

Лабораторная работа 1. Классические шифры.

В данной лабораторной работе вам необходимо реализовать зашифрование и расшифрование двумя классическими шифрами. Зашифровать текст согласно вашему варианту.

№ вар.	шифр	ключ	открытый текст
1.	Простой замены	Б И У З Р О Ы Э Б Х Г Ш Т Ц Н Ё К Ж П Л В Щ Ч Й М Ю С Я Ъ Д Ф А Е	криптография
2.	Аффинный	2 14	математика
3.	Хилла	26 30 20 32	криптологи
4.	Виженера	И Е Ю	шифртекст
5.	Простой замены	Г Л Ф Ы З Ш Б Ж Х Ё П В Ч Н К Ъ Э Д Ъ Р Е Т С А М Ю Ц Ц Я У И О Й	конфиденциальность
6.	Аффинный	10 25	криптоанализ
7.	Хилла	6 14 2 7	статистика
8.	Виженера	Н Ц Р	целостность
9.	Простой замены	С П Г Ё И Ф Ц У Л Х М К Щ Ы Ъ В О Ю Э Н Д Т Я Ъ Й З Ш Ж Б Е Ч А Р	доступность
10.	Аффинный	17 24	криптосистема
11.	Хилла	25 25 18 22	надежность
12.	Виженера	Я Ъ А	инволюция
13.	Простой замены	Б Я Ж Ъ Н В Щ Г З П К Ш Ъ Д О М Ё Й Ц И Ч У Ы О А Э Е Т Л С Х Р Ф	фальсификация
14.	Аффинный	31 25	нарушение
15.	Хилла	8 10 4 1	стеганография

Расшифровать текст согласно вашему варианту

№ вар.	шифр	ключ	Ш и ф р текст
1.	Аффинный	29 29	Б Ю И Н Л Ц Щ Ё
2.	Виженера	Щ Д Р	Ё Д Ю Э Д Б В С
3.	Простой замены	Ъ З Й Ц Л Ш У И Р Д Ч Ё С Ф Е Т Ц Э М А В П Я Б Ъ Ж Ю О Х Н Ъ Г К	Ъ З Э Д Ё Т М

4.	Хилла	16 29 1 22	ВКУРДХГЁ
5.	Виженера	ЛБВ	ЛИКШЙПЛ
6.	Хилла	15 8 31 26	ОЗЦНИЬЁЖ
7.	Аффинный	17 27	ЛТМЯВФТДУ
8.	П р о с т о й замены	ЧТАЮШДНЫСХФЬУЁЭЦВЕКЛИЪЯМЗОЙГЖЩРБ П	ЮИЧФПАЧ
9.	Хилла	30 4 16 10	БУЙЮЁХИЯ
10.	П р о с т о й замены	ИЮЧЬЩЁЗМШСХУРЦЭЬИНФДБТВЛГАПЯЕОЖК Й	ЩМЁУТНБД
11.	Виженера	ЩКЁ	ЖПРЛКЦВШ
12.	Аффинный	20 13	ВМЬЙЭНХЯ
13.	Хилла	11 7 24 26	ХУВСПЖЁБ
14.	Виженера	ЁЭТ	ТЭАИЛДШЭА
15.	Аффинный	17 20	МУЙУЛЗИЩК

Комментарий по поводу ключей:

1. Шифр простой замены - указана вторая строка подстановки
2. Аффинный шифр – указаны коэффициенты в следующем порядке (a , b)
3. Шифр Хилла – матрица 2 на 2 указана построчно
4. Шифр Виженера – трехсимвольный ключ