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 Sudents
and Young Scientists
«FARABI ALEMI»

Almaty, Kazakhstan, 13-16 April, 2015

Алматы
«Қазақ университеті»
2015

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.

ISBN 978-601-04-1255-2

РАЗДЕЛ 4. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ СИСТЕМ

СРАВНЕНИЕ ШИФРОВ С ОТКРЫТЫМ КЛЮЧОМ

С.А. БУТИНА, А.К. САРБАСОВА, А.В. ЛИ

На сегодняшний день криптографические системы используются в различ человеческой деятельности. Одной из самых популярных систем открытого клю RSA.

RSA - криптографическая система открытого ключа, обеспечивающая такие защиты как шифрование и цифровая подпись (аутентификация – ус подлинности). Криптосистема RSA разработана в 1977 году и названа разработчиков Ronald Rivest, Adi Shamir и Leonard Adleman [1].

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

К преимуществам данной системы относятся: 1) система позволяет правильность ключа; 2) каждый может проверить подпись, если имеется соо быстрая и надежная система.

К недостаткам системы RSA относятся: 1) система все время усло совершенствуется, она делается более надежной, в то же время замедляется работы; 2) в связи с маленькой скоростью шифрования сообщения чаще всего используя более производительные симметричные алгоритмы со случайным к Данный механизм имеет некоторые уязвимости в виду необходимости ис криптостойкий генератор случайных чисел для формирования случайно симметричного шифрования, который может эффективно противостоять внешним

Схема Эль-Гамаля (Elgamal) - криптосистема с открытым ключом, осн трудности вычисления дискретных логарифмов в конечном поле. Схема была пре 1985 г. [2].

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

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

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

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

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

Основным минусом схемы шифрования Elgamal является увеличен зашифрованного текста вдвое. Для схемы вероятностного шифрования ключ и со не определяют шифротекст однозначно.

Итак, криптографическая система RSA значительно проще в использов Elgamal, так как требует меньше мощностей и соответственно времени. О представляет собой наиболее защищенной от взломов, что делает ее одной популярных и распространенных криптографических систем открытого ключа в м

СПИСОК ЛИТЕРАТУРЫ

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. алгоритмы, применение / пер. с англ. В. Б. Афанасьева. - М.: Техносфера, 2006. - 32

2. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шиф методы их анализа: учеб. пособие для вузов. - М.: Гелиос АРВ, 2006. - 376 с.