Тема 3. Арифметика классов вычетов. Шифр сдвига. Аффинный шифр

Теоретическая часть

1. Рассмотрим множество целых чисел $\mathbb{Z}$:
   $\ldots \quad -6 \quad -5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad \ldots$

2. Возьмём некоторое целое число N. Известно, что любое целое число x может быть представлено следующим образом:
   $$x = qN + r,$$
   где N – делитель, q – (неполное) частное, r – остаток. Остаток не может быть отрицательным и не может быть больше делителя:
   $$0 \le r \le N - 1.$$

3. Получается, что все возможные остатки – это числа $0, 1, 2, \ldots, N - 1$.

4. Возьмём, к примеру, $N = 5$. Выпишем под целыми числами их остатки от деления на 5.
   $\ldots \quad -6 \quad -5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad \ldots$
   $\ldots \quad 4 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 0 \quad 1 \quad 2 \quad \ldots$

5. Видно, что остатки циклически повторяются. Можно разбить множество всех целых чисел на подмножества так, что в каждое подмножество попадут числа, имеющие одинаковые остатки от деления на N. Таких подмножеств будет ровно N, и они называются **классами вычетов по модулю** N. К примеру, если $N = 5$, то можно обозначить классы вычетов по модулю 5 так:
   $$\bar{0} \quad \bar{1} \quad \bar{2} \quad \bar{3} \quad \bar{4}$$
   так как остатки – это числа 0, 1, 2, 3, 4.

6. На классах вычетов можно определить арифметические операции. Для этого нужно выполнять обычные арифметические действия с остатками и вместо результата брать остаток от его деления на N. Так, если $N = 5$, то таблицы сложения, вычитания и умножения классов по модулю 5 будут выглядеть следующим образом:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$-$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{4}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

7. По таблице умножения можно искать каждому классу обратный. Класс a' будет обратным к классу a, если $a \times a' = a' \times a = \bar{1}$. Получается, что к $\bar{1}$ обратный $\bar{1}$, к $\bar{2}$ обратный $\bar{3}$, к $\bar{3}$ обратный $\bar{2}$, а к $\bar{4}$ обратный $\bar{4}$, а к $\bar{0}$ обратного не существует.

8. Деление классов можно определить как умножение на обратный: $a \div b = a \times b'$. Получаем таблицу деления:

$\div$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{3}$	$\bar{1}$

9. Используем классы вычетов для того, чтобы определить подстановочные шифры. Данные шифры делятся на **шифры сдвига** и **аффинные шифры**. Представителями шифров сдвига являются шифр Цезаря и шифр Виженера.

10. К примеру, в алфавите N букв, и мы хотим создать шифр Цезаря со сдвигом h. Перенумеруем все буквы алфавита числами от 0 до $N - 1$. Если буква имеет код x, то зашифрованная буква будет иметь код y, который вычисляется по формуле:
    $$y = (x + h) \bmod N.$$

11. Чтобы расшифровать букву с кодом y, пользуются формулой:
$$x = (y - h) \bmod N.$$

12. К примеру, если алфавит [А, О, У, Н, Т], то $N = 5$ и буквы алфавита имеют коды:

А	О	У	Н	Т
0	1	2	3	4

Пусть $h = 3$, тогда соответствие букв:

А	О	У	Н	Т
Н	Т	А	О	У

Вычислим, какой код у зашифрованной буквы О: $y = (1 + 3) \bmod 5 = 4$, это код буквы Т. Чтобы выполнить расшифровку буквы Т, получаем: $x = (4 - 3) \bmod 5 = 1$. Это код буквы О.

13. Аффинный шифр задаётся формулой
$$y = (ax + b) \bmod N,$$
где $\text{НОД}(a, N) = 1$ (это условие важно для однозначной расшифровки). Тогда формула расшифровки:
$$x = \big((y - b)a'\big) \bmod N.$$

14. К примеру, пусть формула шифра $y = (3x + 2) \bmod 5$. Буква О переводится в букву, которая имеет код $y = (3 \cdot 1 + 2) \bmod 5 = 0$, а это А. Расшифровка: $x = \big((0 - 2)\ 3'\big) \bmod 5 = (3 \cdot 2) \bmod 5 = 1$. Это код буквы О.

Практическая часть

Составить компьютерную программу (на любом языке программирования), которая выполняет следующие действия:

1. По заданной текстовой строке, состоящей из символов указанного алфавита, возвращает строку, зашифрованную с помощью аффинного шифра. Параметры a и b задаёт пользователь (не забудьте, что $\text{НОД}(a, N) = 1$).
2. По заданной строке, зашифрованной с помощью аффинного шифра и состоящей из символов указанного алфавита, возвращает строку-оригинал.

В программе предусмотреть:

1. **Модуль**, который содержит структуры, процедуры и функции, которые реализуют арифметику классов вычетов по некоторому модулю.
2. **Основную программу**, которая реализует шифрование и расшифрование.

Дополнение к заданию. Варианты алфавитов и шифруемых строк. Выбирать вариант по последней цифре номера зачётки

Вар	Алфавит	Строка-оригинал
0.	**[А, И, Н, Т, У, _]**	**ТУТ_АННА_И_НАТА**
1.	**[А, О, У, Ы, Н, Т, _]**	**У_АННЫ_НОТЫ**
2.	**[А, О, И, Н, Т, _]**	**НАТА_ИННА_И_АНТОН**
3.	**[О, И, У, Ы, Н, Т, К, _]**	**У_НИКИТЫ_ОКУНИ**
4.	**[А, О, И, У, Н, Т, К, _]**	**У_АНТОНА_ОКУНИ**
5.	**[А, О, У, Н, Т, К, _]**	**А_КОТ_ТУТ_КАК_ТУТ**
6.	**[О, И, У, Н, Т, К, _]**	**НУ_И_КОТИК_КОТОК**
7.	**[О, И, Н, Т, К, _]**	**НИТКИ_ТОНКИ**
8.	**[А, О, И, Н, Т, К, _]**	**НИТКА_И_КОТ**
9.	**[А, О, И, У, Н, Т, К, _]**	**КОТИК_КАТИТ_НИТКУ**

При желании можно запрограммировать атаку прямым перебором по известному N, но неизвестным a и b. Программа перебирает допустимые a и b и выводит дешифрованную строку. Та строка, которая представляет собой осмысленный текст, и есть дешифрованная. К примеру, при $N = 8$ допустимые значения a равны 1, 3, 5, 7, а значения b суть 0, 1, 2, 3, 4, 5, 6, 7. Поэтому будет 32 возможных дешифрованных варианта.