Lucrare de laborator nr. 1

1.1. Шифр Цезаря

В этом шифре каждая буква открытого текста заменяется новой буквой, полученной сдвигом по алфавиту. Секретный ключ k, одинаковый для шифрования и для дешифрования, представляет собой число, обозначающее алфавитный сдвиг, т. е. $k \in \{1, 2, 3, \ldots, n-1\}$, где n – длина алфавита. Шифрование и дешифрование сообщения шифром Цезаря можно определить по формулам

$$c = e_k(x) = x + k \pmod{n},$$

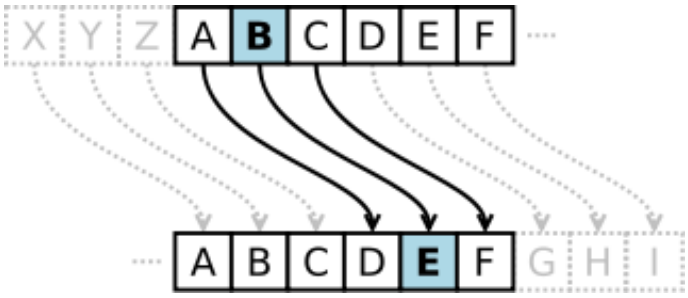
$$m = d_k(y) = y - k \pmod{n},$$

где x и y - числовое представление соответствующего символа открытого текста m и криптограммы c. Функция, называемая *Modulo* (a mod b), возвращает остаток от деления целого числа a на целое число b. Этот метод шифрования называется в честь Юлия Цезаря, который использовал его для связи со своими генералами, используя ключ $k = 3$ (табл. 1).

Например, для $k = 3$ имеем

$$e_k(\text{S}) = 18 + 3 \pmod{26} = 21 = \text{V}$$

$$d_k(\text{V}) = 21 - 3 \pmod{26} = 18 = \text{S}$$



В этом случае для m =„*cifrul cezar*”, получаем c =„*fliuxo fhcdu*”.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
D	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

Таблица 1. Шифр Цезаря с ключом $k = 3$

Шифр Цезаря очень легко взломать, так что это очень слабый шифр. Таким образом, криптоаналитик может узнать исходный текст, перепробовав все 25 ключей. Неизвестно,

насколько полезным был шифр Цезаря, когда его использовал его создатель, но, вероятно, он был достаточно хорошим в то время, поскольку лишь немногие из врагов Цезаря умели писать и читать, не говоря уже про их познания в криптографии и криптоанализе.

Задание 1.1. **Реализовать алгоритм Цезаря для английского алфавита на одном из языков программирования. Используйте только кодировку букв, как показано в Таблице 1 (кодировки, указанные в языке программирования, например, ASCII или Unicode, использовать нельзя). Значения ключей будут находиться в диапазоне от 1 до 25 включительно, и никакие другие значения не допускаются. Значения текстовых символов находятся между «A» и «Z», «a» и «z», и никакие другие значения не допускаются. Если пользователь введет другие значения – ему будет подсказан правильный диапазон. Перед шифрованием текст будет переписан заглавными буквами, а пробелы удалены. Пользователь сможет выбрать операцию - *шифрование* или *дешифрование*, сможет ввести *ключ*, *сообщение* или *криптограмму* и получит соответственно *криптограмму* или *расшифрованное сообщение*.**

1.2. Шифр Цезаря + перестановка

Из-за низкой криптостойкости шифра Цезаря, в основном из-за пространства ключей, состоящего всего из 25 различных ключей для латинского алфавита, его можно взломать последовательной проверкой всех ключей (метод полного перебора ключей). Если сообщение было зашифровано шифром Цезаря, то один из ключей даст нам читаемый текст на том языке, на котором было написано сообщение.

Например, если

$$m = \texttt{BRUTE FORCE ATTACK}$$

это сообщение, написанное на английском языке и зашифрованное с помощью ключа

$$k = 17,$$

мы получаем криптограмму (шифрограмму)

$$c = \texttt{SILKVWFITVRKKRTB}$$

Если криптоаналитик перехватит зашифрованное сообщение и переберет все ключи 1, 2, ..., 25 - он получит следующее:

1	RHKJUVEHSUQJJQSA
2	QGJITUDGRTPIIPRZ
3	PFIHSTCFQSOHHOQY
4	OEHGRSBEPRNGGNPX
5	NDGFQRADOQMFFMOW
6	MCFEPQZCNPLEELNV

7	LBEDOPYBMOKDDKMU
8	KADCNOXALNJCCJLT
9	JZCBMNWZKMIBBIKS
10	IYBALMVYJLHAAHJR
11	HXAZKLUXIKGZZGIQ
12	GWZYJKTWHJFYYFHP
13	FVYXIJSVGIEXXEGO
14	EUXWHIRUFHDWWDFN
15	DTWVGHQTEGCVVCEM
16	CSVUFGPSDFBUUBDL
17	**BRUTEFORCEATTACK**
18	AQTSDENQBDZSSZBJ
19	ZPSRCDMPACYRRYAI
20	YORQBCLOZBXQQXZH
21	XNQPABKNYAWPPWYG
22	WMPOZAJMXZVOOVXF
23	VLONYZILWYUNNUWE
24	UKNMXYHKVXTMMTVD
25	TJMLWXGJUWSLLSUC

Как видите, на английском языке имеет смысл только текст, полученный с помощью ключа $k = 17$, поэтому сообщение, соответствующее криптограмме, имеет вид

m = **BRUTEFORCEATTACK.**

Чтобы повысить криптографическую стойкость шифра Цезаря, вы можете применить перестановку алфавита, применяя ключевое слово (не путать с основным ключом шифра). Этим ключом может быть любая последовательность букв алфавита, а не только слово из словаря.

Пусть второй ключ k_2=***cryptography***. Применяем этот ключ к алфавиту:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

и получаем:

C	**R**	**Y**	**P**	**T**	**O**	**G**	**A**	**H**	B	D	E	F	I	J	K	M	L	N	Q	S	U	V	W	X	Z

Мы получили этот новый порядок букв алфавита, поместив буквы k_2 в начале, а затем другие буквы алфавита в их естественном порядке. Будем иметь в виду, что буквы не должны повторяться, т.е. если буква встречается несколько раз, то ставится только один раз.

Далее применяется шифр Цезаря с учетом нового порядка алфавита:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	**R**	**Y**	**P**	**T**	**O**	**G**	**A**	**H**	B	D	E	F	I	J	K	M	L	N	Q	S	U	V	W	X	Z
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
P	**T**	**O**	**G**	**A**	**H**	B	D	E	F	I	J	K	M	L	N	Q	S	U	V	W	X	Z	**C**	**R**	**Y**

Таблица 2. Шифр Цезаря с ключом k_1=3 и k_2=*cryptography*

Так как существует 26!= 403291461126605635584000000 перестановок букв латинского алфавита, количество ключей для этой версии алгоритма будет

$$26! \cdot 25 = 10082286528165140889600000000,$$

что усложняет взлом методом полного перебора ключей, но не спасает от атаки анализом частот.

Задание 1.2. **Реализовать двухключевой алгоритм Цезаря, соблюдая условия, изложенные в Задании 1.1. Кроме того, ключ 2 должен содержать только буквы латинского алфавита и иметь длину не менее 7.**

Задание 1.3. **Для этого задания учащиеся разбиваются на пары. Каждый из них будет шифровать сообщение, состоящее из 7-10 символов (без пробелов и написанных только заглавными буквами) версией шифра Цезаря с перестановкой. Каждый выбирает свои ключи. Полученные таким образом криптограммы будут переданы коллеге вместе с соответствующими ключами. Каждый из двух выполняет дешифрование, а потом оба сравнивают результаты с исходной версией напарника.**

Итоговый отчет будет загружен в ELSE в установленный преподавателем срок. Каждая неделя просрочки штрафуется одним баллом отметки.