv a_1 + a_2 + \cdots + a_k \pmod 9$. Використовуючи цю властивість перевірити, чи є 78,464 сумою 3569, 24,387 та 49,508?*

Задача 10. *Назвемо цифровим коренем натурального числа m число $1 \leq d \leq 9$, яке утворено за наступним правилом: знайдемо суму цифр числа m, позначимо її s_1. Якщо $s_1 \leq 9$, то $d = s_1$; якщо ж $s_1 > 9$, то знайдемо суму цифр числа s_1, позначимо її s_2. Якщо $s_2 \leq 9$, то $d = s_2$; якщо ж $s_2 > 9$, то знайдемо суму цифр числа s_2, позначимо її s_3. Далі діємо за описаним правилом до тих пір, поки не дістанемо число, яке не перевищує 9; воно і є числовим коренем для m. Наприклад числовим коренем числа 2015 є 8, а 1999 — є 1.*

Нехай $m = (a_1 a_2 \ldots a_k)_{10}$. Довести, що $d \equiv a_1 + \cdots + a_k \pmod 9$.

Задача 11. *Нехай $\rho(n)$ — це числовий корень натурального числа n (див. задачу 10). Довести, що для будь-яких натуральних чисел m та n*

a) $\rho(\rho(n)) = \rho(n)$;
b) $\rho(m+n) = \rho(\rho(m) + \rho(n))$;
c) $\rho(mn) = \rho(\rho(m)\rho(n))$.

Задача 12. *Знайти всі можливі числові корені для квадратів натуральних чисел (див. задачу 10). Використовуючи отриманий результат, довести, що 16,151,613,924 не є квадратом.*

Задача 13. *Чи є вірним твердження, яке є оберненим до результату задачі 12? Іншими словами, чи обов'язково число є квадратом, якщо його числовий корінь дорівнює* 1, 4, 7 *або* 9?

Задача 14. *Нехай $p > 3$ та $p+2$ — числа близнюки. Довести, що числовий корінь їхнього добутку дорівнює 8. Чому це твердження є невірним для $p = 3$?*

Задача 15. *Номер кожної кредитної карти MasterCard складається з 16 десяткових цифр, які позначимо $d_1, \ldots, d_{16}$. Остання цифра d_{16} використовується для контролю. Вона обчислюється за правилом*

$$d_{16} \equiv -\left[\sum_{i=1}^{8} \rho(2d_{2i-1}) + \sum_{i=1}^{7} d_{2i}\right] \pmod{10},$$

де $\rho(m)$ — це числовий корінь числа m (див. задачу 10). Підрахувати d_{16} для карти, перші 15 цифр якої

a) 5300–7402–4001–638　　　b) 5329–0419–4253–736.