ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

- Балжан, Камила, Балауса, Алтынай, Алмас - это все те, чьи аккорды звучат мелодично, к тому же они обладают творческими способностями, косвенно или напрямую связаны с музыкой;

- Разия, Айнура, Расул, Азамат – у них аккорды звучали «резко», они же занимаются изучением точных наук или занимаются спортом.

Следует отметить, что среди них оказались и те, кто по тем или иным причинам ничем не увлекаются и не занимаются в каких либо секциях. Предполагаю, что возможно, они имеют эти склонности, но они ещё не реализовали их.

Данные исследования доказывают существование связи музыки и математики, точнее, то, что музыка представляет закономерность числового ряда. Но для утверждения того, что звучание даты рождения определяет определенный тип особенностей человека, необходимо большее количество исследуемых. Если при более глубоком и многочисленным исследовании, наше предположение будет доказано, это поможет людям понять себя, определить род занятий, выбрать профессию, где наиболее полно раскроется потенциал личности.

Трудовые будни математики состоят в изучении новых теорем, открывающих новые связи между известными понятиями. Однако к этому математика отнюдь не сводится.

Математика подобна искусству – и не потому, что она представляет собой «искусство вычислять» или «искусство доказывать», а потому что математика, как и искусство – это особый способ познания. Имеет, быть может, смысл по аналогии с художественными образами говорить о «математических образах» как специфической для математики форме отражения действительности. Нам следует понять, что математика не просто собрание теорем, а могучий инструмент познания.

В заключение исследования, хотелось бы процитировать слова известного философа, математика 19-20 вв. Бертрана Рассела *«Математика владеет не только истиной, но и высшей красотой – красотой отточенной и строгой, возвышенно чистой и стремящейся к подлинному совершенству, которое свойственно лишь величайшим образцам искусства».* (см. [2]).

Список использованных источников

1. Вахромеев В. Элементарная теория музыки. М: МУЗГИЗ, 1963
2. Кюне М. История построения музыкальной гаммы // реферат
3. Математика в современном мире // сборник статей, М: МИР, 1967, 204с

УДК 512.62: 531.0

О НЕКОТОРЫХ НЕДОСТАТКАХ КРИПТОСИСТЕМЫ RSA

Баймухамбетова Фариза, Шегай Жанна

fariza_1705@mail.ru, *zhanna_jsh2@mail.ru*

Магистрант, студент ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Д.Х. Козыбаев

Криптостойкость цифровых подписей, которые используют модульное возведение в степень, основано на разложении произведения на простые сомножители (RSA) или вычислении дискретного логарифма (DSA, ГОСТ 34.310-95). В связи с достигнутыми успехами в области теории чисел и возрастанием мощности вычислительных систем, а также использованием параллельного программирования, для обеспечения требуемой стойкости таких алгоритмов вынуждены увеличивать длину ключа. Так, для RSA, в пакете PGP уже используются ключи длиной 4096 битов. Увеличение длины ключа не только уменьшает производительность системы при выполнении операций для выработки и проверки цифровой подписи, но и увеличивает размер цифровой подписи. Так как цифровая подпись

обычно добавляется к самому документу, это уменьшает полезную пропускную способность канала связи. Поэтому сейчас повсеместно осуществляется переход на новые стандарты цифровой подписи на основе эллиптических кривых, которые позволяют без увеличения длины цифровой подписи достигнуть высокой криптографической стойкости.

Использование для оценки защищенности информационных систем частных методик и критериев, предназначенных для оценки криптографической стойкости алгоритмов шифрования и защищенности информации от утечки по техническим каналам. При этом происходит фактическая подмена модели угроз, в центре которой стоят проблемы борьбы с легальным пользователем системы, моделью соответствующих ведомств, в центре которых стоят субъекты несанкционированного доступа.

Как известно [1], далеко не все присутствующие на рынке криптографические средства обеспечивают обещанный уровень защиты. Это связано с нарушением нижеперечисленных требований, предъявляемых к криптографическому программному обеспечению [2]:

— использование проверенных алгоритмов, выдержавших попытки взлома в течение достаточного времени;

— длина ключей, достаточная, чтобы исключить снижение безопасности в результате увеличения вычислительных ресурсов потенциальных оппонентов (удваивающихся каждый год, согласно закону Мура) в течение длительного периода времени;

— локальная генерация и локальный менеджмент ключей, исключающие их попадание в чужие руки;

— гибкая схема удостоверения действительности ключей, допускающая как распределенное управление доверием ("сеть доверия"), так и централизованную архитектуру сертификации;

— открытость и доступность для проверки и критики не только алгоритмических решений и форматов файлов, но и исходного текста самой программы.

Однонаправленной функцией является умножение двух больших простых чисел, получить произведение, перемножив числа, нетрудно, но нелегко разложить произведение на множители и получить два больших простых числа. Криптография с открытыми ключами использует эту идею для создания однонаправленной функции с люком. На самом деле, это ложь, *не доказано*, что разложение на множители является тяжелой проблемой [3]. Насколько сегодня известно, это похоже на правду. И даже если это так, никто не может доказать, что трудные проблемы действительно трудны. Все считают, что разложение на множители является трудной задачей, но это никогда не было доказано математически.

В любом случае, доминирующие сегодня алгоритмы шифрования с открытым ключом основаны на трудности разложения на множители больших чисел, которые являются произведением двух больших простых чисел. (Другие алгоритмы основаны на так называемой Дискретной проблемой логарифма, но пока предположим, что к ней применимы те же рассуждения.) Эти алгоритмы также восприимчивы к вскрытию грубой силой, но по разному. Взлом этих алгоритмов состоит не из перебора всех возможных ключей, а из попыток разложения больших чисел на множители (или взятия дискретных логарифмов в очень большом конечной области - точно такая же проблема). Если число слишком мало, вы никак не защищены. Если число достаточно велико, то вы надежно защищены против всей вычислительной мощи мира, если она будет биться над этой задачей с настоящего времени до тех пор, пока Солнце не станет сверхновой - таково сегодняшнее понимание математики этой проблемы.

В последние годы в связи с ростом популярности криптографических методов защиты информации и созданием рынка программных продуктов все чаще появляются программы, не обеспечивающие надежную защиту. Появление таких программ обусловлено разработкой собственных нестойких криптографических средств, а также неправильной реализацией теоретически стойких алгоритмов или некорректным их использованием.

В работах К. Шеннона «Математическая теория связи» и «Теория связи в секретных системах» разрабатывается полноценный математический аппарат для криптографических задач [4].

Используемые в Казахстане (в основном) зарубежные программно-аппаратные средства являются прозрачными для их разработчиков. В связи с этим в Концепции информационной безопасности Республики Казахстан, принятой Советом Безопасности Республики Казахстан, указывается на необходимость создания отечественной системы обеспечения информационной безопасности, разработки методов, моделей и алгоритмов защиты информации для различных уровней ее секретности с последующей их аппаратно-программной реализацией.

В настоящее время в современной криптографии существуют следующие проблемы, которым необходимо математическое обоснование:

1. Ограниченность числа рабочих схем. В отличие от алгоритмов классической криптографии, которые могут быть созданы в неограниченном количестве путем комбинирования различных элементарных преобразований, каждая «современная» схема базируется на определенной «нерешаемой» задаче. Как следствие, количество рабочих схем криптографии с открытым ключом весьма невелико и необходимо изучать современные криптографические алгоритмы.
2. Постоянная «инфляция» размера блоков данных и ключей, обусловленная прогрессом математики и вычислительной техники. Так, если в момент создания криптосистемы RSA считался достаточным размер чисел в 512 бит, то сейчас рекомендуется не менее 2 Кбит. Иными словами, «безопасный» размер пространства ключа в RSA вырос в геометрической прогрессии, что опять же ведет к поиску новых криптоалгоритмов с небольшим размером ключа. Предполагается переход на криптоалгоритмы на эллиптических кривых.

В работе рассматриваются вопросы информационной безопасности эксплуатируемой в Казахстане налоговой системы COHO, а именно вопросы формирования пары ключей для ассиметричных алгоритмов в протоколах системы COHO и используемых алгоритмов шифрования. Кроме того, рассмотрены математические аспекты «дыр» в протоколах формирования пары ключей в системе COHO.

Прежде заметим, что в системе COHO в качестве ассиметричного алгортима реализован общеизвестный алгоритм RSA, что подтверждается практикой использования. В системе может быть реализован алгоритм создания специальных ключей, например, генерируется 512 битные простые числа на основе использования следующих формул:

$$p = n_1 \cdot 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4} + 1,\ q = n_2 \cdot 2^{k_5} \cdot 3^{k_6} \cdot 5^{k_7} \cdot 7^{k_8} + 1$$

где n_1 и n_2 – небольшие натуральные числа, а $k_1, k_2, \ldots, k_8$ – любые натуральные числа.

Но сложность разложения результата их перемножения $N = p \cdot q$ не будет порядка 1024 бита. Построенная на таком алгоритме система RSA может быть очень просто взломана по решетке Эратосфена. Клиент, получивший свою часть закрытого (секретного) ключа не имеет возможности вычислить, что он сделан из специальных простых чисел, по причине того, что он будет думать, что вычисляемая задача является NP полной. При этом злоумышленник можеть элементарно создать секретный ключ клиента, зная секрет создания простых чисел.

Список использованных источников

1 Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. –М.: Горячая линия–Телеком, 2007. – 320 с.

2 Брассар Ж. Современная криптология. – М.: Полимед, 1999.

3 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. –М.: Триумф, 2002. -595 с.

4 Шеннон К. Работы по теории информации и кибернетике. - М.: Изд-во иностранной литературы, 1963. - 832 с.

УДК 519

ПРИМЕНЕНИЕ МЕТОДОВ ДЕМОГРАФИЧЕСКОГО ПРОГНОЗА

Башеева Жулдыз Орынбасаровна
b_star77@mail.ru
Магистрант кафедры математического и компьютерного моделирования
Научный руководитель – А.Адамов

Во всем мире в практике демографического анализа широко используются современные методы исследования тенденций рождаемости, смертности и миграции, проводятся специальные массовые обследования населения с целью получения детальной информации, необходимой для уточнения демографических прогнозов.

В составе базовых условий социально-экономического развития страны особую значимость имеют демографические показатели. Это определяется тем, что в каждой стране действует закон соответствия социально-экономического и демографического развития общества. Действие этого закона проявляется в устойчивой зависимости между динамикой количественно-качественных характеристик состояния населения и параметрами развития экономики и социальной сферы (Рисунок 1).

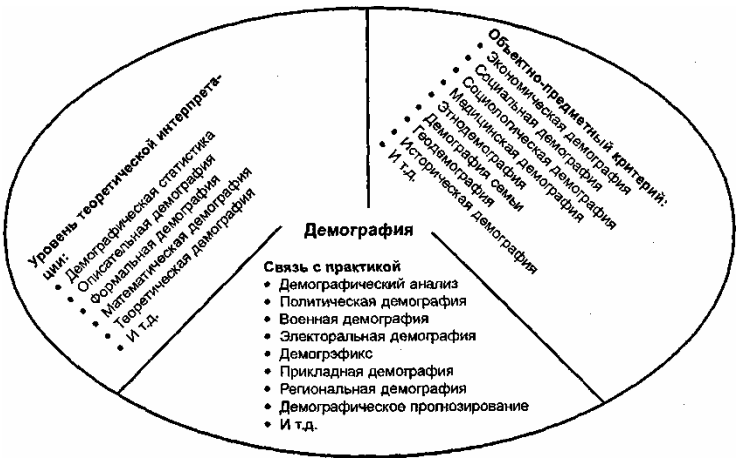

Рисунок 1 – Система демографии

Нельзя отрицать следующие макроэкономические пропорции и взаимосвязи: между численностью населения и размером национального богатства, объемом валового национального продукта, национального дохода; ростом численности населения и масштабами освоения территории страны, отдельных ее регионов; повышением доли населения трудоспособного возраста в общей численности населения и повышением темпов, масштабов социально-экономического развития страны, и наоборот.

Прогнозы, связанные с оценкой будущего состояния населения называются демографическими [1].

Объектами демографических прогнозов являются показатели численности населения, темпы роста (снижения) численности населения; рождаемости, смертности, миграции, половозрастной структуры населения, а также трудовой, экономический, потребительский потенциалы, жизненный фонд населения и др.

Демографические прогнозы разрабатываются на различные периоды времени. В частности, по периоду упреждения различают следующие демографические прогнозы: краткосрочные – разработанные на срок от одного года до 10 лет; среднесрочные – от 10 до 25 лет; долгосрочные – от 25 до 50 лет; сверхдолгосрочные – свыше 50 лет. Однако