Лабораторная работа №1

Тема: Классические шифры
(срок выполнения – 2 недели)

Введение: В данной лабораторной работе вам необходимо реализовать два классических шифра. Это могут быть (в зависимости от варианта):

- Шифр простой замены;
- Аффинный шифр;
- Шифр Хилла;
- Шифр Виженера.

Данные шифры не отличаются высокой криптостойкостью, однако хорошо иллюстрируют приемы, которые могут применяться для шифрования сообщений. Лабораторные работы сдаются очно, за день до сдачи лабораторной работы нужно сбросить код преподавателю (до 00:00). Почта: lolita.harmatnaya@gmail.com

Алфавит: Во всех заданиях (в том числе и бонусных) используется одинаковый алфавит: 33 заглавные русские буквы от «А» до «Я» («АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ»). В открытом тексте удаляются все пробелы и знаки препинаний.

Шифр простой замены: В качестве ключа задается вторая строка подстановки: она должна содержать все символы алфавита, записанные в произвольном порядке по одному разу каждый.

Аффинный шифр: В качестве ключа задается ключевая пара (a, b), где $\text{НОД}(a, 33) = 11$ и $\{a, b\} \in Z_{33}$.

Шифр Хилла: В качестве ключа задается матрица 2 × 2, все элементы которой лежат в кольце Z_{33}, а определитель по модулю 33 не равен 0 и взаимно простой с 33. Матрица указывается построчно. Для шифрования следует умножать вектор с открытым текстом на матрицу-ключ, а для расшифрования – вектор с шифртекстом на обратную матрицу ключа.

Шифр Виженера: В качестве ключа задается строка произвольной длины, состоящая из символов алфавита.

Условие лабораторной работы: Ваша задача – реализация двух классических шифров согласно вашему варианту (первый шифр смотрите в таблице № 1, второй – в таблице №2).

Отчет: Реализовав шифры, вам необходимо продемонстрировать их работу, зашифровав открытый текст из таблицы №1 и расшифровав шифртекст из таблицы №2, согласно вашему варианту. В отчете указать полученные результаты и способ их получения: или программу, которую вы написали, или вручную с иллюстрацией вычислений (можно просто вставить фото). Сторонними готовыми программами, сайтами, реализованными функциями и пр. пользоваться можно лишь для самопроверки. Можно использовать любой язык программирования. Варианты распределяются согласно порядковому номеру в списке группы.

Таблица №1: Зашифровать текст согласно вашему варианту

№ вар.	Шифр	Ключ	Открытый текст
1.	Простой замены	ЫЗЁДТЖЭОМБНЬШРСЙФЯВПХУЕКИЮЦЛЩАЧГЪ	В КАЧЕСТВЕ ОТКРЫТОГО ТЕКСТА БЕРЕТЕ ВАШУ ФАМИЛИЮ
2.	Аффинный	7 17	
3.	Хилла	7 1 7 6	
4.	Виженера	АЭХ	
5.	Простой замены	ЛОРЬШЦКЧИСНМВЗХЪАДЯГЮБУФЁЙЫЭТЕПЖЩ	
6.	Аффинный	25 27	
7.	Хилла	14 16 13 4	
8.	Виженера	СЬТ	
9.	Простой замены	СЕЭШБВЁИЛОЧЫКЩУХЮДЪЙНЗФАЬГЖРМПЯТЦ	
10.	Аффинный	14 18	
11.	Хилла	32 3 18 17	
12.	Виженера	ОЮВ	
13.	Простой замены	ЩИМПДОШХЭБЗРЫТЪГЦЬЧНСЙКЯВАУЕЖФЛЁЮ	
14.	Аффинный	4 4	
15	Хилла	9 28 31 29	
16	Виженера	ШДФ	
17	Простой замены	ЧЩЮОНИФЛАУЭЗХБДЪЬГЯМЫВКСЕПЁТЖШЙРЦ	
18	Аффинный	10 20	
19	Хилла	17 16 5 12	
20	Виженера	ЩЁЙ	
21	Простой замены	ЭЫНФЗАУЮСРЕХКШВТЩЪЙМИДЧЬОБЦЖЛГЁЯП	
22	Аффинный	2 5	
23	Хилла	9 31 17 14	

Таблица №2: Расшифровать текст согласно вашему варианту

№ вар.	Шифр	Ключ	Шифротекст
1.	Аффинный	16 26	НЖБТВИЛУЫ

2.	Виженера	ХИШ	ДЮЖЗЦБАРШЁИАИХЖВ
3.	Простой замены	ЬУЦХЩШГЖДВЙЧОСНЭЪЫРЮМФКПИАБЁТЕЯЛЗ	СЬНЩЬОЭЫШП
4.	Хилла	24 32 20 7	ЧЦЪЪСДЫИЪЛГНЪНФП
5.	Виженера	ЁЪЬ	ГДХФКЙЕ
6.	Хилла	23 25 15 5	ФИЫЬЬЦХРВХЁЛ
7.	Аффинный	28 20	ЬЫФЫГПЛГОБУЮ
8.	Простой замены	ФЖЩПЪАДЯИКЧТБЦЬЗСЕЫШВНЙЭУОГХЮМРЛЁ	РСКЪАЦКЁ
9.	Хилла	20 4 32 9	СУЕНВРЬЯЦД
10.	Простой замены	ЙЛТРЖЯШНБАЮГЧЭОЩЪФЕИКЦЁПЗСХМУЫДВЬ	ФАГАЭЩФИА
11.	Виженера	ИЪЕ	ЪИРЦРЙЪМУЗЗНН
12.	Аффинный	2 24	ЩШЧЁТЧХИЪЬФШИХ
13.	Простой замены	БЯАТДНКЛЁЦГПЕЪСФШЙИЬОУЖЗЫЩЧРЮЭХВМ	ФДСБЛДЮАТФЕЕЦАОДН
14.	Аффинный	25 12	ПЛЗЛНЁШТ
15.	Хилла	21 20 11 30	ЁЦФЮЗЮ
16	Виженера	ЩЭП	ЪЛЫХЁБЕЭСЩ
17	Аффинный	2 30	ЪФЖШХЫТЪКЭ
18	Виженера	НЧМ	ЦЗШНЕРТН
19	Простой замены	ФУЕГЭЪРЩКСЗИШЮЯЧПНЛБАЙЦЫМХОЁЬТЖВД	ЭЧЛЬФБТЯЧЩС
20	Хилла	8 4 10 19	ГРЯЕЛМ
21	Виженера	БФН	ХГЮЕДЮПЖЦГИТСЕНСЭ
22	Хилла	27 16 4 30	ОЭПФЛД
23	Аффинный	19 15	ЩОХФМОРЮОЗУКЛ