7. Шифр Віженера

Шифр Віженера — це один з *поліалфавітних шифрів*.

Таблиця 5. Tabula recta для шифру Віженера

	а	**б**	**в**	**г**	**ґ**	**д**	**е**	**є**	**ж**	**з**	**и**	**і**	**ї**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ь**	**ю**	**я**
а	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
ґ	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

Поліалфавітні шифри циклічно використовують кілька моноалфавітних шифрів. Цей принцип пояснімо на прикладі шифра Віженера.

Перед початком шифрування за Віженером зручно створити таблицю (tabula recta, таблиця 5), кожний наступний рядок якої є попереднім рядком, циклічно зсунутим вліво на одну позицію. У першому рядку записано всі букви українського алфавіту у їхньому природному порядку. Таким чином, в кожному рядку записано букви чергового моноалфавіту для шифру Віженера.

Кожен шифр Віженера має ключ; ним є певне слово, яке обирається довільним чином. Утворимо тепер *шифр-матрицю* з двох рядків: перший рядок складається з фрази, яку необхідно зашифрувати. У другому рядку записуємо ключове слово стільки разів, скільки необхідно, щоб він став довшим за перший. Якщо на певній позиції у першому рядку стоїть буква `Х`, а в шифр-матриці під нею розташовано букву `Ү`, то для шифрування букви `Х` знаходимо символ у tabula recta, який стоїть на перетині рядка `Ү` та стовпчика `Х`. Саме цей символ і є шифром Віженера букви `Х`.

Наприклад, якщо текст починається з букви `Б`, а першою буквою ключового слова є `Г`, то першим символом шифрованої фрази є буква, яка знаходиться у tabula recta на перетині рядка `Г` та стовпчика `Б`, тобто `Ґ`.

Приклад 3. Зашифруємо повідомлення `ШИФР ВІЖЕНЕРА` за допомогою ключового слова `ШИФР ВІЖЕНЕРА`, тобто шифр-матрицею є

Ш И Ф Р В І Ж Е Н Е Р А
Ш И Ф Р В І Ж Е Н Е Р А

Особливістю цього прикладу є те, що всі шифр-букви визначаються перетином рядків та стовпчиків з однаковими номерами. Оскільки на перетині рядка Ш та стовпчика Ш в таблиці 5 розташовано У, то шифром Ш є У. Аналогічно шифруємо інші букви повідомлення:

Ш	И	Ф	Р	В	І	Ж	Е	Н	Е	Р	А
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
У	Р	Л	Є	Ґ	Т	М	Ї	Б	Ї	Є	А

8. Шифр Вернама

Шифр Вернама або схема *одноразового блокноту* (англ. one-time pad) — система *симетричного шифрування*, винайдена в 1917 році співробітниками AT&T М. Моборном і Г. Вернамом. Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість. Під криптографічною стійкістю ми розуміємо властивість системи шифрування протистояти спробам дешифрування навіть при наявності усіх існуючих комп'ютерних ресурсів.

Принцип шифрування за Вернамом подамо на прикладі шифру Віженера. В цьому випадку єдиною відмінністю між ними є принцип, за яким обирається ключове слово. Якщо у шифрі Віженера воно обирається так, щоб його легко було запам'ятати, то у шифрі Вернама ключове слово

(a) має бути випадковим;
(b) має довжину, яка дорівнює довжині повідомлення;
(c) застосовується лише один раз.

До речі, ключове слово у прикладі 3 задовольняє умову (b).

Слово "*блокнот*" у назві шифру пояснюється такою схемою утворення випадкового ключа: шифрувальник забезпечується блокнотом, кожна сторінка якого містить новий ключ. Такий же блокнот є і у дешифрувальника. Використані сторінки знищуються.

Проблемою у застосуванні шифру Вернама є таємна передача блокноту з ключовими словами та збереження його у таємниці. Для цього необхідно мати надійно захищений канал для спілкування між шифрувальником та отримувачем інформації. Але, якщо існує надійно захищений канал передачі повідомлень, то шифри взагалі не потрібні: секретні повідомлення можна передавати через цей канал.

9. Контрольні питання

1. Впевнитись, що перший рядок таблиці 3 є циклічним зсувом другого рядка вправо на 3 позиції (або вліво на 30 позицій). (стор. 30).

2. Як випадки $b < 0$ або $b > 33$ для шифру Цезаря зводяться до $0 \le b \le 33$? (стор. 30).

3. Чому теорема 1 є вірною для $m = 0$? (стор. 33).

4. Довести, що число $-|m|$ належить множині M. (стор. 33).

5. Чому жоден елемент M не перевищує $|m|$? (стор. 33).

6. Чому $r \ge 0$ у доведенні теореми 1? (стор. 33).

7. Пояснити, чому $q + 1 \in M$, якщо $r \ge n$? (стор. 33).

8. Пояснити оцінки $-n < r - r' < n$. (стор. 33).

9. Чому з $n|q' - q| < n$ випливає $q' = q$? (стор. 33).

10. Переконатись, що $k \pmod{33} = k \bmod 33$ для $1 \le k < 66$. (стор. 34).

11. Перевірити, що властивості 1, 2 та 3 випливають з означення 4. (стор. 35).

12. Довести, що властивості 4–5 випливають з означення 4 (стор. 35).

13. Перевірити, що доведення властивостей 7 та 8 є таким же, як і доведення властивості 6. (стор. 36).

14. Чому теорема 5 є очевидною для $n = 2$? (стор. 37).

15. Чому існування розкладу є справедливим для простих чисел? (стор. 37).

16. Пояснити, чому знайдуться натуральні числа $a \neq 1$ та $b \neq 1$, для яких $m = ab$, якщо m не є простим числом? (стор. 37).

17. Чому n ділиться на $p_0 \cdot q_0$ у доведенні теореми 5? (стор. 39).

18. Чому жодне з чисел $q_1, \ldots, q_m$ не може дорівнювати жодному з чисел $p_1, \ldots, p_k$? (стор. 39).

19. Чому кожне з чисел $q_1, \ldots, q_m$ є більшим за p? (стор. 39).

20. Пояснити чому з теореми 6 випливає, що на кожному з проміжків $[n, n! + 1]$ ряду натуральних чисел є принаймні одне просте число. (стор. 39).

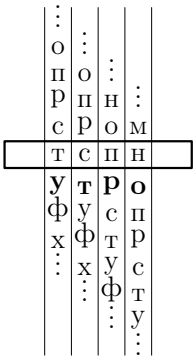
21. Чому $N! + 2$ ділиться на 2? (стор. 40).

22. Довести, що $N!+k$ ділиться на k для будь-якого $k \leq N$. (стор. 40).

10. Задачі для самостійної роботи

Задача 1. *Використати шифр Цезаря з $b = 5$ й зашифрувати слово* ЧИСЛО.

Задача 2. *Дешифрувати фразу* ЮІФХУЦЧУ, *яку зашифровано за допомогою шифру Цезаря з $b = 5$.*



Задача 3. *Для шифру Цезаря існує простий спосіб дешифрації — так званий метод смужок. Для дешифрування тексту на кожну зі смужок записують у природному порядку букви українського алфавіту. Нехай слово* ТСПН *зустрічається в повідомленні, зашифрованому шифром Цезаря. Смужки суміщають так, щоб утворилась послідовність* ТСПН. *Зафіксувавши таке положення смужок, тепер читають одне за іншим "слова" у рядках цієї "таблиці". У прикладі з* ТСПН *виявляється, що єдиним змістовним словом є* УТРО. *Це дозволяє обчислити параметр b та прочитати все повідомлення. Яким є параметр b у цьому прикладі? Пояснити чому цей прийом є універсальним?*

Задача 4. *Відомо, що текст зашифровано спочатку шифром Цезаря з параметром b_1, а потім ще раз шифром Цезаря з іншим параметром b_2. Чи є такий спосіб шифрування більш стійким, ніж спосіб, коли шифр Цезаря використовується тільки один раз?*

Задача 5. *Зашифрувати слово* `МАТЕМАТИКА` *за допомогою шифра Віженера та ключового слова* `ФІЗМАТ`.

Задача 6. *Замість зсуву букв алфавіту на певну величину, як у шифрі Цезаря, можна застосувати перестановку.*

(a) *Скільки існує різних шифрів перестановки для українського алфавіту?*

(b) *Чи є метод грубої сили ефективним, якщо відомо, що при дешифруванні використано один з таких шифрів?*

Задача 7. *Моноалфавітні шифри легко зламати, бо вони містять дані про частоту букв алфавіту. Контрзаходом є використання декількох замінників, відомих як гомофони, для однієї і тієї ж букви. Наприклад, букві* `Е` *можна призначено кілька різних символів при шифруванні, наприклад, 7, 35, 56 і 89. Кожен гомофон використовується циклічно або обирається випадковим чином. Якщо кількість гомофонів, призначених кожній букві, є пропорційною до відносної частоті цієї букви, то однобуквені частоти у повідомленні є абсолютно однаковими. Великий математик Гаусс вважав, що, використовуючи гомофони, ми маємо незламний шифр. Тим не менш, у сучасній криптографії вважається, що криптоаналіз шифрів з гомофонами є відносно простим. Поясніть це.*

Задача 8. *Довести, що шифр Цезаря є частковим випадком шифра Віженера (див. розділ 7) й знайти відповідне ключове слово.*

Задача 9. *Нехай черговою буквою у фразі, яку необхідно зашифрувати за допомогою шифру Віженера (див. розділ 7), є* `Х`*, а їй відповідає буква* `Ү` *у шифр-матриці. Нехай буква* `Ү` *має позицію i, в алфавіті, а* `Х` *— позицію j. Довести, що елементом (i, j) в tabula recta є*

$$i + j - 1 \pmod{33}.$$

Задача 10. *Зашифрувати фразу*

ШИФРВЕРНАМА

за допомогою шифру Вернама (див. розділ 8). Для цього використати наступне ключове слово:

ТЇВХЛДШОЖЮС

Задача 11. *Ключове слово у задачі 10 утворено за правилом:*

$$\mathtt{X}_{n+1} = 23 + \mathtt{X}_n \pmod{33},$$

тобто кожна наступна буква обчислюється через попередню за допомогою зсуву на 23 та обчислення конгруенції за модулем 33. Перевірити це.

Задача 12. *Вернам фактично запропонував наступну процедуру. Спочатку перевести букви (як повідомлення, так і ключового слова) у десяткові числа; потім записати двійкове представлення для кожного числа, отримавши дві довгі послідовності 0 та 1 (бітів); нарешті, до кожного біта m_i повідомлення застосувати операцію $m_i \oplus k_i$, де k_i — це відповідний біт ключового слова. Тут $x \oplus y = 0$ або 1 в залежності від $x = y$ чи $x \neq y$. Зашифрувати повідомлення* КІТ, *якщо ключовим словом є* ПЕС.

Задача 13. *Підрахувати суми*

$$\sum_{d|12} d, \qquad \sum_{d|12} 1, \qquad \sum_{d|18} \frac{1}{d}, \qquad \sum_{d|18} \frac{18}{d}.$$

Задача 14. *Довести, що якщо*

a) $a|b$ *та* $b|a$, *то* $a = b$;
b) $a|b$ *та* $c|d$, *то* $ac|bd$.

Задача 15. *Довести, що якщо квадрат цілого числа*

a) *є парним, то і саме число є парним*;
b) *є непарним, то і саме число є непарним.*

Задача 16. *Довести, що*

a) *добуток двох послідовних цілих чисел є парним*;
b) $n^2 + n$ *є парним для будь-якого натурального числа* n.

Задача 17. *Довести, що* $2n^3 + 3n^2 + n$ *є парним для будь-якого натурального числа* n.

Задача 18. *Довести, що* $30|(n^5 - n)$ *для будь-якого натурального* n.

Задача 19. *Довести, що різниця квадратів двох натуральних чисел не може дорівнювати 1.*

Задача 20. *Довести, що якщо сума кубів трьох послідовних натуральних чисел є кубом* k^3, *то* $3|k$.

Задача 21. *Які з наступних тверджень є вірними, якщо* a, b, c — *натуральні числа, а* p — *просте?*

a) $(a, b) = (b, a)$ *b)* $(a, b) = (a, a - b)$ *c)* $(a, b) = (a, a - 2b)$
d) $(a, a + 2) = 1$ *e)* $(p, p + 2) = 1$ *f)* $(ac, bc) = c(a, b)$

Задача 22. *Знайти* (a, b), *якщо*

a) $b = 1$ *b)* $b = a$ *c)* $b = a + 1$ *d)* $b|a$
e) $b = a^2$ *f)* $b = a^n$ *g)* $b = na$ *h)* $b = (b, a)$

Задача 23. *Нехай* $a > b$. *Знайти*

a) $(a + b, a^2 - b^2)$; *b)* $(a^2 - b^2, a^4 - b^4)$; *c)* $(a^2 - b^2, a^3 - b^3)$.

Задача 24. *Спростувати твердження*:

a) *якщо* $(a, b) = 1$ *та* $(b, c) = 1$, *то* $(a, c) = 1$;
b) *якщо* $(a, b) = 2$ *та* $(b, c) = 2$, *то* $(a, c) = 2$.

Задача 25. *Довести, що* $(a, a-b) = 1$ *тоді і тільки тоді, коли* $(a, b) = 1$.

Задача 26. *Довести, що якщо* $(a, b) = 1$ *та* $(a, c) = 1$, *то* $(a, bc) = 1$.

Задача 27. *Нехай* n *— будь-яке чотиризначне число, утворене з перестановки десяткових цифр* $0 \le d \le c \le b \le a \le 9$, *не всі з яких є однаковими. Покладемо* $n' = (abcd)_{10}$ *та* $n'' = (dcba)_{10}$. *Значенням функції Капрекара для аргумента* n *називається* $K(n) = n' - n''$. *Наприклад,* $K(1995) = 9951 - 1599 = 8352$.

(a) *Обчислити* $K(K(1995))$;
(b) *довести, що* $K(6174) = 6174$;
(c) *чи існують інші числа* n, *крім* 6174 (*константа Капрекара*), *для яких* $K(n) = n$?

Задача 28. *Нехай* $K^1(n) = K(n)$, *де* K *— це функція, означена в задачі* 27. *Покладемо тепер* $K^2(n)) = K(K(n))$ *и взагалі* $K^m(n) = K(K^{m-1}(n))$ *для довільного* $m \ge 2$. *Перевірити, що* $K^7(2016) = 6174$.

Задача 29. *Абсолютно простим числом називають таке просте число, що кожна перестановка його цифр також є простим числом. Наприклад,* 2, 3 *та* 5 *є абсолютно простими числами.*

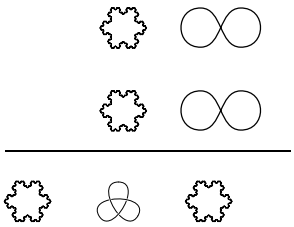
(a) *Існує вісім абсолютно простих чисел, які складаються з двох різних десяткових цифр. Знайти їх.*
(b) *Існує дев'ять абсолютно простих чисел, які складаються з трьох різних десяткових цифр. Знайти їх.*
(c) *Довести, що абсолютно просте число, яке складається з двох або більших десяткових цифр, може складатися лише з десяткових цифр* 1, 3, 7 *або* 9.

Задача 30. *Англійський математик де Морган, який жив у XIX сторіччі, одного разу сказав, що у році* x^2 *йому виповнилось* x *років.*

a) *Коли він народився?*
b) *Чи може таке ж стверджувати математик, який жив у XX сторіччі?*

Задача 31. *Цю задачу в* 1968 *році опублікував М. Гарднер, відомий популяризатор математики, автор численних книг. Ми подаємо переклад оригінального формулювання задачі.*

Астронавти, які досліджують Венеру, знайшли запис домашнього завдання з математики, виконане венеріанським школяром на тему додавання двох чисел у стовбчик:



Числова система венеріанців є схожою на нашу, а основою для неї служить кількість пальців на руці венеріанців. Визначити кількість пальців на руці венеріанських аборигенів.