Практическое занятие №1.
Криптоанализ классических шифров

Шифры перестановки, шифры замены.
Примеры шифрования и дешифрования.

Шифр Цезаря

Шифр Цезаря относится к группе так называемых ***одноалфавитных шифров*** подстановки. При использовании шифров этой группы «каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита». Способы выбора ключей могут быть различны. В шифре Цезаря ключом служит произвольное число **k**, выбранное в интервале от **1** до **25**. Каждая буква открытого текста заменяется буквой, стоящей на **k** знаков дальше нее в алфавите. К примеру, пусть ключом будет число **3**. Тогда буква **A** английского алфавита будет заменена буквой **D**, буква **B** — буквой **E** и так далее.

Для наглядности зашифруем слово **HABRAHABR** шифром Цезаря с ключом **k=7**. Построим таблицу подстановок:

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
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g

И заменив каждую букву в тексте получим: C ('HABRAHABR', 7) = 'OHIYHOHIY'.

При расшифровке каждая буква заменяется буквой, стоящей в алфавите на k знаков раньше: D ('OHIYHOHIY', 7) = 'HABRAHABR'.

Криптоанализ шифра Цезаря Малое пространство ключей (всего 25 вариантов) делает простой перебор самым эффективным и простым вариантом атаки. Для вскрытия необходимо каждую букву шифртекста заменить буквой, стоящей на один знак левее в алфавите. Если в результате этого не удалось получить читаемое сообщение, то необходимо повторить действие, но уже сместив буквы на два знака левее. И так далее, пока в результате не получится читаемый текст.

Шифр простой замены

Шифр простой замены относится к группе ***одноалфавитных шифров подстановки***. Ключом шифра служит перемешанный произвольным образом алфавит. Например, ключом может быть следующая последовательность букв: XFQABOLYWJGPMRVIHUSDZKNTEC.

При шифровании каждая буква в тексте заменяется по следующему правилу: Первая буква алфавита замещается первой буквой ключа, вторая буква алфавита — второй буквой ключа и так далее. В нашем примере буква **A** будет заменена на **X**, буква **B** на **F**.

При расшифровке буква сперва ищется в ключе и затем заменяется буквой стоящей в алфавите на той же позиции.

Криптоанализ шифра простой замены

Пространство ключей шифра простой замены огромно и равно количеству перестановок используемого алфавита. Так для английского языка это число составляет 26! = 288. Разумеется наивный перебор всех возможных ключей дело безнадежное.

Выбирается случайная последовательность букв — основной ключ. ***Шифртекст*** расшифровывается с помощью основного ключа. Для получившегося текста *вычисляется коэффициент*, характеризующий вероятность принадлежности к естественному языку.

Основной ключ подвергается небольшим изменениям (перестановка двух произвольно выбранных букв). Производится расшифровка и вычисляется коэффициент полученного текста.

Если коэффициент выше сохраненного значения, то основной ключ заменяется на модифицированный вариант.

Шаги 2-3 повторяются пока коэффициент не станет постоянным.

Для вычисления коэффициента используется еще одна характеристика естественного языка —***частота встречаемости триграмм***. Чем ближе текст к английскому языку тем чаще в нем будут встречаться такие триграммы как **THE**, **AND**, **ING**. Суммируя частоты появления в естественном языке всех триграмм, встреченных в тексте получим коэффициент, который с большой долей вероятности определит текст, написанный на естественном языке.

Задание

1. Ниже два шифртекста одного и того же сообщения, зашифрованные с помощью классических шифров:

a. Цезарь - Шифртекст 1.

Srobdoskdehwlf vxevwlwxwlrq flskhuv

b. простой замены - Шифртекст 2.

KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn

Напишите программу дешифрования, используя любой известный вам язык программирования:

- найдите соответствующий открытый текст, вскрыв шифр Цезаря,
- а затем найдите *ключ шифра простой замены*, используя для дешифрования известный открытый текст.

Обе атаки должны быть полностью описаны.

2. Напишите программу, используя любой известный вам язык программирования:
   - зашифруйте свою фамилию, имя отчество
   - дешифруйте полученный текст
   - сравните с исходным текстом
3. Подготовьте отчет, включая задание, код программы, скриншоты, результаты работы программы.