

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
Математика және механика ғылыми-зерттеу институты
Механика-математика факультеті
Механико-математический факультет
Faculty of Mechanics and Mathematics



Қазақстан 2050

II ХАЛЫҚАРАЛЫҚ ФАРАБИ ОҚУЛАРЫ

Алматы, Қазақстан, 2015 жыл, 7-17 сәуір

Студенттер мен жас ғалымдардың

«ФАРАБИ ӘЛЕМІ»

атты халықаралық ғылыми конференциясының

МАТЕРИАЛДАРЫ

Алматы, Қазақстан, 2015 жыл, 13-16 сәуір



II МЕЖДУНАРОДНЫЕ ФАРАБИЕВСКИЕ ЧТЕНИЯ

Алматы, Казахстан, 7-17 апреля 2015 года

МАТЕРИАЛЫ

международной научной конференции
студентов и молодых ученых

«ФАРАБИ ӘЛЕМІ»

Алматы, Казахстан, 13-16 апреля 2015 года



II INTERNATIONAL FARABI READINGS

Almaty, Kazakhstan, 7-17 April, 2015

MATERIALS

International Scientific Conference of Students
and Young Scientists

«FARABI ALEMI»

Almaty, Kazakhstan, 13-16 April, 2015

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Математика және механика ғылыми-зерттеу институты

МЕХАНИКА-МАТЕМАТИКА ФАКУЛЬТЕТІ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
FACULTY OF MECHANICS AND MATHEMATICS

II ХАЛЫҚАРАЛЫҚ ФАРАБИ ОҚУЛАРЫ

Алматы, Қазақстан, 2015 жыл, 7-17 сәуір

Студенттер мен жас ғалымдардың
«ФАРАБИ ӘЛЕМІ» атты
халықаралық ғылыми конференциясының

МАТЕРИАЛДАРЫ

Қазақстан, Алматы, 13-16 сәуір, 2015 жыл

II МЕЖДУНАРОДНЫЕ ФАРАБИЕВСКИЕ ЧТЕНИЯ

Алматы, Казахстан, 7-17 апреля 2015 года

МАТЕРИАЛЫ

международной научной конференции
студентов и молодых ученых

«ФАРАБИ ӘЛЕМІ»

Казахстан, Алматы, 13-16 апреля 2015 г.

II INTERNATIONAL FARABI READINGS

Almaty, Kazakhstan, 7-17 April, 2015

MATERIALS

international Scientific Conference of Students
and Young Scientists

«FARABI ALEMI»

Almaty, Kazakhstan, 13-16 April, 2015

Алматы

«Қазақ университеті»

2015

Организационный комитет:

Қыдырбекулы А.Б.
Иманғалиев Е.И.
Абдибеков А.У.

Тунғатаров Н.Н.
Аетова Б.
Джолдаспаев С.
Дракунов А.
Жакебаев Д.Б.

Маусумбекова С.Ж.
Мухамбетжанов С.Т.

Елеуов А.А.

Кангужин Б.Е.
Шаймерденова А.

Калтаев А.Ж.
Тунғатарова М.С.

Есенғалиева Ж.С.
Копбосын Л.С.

Урмашев Б.А.
Макашев Е.П.

Сагитжанов Б.

председатель, декан механико-математического факультета, профессор
И.о.директора НИИ ММ
заместитель декана по научно-инновационной работе и межд.связям,
доцент
заместитель декана по учебно-методической и воспитательной работе
ученый секретарь НИИ ММ
председатель Совета НИРС, магистрант 2-го курса
председатель Совета молодых ученых, преподаватель
зав. кафедрой математического и компьютерного моделирования,
доцент
Зам.зав.каф.по научно-инновационной работе и межд.связям, доцент
зав. кафедрой дифференциальных уравнений и теории управления,
профессор
Зам.зав.каф. дифференциальных уравнений и теории управления по
научно-инновационной работе и межд.связям, доцент
зав. кафедрой фундаментальной математики, профессор
Зам. зав. каф. фундаментальной математики по научно-инновационной
работе и межд. связям, доцент
зав. кафедрой механики, профессор
Зам.зав.каф. механики по научно-инновационной работе и межд.связям,
доцент
зав. кафедрой информационных систем, профессор
Зам.зав.каф. информационных систем по научно-инновационной работе
и межд.связям, доцент
зав. кафедрой информатики, доцент
Зам.зав.каф. информатики по научно-инновационной работе и
межд.связям, доцент
председатель НСО

Редакционная коллегия:

Қыдырбекулы А.Б., Иманғалиев Е.И., Аетова Б.,
Сарсембаева Т.С., Аджигит К.

**Материалы международной конференции студентов и молодых ученых «Фараби
әлемі». г. Алматы, 13-16 апреля 2015 г. – Алматы: Қазақ университеті, 2015. – 200 с.
ISBN 978-601-04-1255-2**

Материалы, публикуемые в сборнике, являются изложением докладов студентов и молодых ученых на международной конференции студентов и молодых ученых «Фараби әлемі» по различным вопросам математики, механики, прикладной математики и информатики.

БАЙТУРЕЕВА А.Р. Математическое моделирование обтекания ветровыми потоками техногенных препятствий.....	94
ГАЛИЕВА Ф.М. Екіфазалы стефан типтес есептің адапталған тордағы математикалық моделін құру.....	95
ЕЛЕШҚЫЗЫ С. Схема коррекции потоков для численного решения гиперболического уравнения.....	96
ЕСИРКЕНОВ С.Р. Табиғат Катаклизмаларын Компьютерлік 3d Модельдеу.....	97
ЖАКСЫЛЫК С.Е. Виртуальный автомир трехмерного моделирования.....	98
ЖУМАТАЕВА А.Б. Математическое моделирование процесса взаимосвязанного тепло- и массопереноса в грунте.....	99
MASSIMOVA G.G., ZAMANOVA S.K. Developing apps for mobile devices in rad studio xe 7.....	100
ЗАУРБЕКОВА Г.Н. Разработка программного комплекса для моделирования загрязнения приземного слоя атмосферы промышленными выбросами.....	101
ИЗБАСАРОВА Ж.Б. Адамның бет-әлпетін zbrush программасы арқылы модельдеу.....	102
КАЛИЕВА Д.А. Математическая модель изменения концентрации норадреналина и адреналина.....	103
МУҚАНОВА М.А. Көлденең бұрғылаудағы кездейсоқ үйкеліс күшінің өзгерісін талдау.....	104
НУРАХМЕТОВ И.Б. Итерационный регуляризации.....	105
НУРБАЕВА Ж.З. Исследование эффективности теплоизоляционных конструкций нефтяного трубопровода.....	106
ПУЗИКОВ Е.М. Математическое моделирование распространения загрязняющих веществ с учетом турбулентности.....	107
СЕЙДУЛЛА И.Д. Киноөндіріс Және Теледидар Үшін Арнайы Әсерлі Сахнаны Жоғары Сапалы Көрсетушіліктендіру Және 3d-Моделдеу.....	108
ТАНАТОВА С.М. Изотермиялық емес шарт кезіндегі механикалық тепе-теңдіктің орныксыздығын сандық моделдеу.....	109
ТОЛЕГЕН Ж. Моделирование процесса переноса тепла в засыпном грунте подземного трубопровода.....	110
ТЛЕУОВА Ғ.Н. Моделирование сцен средствами OpenGL.....	111
ТОРТКУЛЬБАЕВ А.Д. Mathematical modeling of optimal portfolio of securities.....	112
ТӨЛЕУХАН А.Ж. 3d-Мультфильмдерді Моделдеу Үшін Заманауи Технологияларды Қолдану.....	113
ХАН Е.Р. Численное моделирование процесса отрыва течения в канале с обратным уступом.....	114

РАЗДЕЛ 4. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ СИСТЕМ

АВАКАН М.Е. Development of models and methods for solving the lexical selection problem in mt.....	115
АБДУАЛИ Б.А. Орыс-қазақ тілдік жұбы үшін апериум платформасында ережелерді пайдалана отырып аударма машинасын жасау.....	116
АБИКЕНОВ Е.А. Эффективность внедрения системы обработки клиентских запросов.....	117
АДИЛЬБЕКОВА А.Ж. Apertium платформасы негізінде машиналық аудармада лингвистикалық сөздіктердегі қазақ татар тілдерінің айырмашылығы.....	118
АКЖИГИТ К.Ж. Оценка стоимости компаний информационно-технологического сектора.....	119
АКЖИГИТ К.Ж. Моделирование процесса трудоустройства выпускников из учреждений профессионального образования.....	120

94	AKIMOVA A.B., KASSYMOVA D.B. Cryptanalysis of an algorithm for encryption Built on the principle network spn.....	121
95	АЛМАТОВ А.Ж. ГИС технологии для банковских учреждений.....	122
96	АЛТЫБАЙ А., ЕЛАМАНОВА Ә. Елімізде онлайн университет ашудың маңыздылығы.....	123
97	АРЫШ М.С. Стохастикалық есептерді mathcad жүйесінде шығарудың тиімділігі.....	124
98	АСТАНАКУЛОВ Е.И. Ақпаратты қорғаудың стеганографиялық әдістері	125
99	АХМАДИЕВА Ж.Е. Қазақ-орыс тілдік жұбы үшін apertium платформасында сөздікке етістіктерді енгізу ерекшеліктерін зерттеу.....	126
100	ӘМІРОВА Д.Т. Исследование моделей и алгоритмов решения задачи лексического выбора для англо-казахской пары языков.....	127
101	БАЙРАМ У. Интеграция общедоступных программных средств систем управления ресурсами предприятия и систем бизнес-аналитики.....	128
102	БАЛГАБЕКОВ А.Б. Қашықтан оқыту формасын талдау мен жобалауды автоматтандыру үшін объектілік модель жасау.....	129
103	БАСКАКОВ К.В. Методика расчета максимальных волн цунами.....	130
104	БЕЙБІТХАН Е. Перспективы развития поисковых систем и построение семантической сети предметной области.....	131
105	БЕКБУЛАТОВ Е. Анализ и проектирование современных технических систем безопасности.....	132
106	БЕКБУЛАТОВ Е. Бағдарламалық қауіпсіздік жүйелерін құрастыру және талдау.....	133
107	БЕКБОЛАТОВ Е.А., СЕРІКОВ С.А. Кафедраның тәрбие жұмысының кейбір есептерін ақпараттық технологиялардың көмегімен автоматтандыру.....	134
108	БОЛАТ А.Л. Техникалық қауіпсіздік жүйелерінде еңбек тиімділігін арттыру есептерін шешу.....	135
109	БОЛАТБЕК М.А. Қазақ-орыс машиналық аудармасындағы келер шақты аудару алгоритмдері.....	136
110	BORASHOVA S.M., YELTAYEVA D.K. Differential cryptanalysis of one encrypting algorithm.....	137
111	БӨРІБЕКОВА А.Е., ЕРБОЛАТОВА А.Е. Биометриялық идентификацияның статикалық әдістерін зерттеу.....	138
112	БУТИНА С.А., САРБАСОВА А.К., ЛИ А.В. Сравнение шифров с открытым ключом.....	139
113	ВОЛОШИН О.О. Глубокое обучение нейронных сетей для распознавания лиц.....	140
114	ГАТАУОВ А. М. Настройка прокси-сервера squid в веб-оболочке Webmin.....	141
115	ЕРМАКОВА К. Виртуальный мир и его технологии.....	142
116	ЕШИМБЕТОВ А.К., ВОЛОШИН О.О. Искусственный интеллект: расцвет или гибель человеческой рассы.....	143
117	ЕШИМБЕТОВ А.К. Скрытые недостатки глубинных нейронных сетей.....	144
118	ЖАҚАН Д.Б. Компьютерлік желілердің инфрақұрылымдық шабуылдардан қорғанысының механизмдерін құру.....	145
119	ЖАҚАН Д.Б. Анализ возможности использования систем искусственного интеллекта на основе нейронных сетей в области защиты информации.....	146
120	ЖАНБУСУНОВ Н.Ш. Қазақ-ағылшын тілдік жұбы үшін қос тілдік корпус аударма машинасын жасауда пайдалану.....	147
121	ЖАНБУСУНОВ Н.Ш. Қазақ-ағылшын тілдік жұбы үшін қос тілдік корпус аударма машинасын жасауда пайдалану.....	148
122	ЖОЛДЫБЕКОВА С.К. Қазақ орыс тілдері бағытындағы машиналық аудармада лексикалық таңдама жасау.....	149

СРАВНЕНИЕ ШИФРОВ С ОТКРЫТЫМ КЛЮЧОМ

С.А. БУТИНА, А.К. САРБАСОВА, А.В. ЛИ

На сегодняшний день криптографические системы используются в различных сферах человеческой деятельности. Одной из самых популярных систем открытого ключа является RSA.

RSA - криптографическая система открытого ключа, обеспечивающая такую же защиту как шифрование и цифровая подпись (аутентификация - удостоверение подлинности). Криптосистема RSA разработана в 1977 году и названа в честь разработчиков Ronald Rivest, Adi Shamir и Leonard Adleman [1].

В основе лежат два ключа - публичный и приватный. Публичным ключом является пара (e, n) , а приватным - пара (d, n) .

К преимуществам данной системы относятся: 1) система позволяет легко проверить правильность ключа; 2) каждый может проверить подпись, если имеется соответствующий приватный ключ. Это делает систему быстрой и надежной.

К недостаткам системы RSA относятся: 1) система все время усложняется, она делается более надежной, в то же время замедляется ее работа; 2) в связи с маленькой скоростью шифрования сообщения чаще всего используют более производительные симметричные алгоритмы со случайным ключом. Данный механизм имеет некоторые уязвимости в виду необходимости использования криптостойкий генератор случайных чисел для формирования случайного симметричного шифрования, который может эффективно противостоять внешним атакам.

Схема Эль-Гамала (Elgamal) - криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Схема была предложена в 1985 г. [2].

Для шифрования, как и в RSA, необходимо сгенерировать ключи. Для этого выбирается случайное число $p = 7$, далее подбираем g , $1 < g < p$, $g = 5$. Следующим действием выбираем случайное число x , $1 < x < p$, $x = 4$.

Еще одним ключом будет y , вычисляем его по формуле: $y = g^x \bmod p = 5^4 \bmod 7 = 2$.

Таким образом, открытый ключ $(p, g, y) = (7, 5, 2)$, а закрытый ключ $x = 4$.

Для зашифровки сообщения M , выбираем случайное число k , которое должно быть взаимно простым с $(p - 1)$ и соответствовать виду $1 < k < p - 1$.

Главным преимуществом для данной схемы является ее вероятностный характер шифрования, так как такие схемы наиболее стойкие в сравнении со стандартным определенным процессом шифрования. Этот вероятностный характер достигается за счет наличия переменной k .

Основным минусом схемы шифрования Elgamal является увеличение длины зашифрованного текста вдвое. Для схемы вероятностного шифрования ключ и сообщение не определяют шифротекст однозначно.

Итак, криптографическая система RSA значительно проще в использовании, чем Elgamal, так как требует меньше мощностей и соответственно времени. Однако RSA представляет собой наиболее защищенную от взломов, что делает ее одной из самых популярных и распространенных криптографических систем открытого ключа в настоящее время.

СПИСОК ЛИТЕРАТУРЫ

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Алгоритмы, применение / пер. с англ. В. Б. Афанасьева. - М.: Техносфера, 2006. - 320 с.
2. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шифрования. Методы их анализа: учеб. пособие для вузов. - М.: Гелиос АРВ, 2006. - 376 с.