



IX ОЛИМПИАДА ПО ИНФОРМАТИКЕ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Задача 1. Алгоритм. (3 балла)

Дана блок-схема алгоритма обработки строки STR (см. рис. 1), в которой функция $length$ возвращает количество символов в строке.

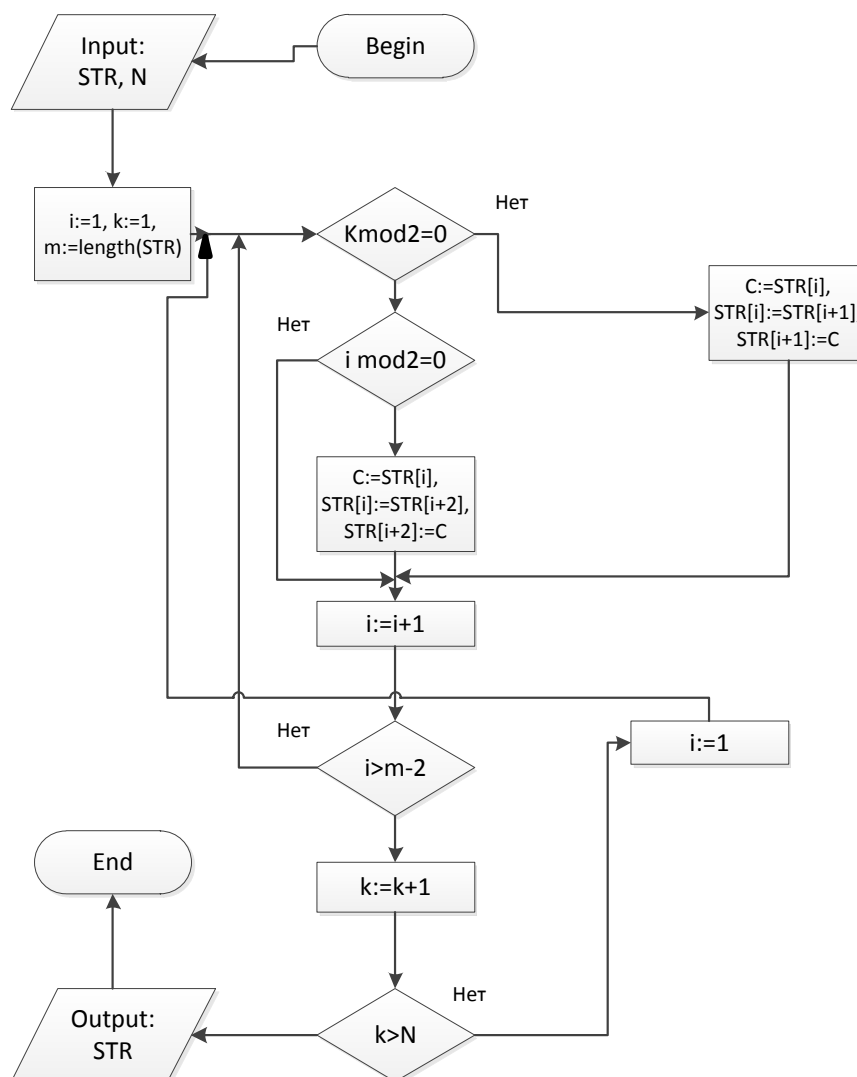


Рис. 1. Блок-схема алгоритма обработки строки STR

Чему была равна переменная STR перед началом выполнения алгоритма, если при $N=10$ в результате обработки было получено значение переменной $STR = \text{'bdieghtreen tre'}$?

Задача 2. Коллизия. (4 балла)

В результате анализа подсистемы защиты удалось выяснить, что подтверждение имени пользователя, работающего за компьютером, осуществляется посредством паролей. Для реализации проверки введенный пароль подвергается преобразованию при помощи функции, исходный код которой также был восстановлен и представлен на языке C (см. рис. 2). Результат работы функции сверяется с эталонами, хранимыми в базе данных, для принятия решения о том верен пароль или нет. Если известно, что пароль «КОНФИДЕНЦИАЛЬНОСТЬ» верен, то можно ли утверждать, что существуют пароли, отличные от указанного, которые пройдут описанную проверку? Если да, то приведите пример такого пароля.

```
int HASH(char *text)
{
    int k=0, H;
    char temp[6], letter = 'G';
    for( ; (k<strlen(text)) && (k<6); ++k) temp[k]=text[k];
    if (k < 6) for( ;k<6;k++) temp[k]= letter;
    H = ((temp[0]+temp[1]+temp[2]) &7) *64;
    H += ((temp[0]+temp[2]+temp[4]) &7) *8;
    H += ((temp[1]+temp[3]+temp[5]) &7);
    return H;
}
```

Рис. 2. Исходный код

Фрагмент таблицы ASCII

hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2		!	“	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	:	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL
8	A	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
9	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Задача 3. Провал. (3 балла)

В штате секретной службы состоят 10 агентов (под номерами 1, 2, ..., 10). Для связи с ними при проведении разведывательной операции используются устройства, которые работают в заданном диапазоне частот, но в них можно настроить индивидуально интенсивность передачи сигнала в минуту (число сигналов в минуту). В случае провала агент отключает передатчик. В штате стоит приёмное устройство, которое считает общее количество пришедших в минуту сигналов от всех агентов. Как надо задать частоты передатчиков, чтобы в штате в случае провалов агентов можно было бы определить их номера.

Задача 4. Стеганография. (5 баллов)

Необходимо реализовать приложение, извлекающее секретное сообщение из входного файла. Известно, что для скрытного внедрения данных используется регистр символа. Если буква в нижнем регистре – это соответствует «0», если буква в заглавном регистре – это соответствует «1». Очередной символ секретного сообщения составляется из 8-ми битов, которые формируют код этого символа. В шифровании используются только буквы русского или английского алфавита. Знаки препинания и цифры не учитываются.

Указание:

Приложение разрабатывается на базе реализованного шаблона чтения из файла (см.*. \\ntofsm\Олимпиада\). Для получения зашифрованного текста необходимо вызвать функцию:

```
void GetCryptoText(char *massiv, int *resultlen);
```

massiv – указатель на массив символов, который будет заполнен сообщением после возврата из функции (не менее 500 байт);

resultlen – указатель на целочисленную переменную, которая будет равна количеству байт, записанных в *massiv* во время выполнения функции.

Декодированное сообщение необходимо вывести на консоль.

Если необходимо проверить, является ли символ буквой, используйте функцию

```
int iswalpha(unsigned char c);
```

Для перевода символов в верхний и нижний регистр используйте функции

```
int towupper(unsigned char c);
```

```
int towlower(unsigned char c);
```

Строки, содержащие русские буквы, должны быть объявлены как *unsigned char*.

Заметим, что если вы работаете со средой разработки *Visual Studio*, то необходимо обратить внимание на настройку проекта (правой кнопкой на проекте, «Свойства»): параметр «*Character Set*» должен быть установлен в «*Use Multi-Byte Character Set*».

* для разработки с помощью *MS Visual Studio* используйте шаблон в папке *../For Visual Studio/*, а для среды *CodeBlock* – в папке *../For CodeBlock/*

Задача 5. Шифрование. (4 балла)

Иван написал Егору сообщение и закодировал его, используя таблицу 1.

Таблица 1

№	СИМВОЛ	КОД	№	СИМВОЛ	КОД	№	СИМВОЛ	КОД
1	<i>а</i>	010	12	<i>к</i>	100	23	<i>х</i>	110101
2	<i>б</i>	000	13	<i>л</i>	0111100	24	<i>ц</i>	110110
3	<i>в</i>	011000	14	<i>м</i>	0111101	25	<i>ч</i>	110111
4	<i>г</i>	011001	15	<i>н</i>	0111110	26	<i>ш</i>	111000
5	<i>д</i>	101	16	<i>о</i>	0111111	27	<i>щ</i>	111001
6	<i>е</i>	011010	17	<i>п</i>	110000	28	<i>ъ</i>	111010
7	<i>ё</i>	011011	18	<i>р</i>	001	29	<i>ы</i>	111011
8	<i>жс</i>	0111000	19	<i>с</i>	110001	30	<i>ь</i>	111100
9	<i>з</i>	0111001	20	<i>т</i>	110010	31	<i>э</i>	111101
10	<i>и</i>	0111010	21	<i>у</i>	110011	32	<i>ю</i>	111110
11	<i>й</i>	0111011	22	<i>ф</i>	110100	33	<i>я</i>	111111

В результате была получена последовательность бит открытого текста $O(i)$, $i=1, \dots, 33$. Затем Иван произвёл преобразование $S(i) = (O(i) + S(i - 1)) \bmod 2$, $S(0)=0$ (см. рис. 2). В результате чего была получена последовательность бит шифрованного текста $S(i)$, $i=0, \dots, 33$:

0011111110011000011001100000001100.

Какое сообщение Иван написал Егору?

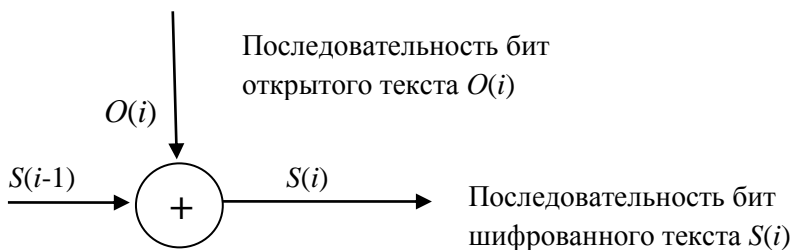


Рис. 2. Схема преобразования закодированного сообщения