Практическое занятие №3.

Шифрование, дешифрование информации с применением криптографических алгоритмов гаммирования
Примеры шифрования и дешифрования.

Гаммирование

Гамми́рование (или Шифр XOR) — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа GF(2) суммирование принимает вид операции «исключающее ИЛИ (XOR)».

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на открытые данные обратимым образом, например, используя операцию "Исключающего ИЛИ" –

a Å b = 1, если a ¹ b;

a Å b = 0 если a = b.

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей.

При определённые свойствах гаммы метод шифрования является абсолютно стойким (то есть не поддающимся взлому).

Доказательство Шеннона.

Пусть X, Y и Z — дискретные случайные величины.

Пусть:

X — значение бита открытого текста; то есть, переменная X (бит) способна принимать два значения: 0 и 1;

p — вероятность события, заключающегося в том, что переменная X примет значение 0;

(1-p) — вероятность противоположного события (то есть, вероятность того, что переменная X примет значение 1).

Запишем закон распределения значений X:

X	**0**	**1**
Pi	p	1-p

Используем p и (1-p), так как вероятность встретить одну букву в разных словах различна.

Пусть:

Y — бит псевдослучайной последовательности (гаммы); то есть, переменная Y (бит) способна принимать два значения: 0 и 1;

каждое из значений Y равновероятно; то есть, вероятности получить 0 или 1 равны 1/2.

Запишем закон распределения значений Y:

Y	**0**	**1**
Pi	1/2	1/2

Иными словами, в качестве гаммы (Y) подаётся одинаковое количество нулей и единиц, или значения переменной Y имеют симметричный закон распределения.

Пусть:

Z — бит закрытого текста; то есть, переменная Z (бит) способна принимать два значения: 0 и 1;

значение Z вычисляется на основе значений X и Y по формуле:

$Z = X+Y \pmod 2$
или
$Z = \mathrm{xor}(X, Y)$
или
$Z = X \oplus Y$

Найдём следующие вероятности:

P(Z=0) — вероятность события, заключающегося в том, что переменная Z принимает значение 0;

P(Z=1) — вероятность события, заключающегося в том, что переменная Z принимает значение 1.

Используем формулы:

сложения вероятностей несовместных событий:

$P (A + B) = P (A) + P (B)$ {\displaystyle P(A+B)=P(A)+P(B)} {\displaystyle P(A+B)=P(A)+P(B)};

умножения вероятностей независимых событий:

$P (A * B) = P (A) * P (B)$ {\displaystyle P(A*B)=P(A)*P(B)} {\displaystyle P(A*B)=P(A)*P(B)}.

Вероятность того, что переменная Z примет значение 0:

$$P(Z=0)=P(X=0,Y=0)+P(X=1,Y=1)=P(X=0)*P(Y=0)+P(X=1)*P(Y=1)=p*1/2+(1-p)*1/2=1/2$$

$$P(Z=0)=P(X=0,Y=0)+P(X=1,Y=1)=P(X=0)*P(Y=0)+P(X=1)*P(Y=1)=p*1/2+(1-p)*1/2=1/2.$$

Вероятность того, что переменная Z примет значение 1:

$$P(Z=1)=1-P(Z=0)=1/2$$

$$P(Z=1)=1-P(Z=0)=1/2.$$

Так как P(Z=0) и P(Z=1) не зависят от p, p может принимать любое значение.

Запишем закон распределения значений переменной **Z**:

Z	**0**	**1**
Pi	1/2	1/2

Закон распределения **Z** оказался симметричным, как и закон распределения гамма (**Y**) или шум. То есть, **Z** не содержит никакую информацию из **X** (в **Z** нет **p**). Это доказывает, что шифр является абсолютно стойким.

Требования к гамме

Для шифрования каждого нового сообщения нужно использовать новую гамму. Повторное использование гаммы недопустимо ввиду свойств операции «xor». Рассмотрим пример: с помощью одинаковой гаммы Y зашифрованы два открытых текста X_1 и X_2, получено две шифрограммы Z_1 и Z_2:

$$Z_1 = X_1 \oplus Y$$
$$Z_2 = X_2 \oplus Y$$

Выполним сложение двух шифрограмм, используя операцию «xor»:

$$Z_1 \oplus Z_2 = (X_1 \oplus Y) \oplus (X\ 2 \oplus Y) = X_1 \oplus X_2$$

Результат зависит от открытых текстов X_1 и X_2 и не зависит от гаммы Y. Ввиду избыточности естественных языков результат

поддаётся частотному анализу, то есть открытые тексты можно подобрать, не зная гамму Y.

Для формирования гаммы (последовательности псевдослучайных чисел) нужно использовать аппаратные генераторы случайных чисел, основанные на физических процессах. Если гамма не будет случайной, для получения открытого текста потребуется подобрать только начальное состояние (англ. seed) генератора псевдослучайных чисел.

Длина гаммы должна быть не меньше длины защищаемого сообщения (открытого текста). В противном случае для получения открытого текста потребуется подобрать длину гаммы, проанализировать блоки шифротекста угаданной длины, подобрать биты гаммы.

Задания

1. Написать программу генерации шифра для заданных, a и s по формуле:

$$Ci = (a\ Pi + s) \bmod N,$$

где

P – порядковый номер символа открытого текста ($0 \le Pi \le N-1$);

C – порядковый номер символа зашифрованного текста ($0 \le Ci \le N-1$);

N – размер алфавита;

a – десятичный коэффициент;

s – коэффициент сдвига.

Напишите программы шифровки и расшифровки для метода моноалфавитной подстановки по заданному шифру.

Язык русский.

Шифр, открытый текст и зашифрованный текст должны быть в текстовых файлах с кодировкой ASCII.