Лабораторная работа №3
Одноключевая система шифрования Диффи и Хеллмана

Задание:

Построить систему шифрования Диффи и Хеллмана для a=(количество согласных букв в фамилии студента), p больше или равно количеству всех букв в фамилии. Подобрать a и p самостоятельно методом проб и ошибок, выбрать два секретных числа X_i и X_j и для связи пользователей сети i и j вычислить числа Z_{ij} и Z_{ji}.

Описание метода.

Диффи и Хеллман реализовали идею использования функций с лазейкой для построения криптосистемы в сети с открытым распределением ключей. Для решения этой задачи они предложили использовать функцию $F(x) = a^x \bmod p$, где p – большое простое число, x – произвольное натуральное число из множества $\{1,2,...,(p-1)\}$, a – целое число из множества $\{2,3,...,p\}$, для которого выполняется требование, чтобы все степени a от 1 до $(p-1)$ в произвольном порядке по модулю p дали все числа из множества $\{1,2,...,(p-1)\}$.

Например, при модуле $p=7$ можно выбрать $a=3$ ($f(1)=3^1 (\bmod 7)=3$, $f(2)=3^2 \bmod 7=2$, $f(3)=3^3 (\bmod 7)=6$, $f(4)=3^4 (\bmod 7)=4$, $f(5)=3^5 (\bmod 7)=5$, $f(6)=3^6 (\bmod 7)=1$)

Предполагается, что всем пользователям сети известны a и p. Пользователь i случайным образом выбирает число x_i (свою лазейку), т.е. секретное число известное только ему из множества $\{1,2,...,(p-1)\}$. Далее он вычисляет $y_i = a^{xi} (\bmod p)$ и помещает его в открытый для доступа всех пользователей сети справочник. При желании установить секретную связь с пользователем j он берет из справочника его число y_j и с помощью своего секрета x_i для обмена сообщениями с j вычисляет ключ $Z_{ij} = (y_i)^{x_i} (\bmod p)$. После установления контакта аналогичную работу проделывает пользователь j, который с помощью своего секретного числа x_j вычисляет $Z_{ji} = (y_i)^{xj} \bmod p$. Ограничения, наложенные на выбор a, обеспечивают получение равенства $Z_{ij} = Z_{ji}$, т.е. одинаковых ключей для обмена сообщениями. В самом деле, $Z_{ij} = y_j^{xi} \bmod p = (a^{xj})^{xi} \bmod p = a^{xjxi} \bmod p$ и $Z_{ji} = a^{xixj} (\bmod p)$.

Пример ($p=7, a=3, x=\{1,2,3,4,5,6\}$

$x_i = 3$ (секрет i) $y_i = 3^3 \bmod 7 = 6$

$x_j = 4$ (секрет j) $y_j = 3^4 \bmod 7 = 4$

$Z_{ij} = 4^3 \bmod 7 = 1$

$Z_{ij} = 6^4 \bmod 7 = 1296 \bmod 7 = 1$

Цифра 1 может означать некоторую функцию, которая используется при кодировании; страницу в заранее разосланных пользователям материалах и т.д.

Недостаток описанной криптосистемы с открытым распространением ключей состоит в том, что она требует абсолютного доверия партнеров по связи друг к другу, так как в этой одноключевой системе они могут изменять переданный текст. Поэтому она непригодна, например, для не доверяющих друг

другу удаленных абонентов.Вычисление остатков x при делении целых чисел на модуль y можно выполнять с помощью функции mod(x,y).