конструировании технических устройств, выборе экономической стратегии и при лечении больного.

Таким образом, нейрокомпьютеры являются перспективным направлением развития современной высокопроизводительной вычислительной техники, а теория нейронных сетей представляет собой приоритетные направления вычислительной науки, и при соответствующей поддержке интенсивно развиваются.

Литература

1. Журнал «Нейрокомпьютеры: разработка, применение», ISSN 1999-8554
2. Горбань А. Н., Россиев Д.А., Нейронные сети на персональном компьютере:Наука,1996.—276с. DOI: 10.13140/RG.2.1.4114.1600.

УДК 512.642.95:378.147.091.3

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА RSA

Русевич О.А.
Ассистент Крупенкова Т.Г.
Белорусский национальный технический университет

Криптосистема RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм шифрования данных с открытым ключом. Открытый ключ – это информация, помогающая расшифровать сообщение, передающаяся по незащищенным каналам.

RSA основывается на использовании односторонних функций, у которых, при известном значении аргумента x, легко вычислить значение функции f(x), но при известном значении y=f(x), найти значение x невозможно за разумный интервал времени.

Для шифрования исходного сообщения, например “код”, его необходимо привести к цифровому значению. Согласно правилу шифрования RSA, этим числом будет c= 111505. Число соответствует номерам букв в алфавите. Далее выбираются два простых числа p = 61 и q = 89. Находится их произведение $n = p \cdot q = 5429$, причем НОД (c, n) =1. Находим функцию Эйлера от n, $\phi(n) = (p-1)(q-1) = 5280$. Выбираем такое простое число e, что НОД (e, $\phi(n)$) = 1, допустим e = 79.

Если c > n, то сообщение разбивается на блоки c_1 и c_2, такие, что $0 < c_i < n$, c_1 и c_2 возьмем 111 и 505 соответственно. Также запишем *e* в двоичной системе $79_{10} = 1001111_2 = 2^6+2^3+2^2+2+1$.

Тогда блок c_1 шифруется следующим образом:

$111 \equiv 111 (\mathrm{mod}\ 5429)$; $111^2 \equiv 111^2 = 12321 \equiv 1463 (\mathrm{mod}\ 5429)$; $111^4 \equiv 1463^2 = 2140369 \equiv 1343 (\mathrm{mod}\ 5429)$; $111^8 \equiv 1343^2 = 1803649 \equiv 1221 (\mathrm{mod}\ 5429)$; $111^{16} \equiv 1221^2 = 1490841 \equiv 3295 (\mathrm{mod}\ 5429)$; $111^{32} \equiv 3295^2 \equiv 4454$ (mod

5429); $111^{64} \equiv 4454^2 \equiv 550(\text{mod}5429)$; $111^{79} \equiv 550 \cdot 1221 \cdot 1343 \cdot 1463 \cdot 190 \equiv 3606(\text{mod } 5429)$

Это значит, что часть сообщения c_1 зашифрована в виде $\omega_1 = 3606$.

Блок c_2 шифруется аналогично: $\omega_2 = 234$.

Передаваемое сообщение состоит из зашифрованной части исходного сообщения ω_1 и ω_2 и открытого ключа, которым являются числа e и n (3606, 79, 5429) и (234, 79, 5429) соответственно. Для расшифровки сообщения адресат должен знать секретный ключ – такое натуральное число $d < n$, для которого выполняется условие $e \cdot d \equiv 1 \ (\text{mod } (\phi(n)))$. Отсюда следует, что взломать сообщение, зашифрованное в системе RSA, можно только найдя d – решение сравнения $ed \equiv 1(\text{mod } \phi(n))$. Исходя из свойств $\phi(n)$: необходимо разложить n на множители, что является очень сложной задачей и гарантом криптографической стойкости RSA.

УДК 512.624.95:378.147.091.3

КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ЭЛЬ ГАМАЛЯ

Студент гр. 10401115 Иванов А.И.
Ассистент Крупенкова Т. Г.
Белорусский национальный технический университет

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится схема Эль Гамаля, основные положения которой рассматриваются в данной работе.

Криптосистема Эль Гамаля создана американским специалистом по криптографии в 1985 году после появления криптосистемы *RSA*. Она послужила основой для целого ряда систем как шифрования, так и цифровой подписи, использующихся в наше время. В алгоритме Эль-Гамаля существуют некоторые открытые параметры, которые могут быть использованы большим числом пользователей. Они называются параметрами домена. К ним относятся: большое простое число $p \approx 2^q$, где $512 \leq q \leq 102$, то есть имеющее 150–300 десятичных знаков; целое число $\boldsymbol{g}$ — образующая циклической группы Z/pZ *; число $\boldsymbol{y}$, которое вычисляется по формуле $y = g^{X (\text{mod } p)}$. К закрытым ключам относятся: целое число **x** такое, что $1 < x < p$ и сессионный ключ — целое число $\boldsymbol{k}$ такое, что $1 < k < p - 1$

Два секретных ключа $\boldsymbol{x}$ и $\boldsymbol{k}$ являются элементами группы Z /pZ *. Числа ***(p, g, y)*** - тройка открытых ключей криптосистемы Эль Гамаля, число $\boldsymbol{x}$— закрытый ключ.