ресурсов должны быть имена, которые состоят только из букв, цифр и символа подчёркивания - '_'. Иначе вы не сможете обращаться к ресурсам из программы. Также не должно быть таких имён как 'self', 'other', 'global' или 'all', потому что эти слова имеют специальное назначение в GML.

Так что если вы любите игры, то потратить хотя бы неделю на Game Maker стоит.

УДК 535.317

НЕЙРОКОМПЬЮТЕРЫ: РАЗРАБОТКА И ПРИМЕНЕНИЕ

Студент гр. 104144 Крисеева Н.А.
Канд. физ.-мат. наук, доцент Прусова И.В.
Белорусский национальный технический университет

Нейрокомпьютер — устройство переработки информации на основе принципов работы естественных нейронных систем, преимуществами которого являются: надежные нейросистемы, которые делаются очень устойчивыми к разрушениям. Если говорить про основное направление - интеллектуализацию вычислительных систем, придание им свойств человеческого мышления и восприятия, то здесь нейрокомпьютеры практически единственный путь развития вычислительной техники. Разработки нейрокомпьютеров ведутся во многих странах мира, в частности, в Австралии создан образец коммерческого супернейрокомпьютера. Его общие задачи сводятся к обработке нейронною сетью многомерных массивов переменных (контроль кредитных карточек; система выявления скрытых веществ с помощью системы на базе тепловых нейронов и с помощью нейрокомпьютера на заказанных цифровых нейрочипах; система автоматизированного контроля безопасного сохранения ядерных изделий).

Нейрокомпьютеры успешно используются в различных областях народного хозяйства: управление, в режиме реального времени, самолетами, ракетами и технологическими процессами непрерывного производства (металлургического, химического и др.); распознавание образов человеческих лиц, букв и иероглифов, сигналов радара и сонара, отпечатков пальцев в криминалистике, заболеваний по симптомам (в медицине) и местностей, где следует искать полезные ископаемые (в геологии, по косвенным признакам); прогнозы погоды, курса акций (и других финансовых показателей), исхода лечения, политических событий, поведения противников в военном конфликте и в экономической конкуренции; оптимизация и поиск наилучших вариантов при

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