ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ТҰҢҒЫШ ПРЕЗИДЕНТІ - ЕЛБАСЫНЫҢ ҚОРЫ

«ҒЫЛЫМ ЖӘНЕ БІЛІМ – 2017»

студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ – 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2017»

14th April 2017, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

«Ғылым және білім - 2017»
студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«Science and education - 2017»

2017 жыл 14 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2017» студенттер мен жас ғалымдардың XII Халықаралық ғылыми конференциясы = The XII International Scientific Conference for students and young scholars «Science and education - 2017» = XII Международная научная конференция студентов и молодых ученых «Наука и образование - 2017». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2017. – 7466 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-827-6

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 378

ББК 74.58

ISBN 978-9965-31-827-6

С.105 – 111.
2. Воробьев А. И. Исследовательский комплекс моделирования интеллектуальных транспортных систем / А.И. Воробьев, И.С. Морданов // Автотранспортное предприятие. – 2013. – №12. – С.40-41.
3. Жанказиев С.В., Тур А.А., Халилев Р.Ф. Интеллектуальные дороги – современный взгляд // Наука и техника в дорожной отрасли. – 2010. – № 2. – С. 1 – 7.
4. Жанказиев С.В., Научные основы и методология формирования интеллектуальных транспортных систем в автомобильно-дорожных комплексах городов и регионов, диссертация доктора технических наук. М., 2012 г. с. 451.
5. Пржибыл, Павел. Телематика на транспорте/ Павел Пржибыл, Мирослав Свитек; перевод с чешского О. Бузека и В. Бузковой.; под ред. проф. В. В. Сильянова. - М.: Изд-во МАДИ (ГТУ), 2003. - 540с.
6. Халилев Р.Ф. Проектирование интеллектуальных транспортных систем/Р.Ф.Халилев// Международный научно-исследовательский журнал. –2013. –№ 7-2 (14).– С. 98-100.
7. Жанказиев С.В. Становление жизненного цикла локального проекта интеллектуальной транспортной системы/ С.В.Жанказиев, Р.Ф.Халилев// Автотранспортное предприятие.– 2012. –№ 11.– С. 31-33.
8. Халилев Р.Ф. Новые подходы к оценке эффективности технических решений ИТС // Научно – практический журнал Актуальные вопросы инновационной экономики. –2013. – № 4. С. 176-179.

УДК 004.056.55

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОПУЛЯРНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ СИММЕТРИЧНОГО И АССИММЕТРИЧНОГО ШИФРОВАНИЯ

Баймакова Улжан Жандосовна
uljana05.95@mail.ru
Студент ЕНУ им.Л.Н.Гумилева, Астана, Казахстан
Научный руководитель- К.И.Танырбергенова

Методы защиты, значимой информации, пользовались популярность с давних времен для скрытия от посторонних глаз секретных данных.

В наше время, где общество становится информационно-обусловленным , защита информации является необходимой частью, в этом нам помогает наука занимающаяся шифрованием и защитой данных, криптография. В свою очередь, эта наука использует различные методы и алгоритмы шифрования предназначенные защищать информацию в целях ее целостности и сохранении авторских прав.

Наука криптографии состоит из следующих разделов :

1. Симметричные криптоситемы
2. Криптосистемы с открытым ключем
3. Системы электронной подписи
4. Управление ключами

Под симметричными криптоситемами, понимаются такие системы в которых используется один и тот же ключ для шифрования и дешифрования информации.

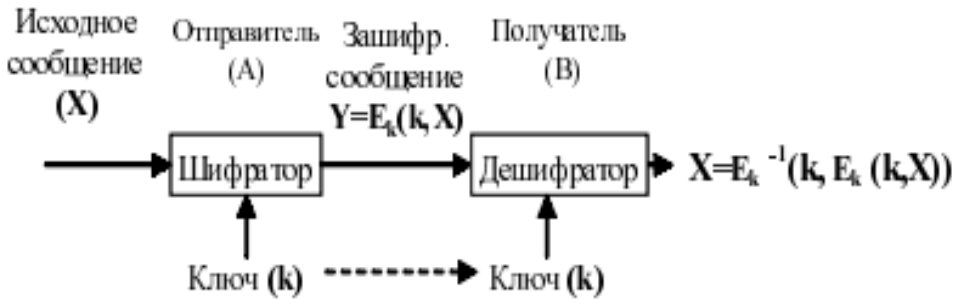

Рис.1: Схема симметричной криптоситемы

Симметричные криптосистемы основываются на базовых классах моно- и многоалфавитных подстановок, перестановках, блочных шифрах и гаммировании.

Блочный шифр оперируется группами бит фиксированной длины — блоками, которых состоит в пределах от 64–256 бит.

Одним из наиболее распространенных способов задания блочных шифров является использование сетей Фейстеля. Сеть Фейстеля представляет собой общий метод преобразования произвольной функции в перестановку на множестве блоков. [1]

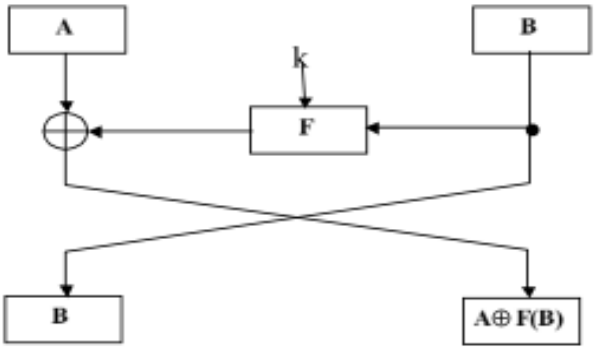

Рис.2: Структура итерации сети Фейстеля[6]

К алгоритмам блочного шифрования относятся такие алгоритмы как DES, AES, ГОСТ 28147-89.

Симметричный алгоритм шифрования DES (Data Encryption Standard)- это известная криптосистема с открытым ключом, которая была разработана в 1977 компанией IBM и утвержденная в качестве стандарта FIPS 46-3. [8]

DES шифрует 64- битовые блоки данных с использованием 56-битного ключа. Процесс шифрования состоит в начальной перестановке битов входного блока, шестнадцати циклах шифрования и конечной перестановки данных.[5][9]

В алгоритме шифрования DES все данные на первом этапе переводят в бинарный вид, затем преобразованный вид данных делят на блоки, и только после этих проделанных процедур осуществляется шифрование. Все действия происходят согласно сети Фейстеля, также в алгоритме используется векторный сдвиг и используется перестановка с 56 битным ключом шифрования.

Шифр DES это результат 33 отображений:

$$DES= IP^{-1}\times\pi T_{16}\times\theta\times\pi T_1\times IP,$$

где IP-исходная перестановка, представляет собой проволочную коммутацию с инверсией IP^{-1}, композиция $\theta\times\pi T_1$, где θ изменение местами правой и левой половин блока данных, представляет собой одну итерацию Фейстеля.В последнем цикле шифрования перестановка местами половин блока не производится.[1][6]

Преимущества этого алгоритма заключается в простоте его ключевой системы, а также

в высокой скорости программной и аппаратной реализации.

DES в течении двадцати лет оставался достаточно криптостойким алгоритмом шифрования.

В данный момент федеральным стандартом шифрования в США является AES (Rijndael),который был утвержден в 2001 году Министерством торговли. Возможные размеры ключа 128, 192 и 256 бит.

Различием алгоритма AES от остальных известных симметричных алгоритмов шифрования является в особенности сети Фейстеля, где значение при входе делятся на два и более субблоков, часть из которых в каждом раунде прерабатывается по заранее определенным законам, далее значения накладывается на необрабатываемые субблоки. **AES** показывает блок данных в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8 (возможно также использование фиксированных размеров блока информации которые шифруется). Все действия выполняются с отдельными байтами массива, а также с независимыми столбцами и строками.

Алгоритм делает четыре преобразования: BS (ByteSub) – осуществляется замена байта в таблице; SR (ShiftRow) – сдвигаются строки массива; MC(MixColumn) - операция над независимыми столбцами массива, где каждый столбец матрицы правилу умножается на фиксированную матрицу c(x) по определенному правилу. И, наконец, AK(AddRoundKey) - добавление ключа. **[2][7]**

Особенностью алгоритма **AES (Rijndael) благодаря которому он стал новым стандартом шифрования данных является его высокая скорость шифрования на всех платформах.[7]**

Российским стандартом симметричного блочного шифрования является алгоритм шифрования ГОСТ 28147-89, который имеет длину ключа шифрования 256 бит. ГОСТ 28147-89, имеет режима работы: простой замены, гаммирования, гаммирования с обратной связью и генерации имитоприставок.

Алгоритм ГОСТ 28147-89 имеет тот же принцип работы , что и DES, это блочный шифр с секретным ключом, но отличием его от DES является большая длина ключа, большое количество раундов и простая схема построения раундов. ГОСТ 28147-89 имеет высокую оценку стойкости – сейчас известен лишь один метод взлома, метод "грубой силы". Стойкость этого алгоритма достигается благодаря его длине ключа в 256 бит. Когда используется секретная синхропосылка эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты.[2]

Еще одним обширным классом криптографических систем являются ассиметричные или двух ключевые системы. Эти системы характерезуются тем, что для шифрования и дешифрования используются разные ключи, связанные между собой некоторой зависимостью.Но при этом знаю один ключ второй ключ востановить достаточно сложный процес.

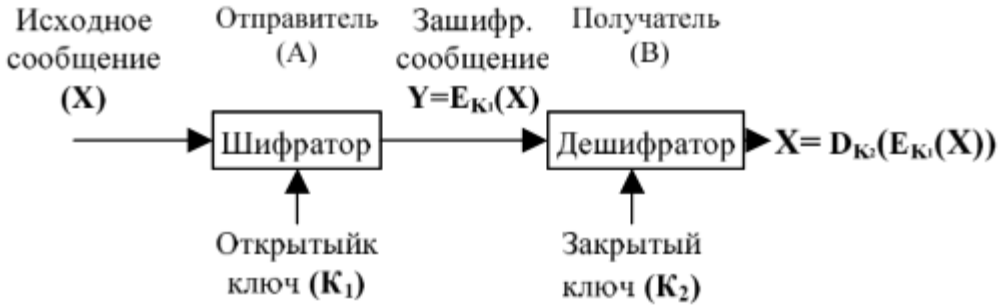

Рис.3: Схема асимметричной криптоситемы

Криптосистема с открытым ключом определяется тремя алгоритмами:генерация ключей, шифрование и дешифрование. Алгоритм генерации ключей имеет открытый вид, каждый имеет право дать ему на входе случайную строку r надлежащей длины и взять пару

ключей (k1, k2). Где один из ключей публикуется, он называется открытым, а второй, называется секретным. Алгоритмы шифрования E_{k1} и дешифрования D_{k2} таковы, что для любого открытого текста m

$$D_{k2}=(E_{k1}(m)).[1]$$

К ассимметричным алгоритмам шифрования относятся такие алгоритмы как RSA и EL-Gamal.

RSA был спроэктирован в 1978 г. Рон Ривестом, Ади Шамиром и Л.Адельманом от сюда он и получил свое название по начальным буквам разработчиков.Криптостойкость данного алгоритма основывается на сложности факторизации больших чисел и вычисления дискретных логарифмов. В основе RSA лежит задача факторизации умножение двух простых больших чисел. При шифровании используют простую операцию возведения в степень по модулю NN. В дешифрования нужно вычислить функцию Эйлера от числа NN, где нужно знать разложение числа n на простые множители. В RSA открытый и закрытый ключ состоит из пары целых чисел. Закрытый ключ хранится в секретности , а второй же ключ сообщается другому участнику, либо где-то публикуется. **Стойкость этой криптографической системы** определяется сложностью задачи разложения больших чисел на простые множители. До сих пор неизвестны эффективные алгоритмы решения этой задачи, что и обеспечивает высокую практическую стойкость системы RSA.[3][9]

Алгоритм Эль-Гамаля также относится к асимметричным типам шифрования информации. Эль-Гамаль это криптосистема основанная на проблеме логарифма. Этот алгоритм включает в себя как шифрование так и цифровую подпись. Отличие этого алгоритма от RSA, это то, что Эль-Гамаль основан на проблеме именно дискретного логарифма.

Также этот алгоритм имеет огромный ряд преимуществ в отличии от RSA :

1. Целые числа, при данном уровне стойкости, с которыми работает этот алгоритм, имеют запись меньше на 25% , что позволяет сократить сложность вычислений в целых 2 раза, и при этом также уменьшается объем используемой памяти;
2. Выбор параметров осуществляется при проверке всего двух легких условий.

Поскольку алгоритм не является запатентованным он не нуждается в специальных лизенциях на его использование. Данный алгоритм электронной подписи, не позволяет его применение в роли алгоритма шифрования (в отличии от RSA, где алгоритмы шифрования и электронная подпись одно и то же).[4]

В современной криптографии при конструировании криптостойких систем используются как и симметричные так и ассиметричные алгоритмы. Поскольку алгоритмы с открытым ключом позволяют назначать ключи и в симметричных алгоритмах, также допускается возможность объяденения в среде предачи защищенной информации оба типа шифрования. Использовать ассимитричный алгоритм для рассылки ключей, а симметричным же шифровать пересылаемую информацию.

Список использованных источников

1. Соколов А. В. Шаньгин В. Ф. "Защита информации в распределенных корпоративных сетях и системах"-М.:ДМК Пресс,2002,С.61-65,84-97,160-168
2. Брассар Ж. Современная криптология , Москва, Издательско-полиграфическая фирма ПОЛИМЕД 1999,С. 15-70.
3. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Госстандарт СССР, 1989
4. http://www.ict.edu.ru/ft/002447/crypto1-3.pdf
5. https://www.bytemag.ru/articles/detail.php?ID=6645
6. http://historyofciphers.blogspot.com/
7. http://5fan.ru/wievjob.php?id=28565
8. http://stfw.ru/page.php?id=11477

9. http://rushkolnik.ru/docs/10/index-13765.html?page=3
10. http://www.volpi.ru/umkd/zki/index.php?man=1&page=12
11. http://mirznanii.com/a/110761/kriptografiya-blochnyy-shifr
12. http://otherreferats.allbest.ru/programming/00197560_0.html

ӘОЖ 004.042

КӨПАҒЫНДЫ БАҒДАРЛАМАЛАУДЫ ЗЕРТТЕУ ЖӘНЕ ҚОЛДАНУ МҮМКІНДІКТЕРІНЕ ШОЛУ

Ерболова Нұрән Арайқызы
nuran95@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің «Есептеу техникасы» кафедрасы, Астана, Қазақстан
Ғылыми жетекшісі –Ташенова Ж.М.

Бұл мақалада көпағынды бағдарламалық зерттеудің мүмкіндіктері қарастырылады. Көпағынды бағдарламалауда көпағындылықтың мағынасын ашамыз. Көпағындық қасиеті - операциялық жүйеде туындайтын процесс уақытта белгіленген ретсіз параллельді орындалатын бірнеше ағыннан тұратын платформа (мысалы, операциялық жүйе, виртуалды машина және т.с.с). Яғни, бірнеше есепті орындаған кезде мұндай бөлу есептеу құрылғысының ресурстарын тиімді қолдануға мүмкіндік береді. Мұндай ағындарды орындау ағындары (thread of execution) деп аталады. Көпағындық маңызы бір орындалатын процесс деңгейінде көпесептік болып табылады, яғни барлық ағындар процесстің адрестік кеңістігінде орындалады. Сонымен қатар, процестің барлық ағындарында бір адрестік кеңістік, дескрипторлары болады. Орындалатын процесте кем дегенде бір (негізгі) ағыны болады. Көпағындықты көпесептік және көп процессорлықпен шатастырмау керек, бірақ көпесептілікті іске асыратын операциялық жүйелер көпағындықты да іске асырады.

Программалаудағы көпағындықтың артықшылықтары:

- Кейбір жағдайларда жалпы адрестік кеңістікті босату арқылы программаны жеңілдету;
- Ағынды құруға кететін уақыттың аз шығыны;
- Процессорлық есептеулер және енгізу-шығару операцияларын параллельдеу арқылы процесс өнімділігін арттыру [1].

Қарапайым процессорда ағындарды басқару операциялық жүйемен іске асырылады. Аппараттық үзу, жүйелік шақыру немесе сол ағынға бөлінген уақыт аяқталғанға дейін ағын орындалады. Осыдан кейін процессор ағын жағдайын сақтайтын операциялық жүйе кодына ауысады немесе, басқа ағын күйіне ауысады. Мұндай көпағындық жағдайында процессордың көп тактер саны контекстерді (бір есептен екінші есепке ауыстыру) ауыстыратын операциялық жүйелер кодына жұмсалады. Егер ағындарды қолдауды аппараттты түрде іске асырса, процессор өзі ағындар арасында ауысу жасап отыра алады, кейбір жағдайларда бірнеше ағындарды әрбір тактте біруақытты орындай алады.

Процессорларда аппаратты іске асырылатын 2 көпағындық түрі болады:

-уақытша көпағындық;

-біруақытты көпағындық.

Ағындарды іске асыру типтері:

- Қолдану кеңістігіндегі ағын. Әрбір процессте ағындар кестесі болады, ядро процестері кестесіне ұқсас. Кемшіліктері:

1. Бір процесс ішінде таймер бойынша үзудің болмауы.
2. Процеске бұғаттау жүйелік сұраныс қолданғанда оның барлық ағындары бұғаттанады.
3. Іске асыру қиындығы.