

ZADANIE 1. Szyfrowanie tekstu

Dany jest ciąg znaków, których dziesiętne kody ASCII są w przedziale od 32 do 127 (zob. tabela 1 – strona 35). **Szyfrowanie z kluczem n** polega na zastąpieniu każdego znaku z ciągu znakiem leżącym o n pozycji dalej (w tabeli znaków ASCII) od zastępowanego znaku. Przy szyfrowaniu znaku należy postępować w sposób cykliczny, tzn. po znaku o kodzie 127 przechodzimy do znaku o kodzie 32.

- Podaj znaki i ich kody dziesiętne ASCII otrzymane po zaszyfrowaniu znaku * (o kodzie 42) dla $n = 121$ i $n = 1000$; dla $n = 1000$ podaj sposób otrzymania wyniku.
- Podaj algorytm, który dla dowolnej liczby naturalnej n szyfruje (powyższą metodą) dowolne słowo złożone z m znaków (z tabeli 1).
- Kod znaku równa się 7A w układzie szesnastkowym. Podaj ten kod w układzie binarnym. Czy znak 1 i liczba 1 mają jednakową reprezentację w komputerze? Odpowiedź uzasadnij.

Punktacja:

Części zadania	Maks.
a (dla $n = 121$)	1
(dla $n = 1000$)	2
b	5
c	2
Razem:	10

Znak	Kod	Znak	Kod	Znak	Kod
spacja	32	@	64	`	96
!	33	A	65	a	97
"	34	B	66	b	98
#	35	C	67	c	99
\$	36	D	68	d	100
%	37	E	69	e	101
&	38	F	70	f	102
'	39	G	71	g	103
(40	H	72	h	104
)	41	I	73	i	105
*	42	J	74	j	106
+	43	K	75	k	107
,	44	L	76	l	108
-	45	M	77	m	109
.	46	N	78	n	110
/	47	O	79	o	111
0	48	P	80	p	112
1	49	Q	81	q	113
2	50	R	82	r	114
3	51	S	83	s	115
4	52	T	84	t	116
5	53	U	85	u	117
6	54	V	86	v	118
7	55	W	87	w	119
8	56	X	88	x	120
9	57	Y	89	y	121
:	58	Z	90	z	122
;	59	[91	{	123
<	60	\	92		124
=	61]	93	}	125
>	62	^	94	~	126
?	63	_	95	Del	127

Tabela 1. Znaki i ich dziesiętne kody ASCII

ROZWIĄZANIE

Komentarz. Przedmiotem zadania jest zastosowanie szyfru przestawieniowego z kluczem n . Jest to uogólnienie znanego szyfru Cezara (w tym przypadku $n = 3$). W naszym przypadku, kody zmieniają się co $(127 - 32 + 1) = 96$, gdyż tyle jest dostępnych znaków. Pamiętać przy tym należy, że kody znaków w tabeli 1 rozpoczynają się od 32.

Punkt a.

Znak * o kodzie 42, po przesunięciu o $n = 121$ ma kod 163, czyli odpowiada mu znak w tabeli 1 o kodzie $163 - 127 + 31 = 67$. Jest to litera C.

Taki sam wynik otrzymamy redukując najpierw kody znaków tak, aby rozpoczynały się od 0. Wtedy obliczamy kod znaku przesunięty o n , redukujemy go cyklicznie i na końcu do tak otrzymanego kodu dajemy 32. Dla $n = 121$ mamy zatem: $[(42 - 32) + 121] \bmod 96 + 32 = 131 \bmod 96 + 32 = 35 + 32 = 67$.

Dla $n = 1000$, w podobny sposób otrzymujemy: $[(42 - 32) + 1000] \bmod 96 + 32 = 50 + 32 = 82$. Kod 82 ma w tabeli 1 znak R.

Punkt b.

Algorytm

Dane: n – klucz szyfrowania (liczba naturalna);

$z_1 z_2 z_3 \dots z_m$ – ciąg m znaków z tabeli 1.

Wynik: Zaszifrowanie danego tekstu metodą przestawieniową z kluczem n .

Krok 1. Niech T oznacza zaszyfrowany tekst. Będziemy dopisywać do niego kolejno szyfrowane znaki. Na początku T jest pustym tekstem.

Krok 2. Dla każdego $i = 1, 2, \dots, m$, dopisz do T od końca znak o kodzie (według tabeli 1)

$$32 + [(z_i - 32) + n] \bmod 96$$

Punkt c.

Mamy

$$(7A)_{16} = 7 \cdot 16 + A = 7 \cdot 16 + 10 = (122)_{10} = 64 + 32 + 16 + 8 + 2 = (1111010)_2$$

Znak 1 i liczba 1 nie mają jednakowej reprezentacji w komputerze. Znak 1, jako element napisu (tekstu) ma kod ASCII równy 49 i jest zapisany w jednym bajcie jako 00110001. Natomiast liczba 1, jeśli przeznaczono na nią jeden bajt, to w reprezentacji stałopozycyjnej, jest reprezentowana jako 00000001.

MODEL ODPOWIEDZI I SCHEMAT OCENIANIA

Zasady oceniania

- Za rozwiązanie zadań z arkusza I można uzyskać maksymalnie 40% całkowitej liczby punktów.
- Model odpowiedzi uwzględnia jej zakres merytoryczny, a nie jest ścisłym wzorcem sformułowania (poza odpowiedziami jednowyrazowymi i do zadań zamkniętych).
- Za odpowiedzi do poszczególnych zadań przyznaje się pełne punkty.
- Za zadania otwarte, za które można przyznać jeden punkt, przyznaje się punkt wyłącznie za odpowiedź w pełni poprawną.
- Za zadania otwarte, za które można przyznać więcej niż jeden punkt, przyznaje się tyle punktów, ile prawidłowych elementów odpowiedzi (zgodnie z wyszczególnieniem w kluczu) przedstawił zdający.

Model odpowiedzi i schemat punktowania

Numer zadania	Numer punktu	Oczekiwana odpowiedź	Maksymalna punktacja za część zadania	Maksymalna punktacja za zadanie
1	a	Za poprawną odpowiedź dla $n = 121$ – 1 punkt . Za poprawną odpowiedź dla $n = 1000$ bez uzasadnienia – 1 punkt , za podanie sposobu otrzymania wyniku – 1 punkt .	3	10
	b	Za opisanie metody szyfrowania jednego znaku dla dowolnego n , ale nie w postaci algorytmu – 2 punkty . Za to samo z usterką – 1 punkt . Za opisanie metody zaszyfrowania wszystkich znaków, ale nie w postaci algorytmu – 1 punkt . Za podanie algorytmu szyfrowania jednego znaku dla dowolnego n – 3 punkty . Za to samo z usterką – 1 lub 2 punkty . Za podanie algorytmu zaszyfrowania wszystkich znaków – 2 punkty .	5	
	c	Za podanie binarnego kodu – 1 punkt . Za poprawną odpowiedź na pytanie i uzasadnienie – 1punkt .	2	