

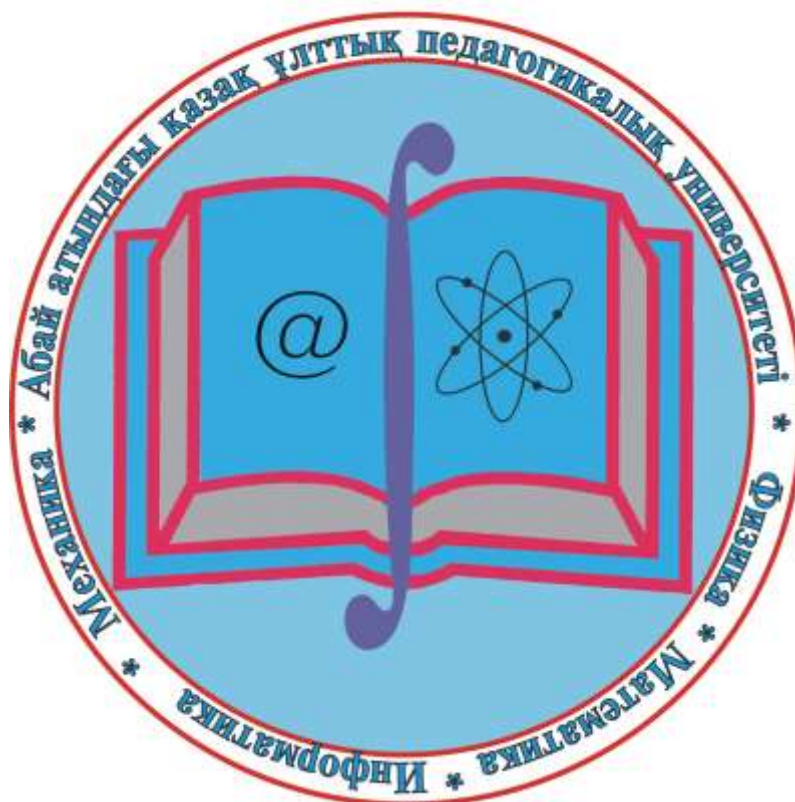


Абай атындағы
Қазақ ұлттық педагогикалық университеті

Казахский национальный педагогический
университет имени Абая

Серия «Физико-математические науки» • «Физика-математика ғылымдары» сериясы

ХАБАРШЫ ВЕСТНИК



Алматы

№ 4 (52)

2015

Казахский национальный педагогический университет имени Абая ВЕСТНИК серия “Физико-математические науки” № 4 (52) Главный редактор Академик НАН РК Г.У. Уалиев Редакционная коллегия: зам.главного редактора: д.п.н. Е.Ы. Бидайбеков, к.ф.-м.н. М.Ж. Бекпатшаев ответ.секретарь к.п.н. Г.А. Абдулкаримова члены: Dr.-ing. Holm Altenbach(Germany), Dr. S.A.Hasan (Pakistan), Dr. YasuhideFukumoto(Japan), Phd.d Shuo-Hung Chang, (Taiwan), д.п.н. А.Е. Абылкасымова, д.ф.-м.н. М.А. Бектемесов, д.ф.-м.н. А.С.Бердышев, д.п.н. В.В. Гриншкун (Россия), к.ф.-м.н. Ф.Р. Гусманова, д.т.н. А.Д.Джураев(Узбекистан), д.ф.-м.н. С.И. Кабанихин (Россия), д.ф.-м.н. Б.А. Кожамқұлов, д.ф.-м.н. В.Н. Косов, д.ф.-м.н. К.К. Коксалов, д.т.н. М.К. Кулбеков, д.п.н. М.П. Лапчик (Россия), д.ф.-м.н. Қ.М. Мукашев, д.ф.-м.н. С.Т. Мухамбетжанов, д.т.н. Г.Я. Пановко (Россия), д.п.н. Б.Д. Сыдыков, д.ф.-м.н. Н.Ж. Такибаев, д.ф.-м.н. К.Б. Тлебаев, д.т.н. А.К. Тулешов, д.ф.-м.н. З.Г. Уалиев, д.ф.-м.н. Л.М. Чечин, к.ф.-м.н. Е.Б. Шалбаев, к.т.н. Ш.И. Хамраев ©Казахский национальный педагогический университет им. Абая, 2015	
Зарегистрирован в Министерстве информации Республики Казахстан, № 4824 - Ж - 15.03.2004 (периодичность—4 номера в год) Выходит с 2000 года	
Редакторы:Ф.Р. Гусманова, Г.А. Абдулкаримова	
Компьютерная верстка: Г.А. Абдулкаримова Ф.Р. Гусманова	
Подписано в печать 23.12.2015 г. Формат 60х84 1/8. Об 9,45 уч.-издл. Тираж 300 экз.	
050010, г.Алматы, пр.Достык, 13, КазНПУ им.Абая Отпечатано в типографии “TOO Palitra Press” г.Алматы, ул.Хамиди 4а	
Д.А. Кинжебаева Построение планов скоростей и ускорений механизма IV класса с использованием метода особых точек Ассура	104
М.Қ. Құлбекұлы, Д.М. Кулбеков, Е.А. Оспанбеков, Б. Ерженбек Шар пішіндес керамикалық үлгідердегі кристалдық судың ыдырап шығуына байланысты жүретін диффузиялық үдерістер кинетикасы	108
Б.А. Мукушев Күн жүйесін құрайтын планеталардың қозғалысын сандық әдістер негізінде зерттеу	114
Б.А. Мукушев Суда қалқитын денелердің орнықтылығын физикалық модельдер көмегімен зерттеу	120
З.Г. Уәлиев, И.М. Уәлиева, Р.У. Бекмуратов, Н. Оган Серпімді итергішті жұдырықшалы механизмнің бірімсаллы динамикалық моделі	126
З.Г. Уәлиев, И.М. Уәлиева, Р.У. Бекмуратов, Н. Оган Жұдырықшалы механизмнің жетектегі звеноларының тербелістері	130
ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ. БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ. ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ	
Е.С. Алимжанов, М.Е. Мансурова Построение тезаурусов и онтологий по областям математических и компьютерных наук	134
Д.И. Дадашев-Юсупов, А.Ю. Пыркова Разработка антивирусной оболочки для клиент-серверных приложений	140
Е.В. Дудышева, Л.А. Романова Применение «перевернутого класса» как технологии проектного смешанного обучения	146
С.С. Ихсанов, А.Ю. Пыркова Анализ работы распараллеленных алгоритмов шифрования в различных системах	149
J. Kultan, Н. Керимбаев LMS MOODLE в международном образовании	155
Р.Н. Курманалиева Управление многомерными объектами по передаточным функциям	162
Т.Ж. Мазаков, С.А. Нугманова, Г.С. Байрбекова О некоторых проблемах организации защиты информации РАИС «Демография»	166
Г.С. Муханова Имитационное моделирование в управлении рисками проекта	175
А.Е. Сағымбаева, А.Т. Дүйсек Мониторинг оқушылардың оқу жетістіктерінің нәтижесі ретінде	182
М.А. Скиба, А.Р. Турганбаева Оценка е-портфолио выпускника на основе применения таксонов Блума	187
В.Б. Тарасов, Б.С. Карабеков, М.А. Нуркаманова Управление знаниями на базе онтологического моделирования в инжиниринге предприятий	192
Г.И. Тлеубердиева Использование рекомендаций библиотеки information technology infrastructure library в системах управления взаимоотношениями с клиентами	201
А.Р. Турганбаева, М.А. Скиба Типовая структура е-портфолио: особенности проектирования и наполнения	207
К.З. Халықова Жеке тұлғаның интеллектуалдық әлеуетін дамытудағы ақпараттық білім беру ортасының алатын орны мен ролі	213
Ш.Т. Шекербекова, Г.А. Абдулкаримова Болашақ информатика мұғалімдерін кәсіптік-педагогикалық бағытта даярлау	219

- процессы. 2011. № 8. С. 53-59. Режим доступа: <http://cyberleninka.ru/article/n/problemy-i-perspektivy-ispolzovaniya-vozmozhnostey-seti-internet-studentami>.
3. Galway et al. A novel integration of online and flipped classroom instructional models in public health higher education. BMC Medical Education, 2014. Pp. 14-181.
 4. Мокрецова Л.А. и др. Подготовка к инновационному предпринимательству в гуманитарном вузе в региональных социально-экономических условиях : коллективная монография. Бийск: ФГБОУ ВПО «АГАО», 2015.
 5. Мокрецова Л.А., Дудышева Е.В., Романова Л.А. Подготовка студентов к инновационной проектной деятельности в условиях регионального информационного образовательного пространства. Наука и школа. 2015. № 2. С. 196-203.

Аңдатпа. Мақалада аралас оқу жағдайындағы студенттердің өнімділік, шығармашылық инновациялық қызметтерін белсендіру тәсілі ретінде төңкерілген кластың білім беру технологиясына талдау жүргізіледі. Студенттік жобаларды ұйымдастыру мысалында осындай технологияларға әлеуметтік желілерді қолдану мүмкіндіктері талқыланады. В.М. Шукшин атындағы Алтай мемлекеттік білім беру академиясында қатысушылардың тікелей және қашықтан коммуникациялық сипаттаумен инновациялық студенттік жобаларды дайындау кезеңдері келтірілген.

Түйін сөздер: аралас оқу, төңкерілген кластың білім беру технологиясы, инновациялық студенттік жобалар

Abstract. The article analyzes the idea of educational “flipped classroom” technologies as ways of activating productive, creative innovative detail of students in blended learning. The possibility of the use of social networking technologies on the example of the organization of students’ projects discusses. We present the stages of development of innovative students’ projects in the Shukshin Altai State Academy of Education describing the immediate and distance communication participants.

Keywords: blended learning; flipped classroom educational technology; innovative student projects.

УДК 004.05

С.С. Ихсанов, А.Ю. Пыrkova

АНАЛИЗ РАБОТЫ РАСПАРАЛЛЕЛЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ В РАЗЛИЧНЫХ СИСТЕМАХ

(г. Алматы, Казахский национальный университет имени аль-Фараби)

Аннотация. Защита информации всегда была актуальна. Высочайшая степень автоматизации, к которой стремится современное общество, ставит его в зависимость от уровня безопасности используемых информационных технологий. Массовое применение компьютерных систем, позволившее решить задачу автоматизации процессов обработки постоянно нарастающих объемов информации, сделало эти процессы чрезвычайно уязвимыми по отношению к агрессивным воздействиям и поставило перед потребителями информационных технологий новую проблему, - проблему информационной безопасности. Проблема информационной безопасности уже длительное время решается для стационарных компьютеров, но с появлением мобильных приложений со своими специфическими особенностями возникла потребность в новых решениях в области криптозащиты.

В данной статье рассматривается реализация и сравнительный анализ работы двух алгоритмов криптозащиты на различных устройствах: Blowfish и AES128, которые были

распараллелены.

Ключевые слова: защита информации, Blowfish и AES128, шифрование, параллельные алгоритмы, анализ.

Описание алгоритма Blowfish.

Blowfish это 64-битовый блочный шифр с ключом переменной длины. Алгоритм состоит из двух этапов [1]:

- 1) Расширение ключа
- 2) Шифрование/ дешифрование данных

На первом этапе исходный ключ преобразуется в матрицу раундовых ключей и матрицу подстановки с объемом 4168 байт.

Второй этап происходит путём использования сети Фейстеля, которая состоит из 16 раундов. Создание раундовых ключей и подстановки также используют сеть Фейстеля.

Шифрование данных [1] состоит из простой функции, последовательно выполняемой 16 раз. Каждый этап состоит из зависимой от ключа перестановки и зависимой от ключа и данных подстановки (Рис. 1). Используются только сложения и XOR 32-битовых слов. Единственными дополнительными операциями на каждом этапе являются четыре извлечения данных из индексированного массива. В Blowfish используется много подключей. Эти подключи должны быть рассчитаны до начала шифрования или дешифрования данных.

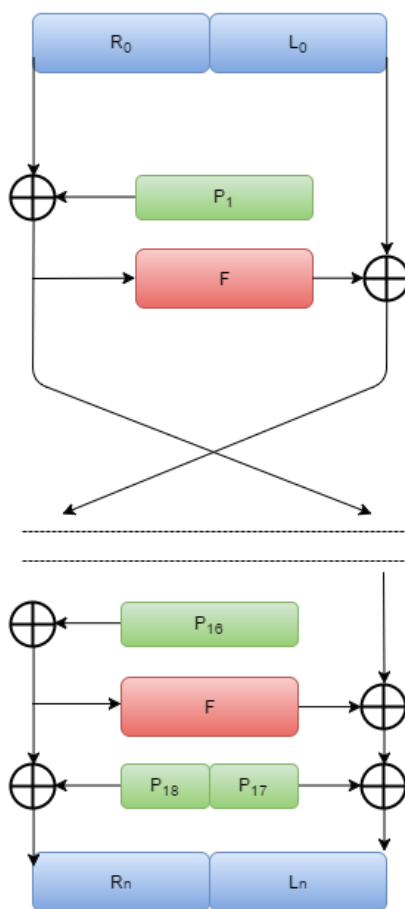


Рис. 1. Структура алгоритма Blowfish

В алгоритме Blowfish при шифрации выполняется 16 раундов (внутри сети

Фейстеля), а 17-й и 18-й ключи складываются с левым и правым выходным блоком последнего раунда. Такое количество раундов было выбрано, поскольку именно оно определяет длину возможного ключа.

$$F(X_1, X_2, X_3, X_4) = \left(\left((S_1[X_1] + S_2[X_2]) \bmod 2^{32} \right) \oplus S_3[X_3] \right) + S_4[X_4] \bmod 2^{32} \quad (1)$$

Функция использует матрицы подстановок S_1 — S_4 для того, чтобы линейно преобразовать входящие 32 бита данных в значение из матрицы подстановки [2].

Описание алгоритма AES128. Алгоритм AES [3, 4] состоит из часто повторяющихся раундов шифрования, как видно из рисунка 2. Сначала на основе 128-битового ключа получают одиннадцать ключей раундов, каждый из которых имеет размер 128 бит. Каждый раунд включает в себя преобразование с использованием соответствующего криптографического ключа, для того чтобы обеспечить секретность шифрования (Рис. 2).

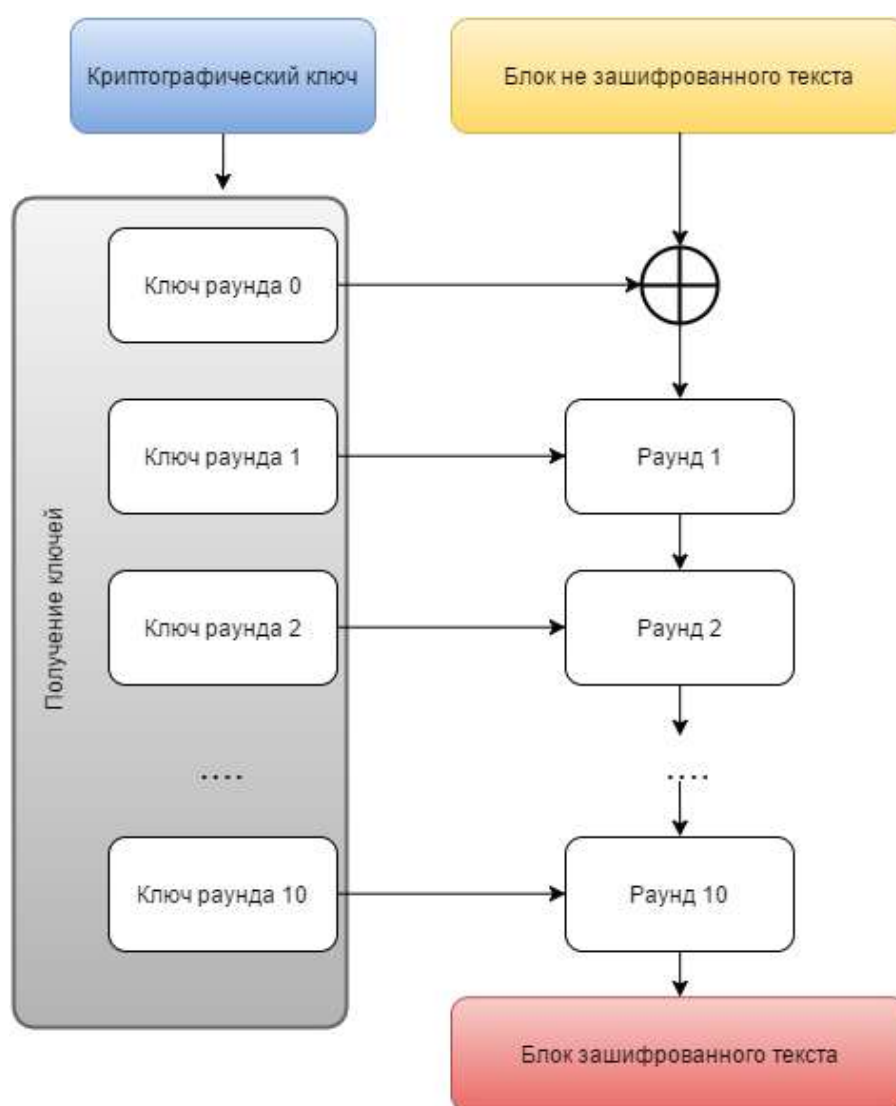


Рис. 2. Структура алгоритма AES

После начального раунда, во время которого осуществляется логическая операция исключающего или первого ключа раунда и незашифрованного текста (операция «Addroundkey»), следуют девять одинаково структурированных раундов. Каждый раунд

**ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ.
БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ
ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ
ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ**

состоит из следующих операций:

- замещение байтов;
- сдвиг строк;
- перемешивание столбцов;
- добавление ключа раунда.

Десятый раунд подобен раундам с первого по девятый, но без операции перемешивания столбцов.

Распараллеливание алгоритма. Распараллеливание происходит следующим образом (Рис. 3):

- 1) Данные разделяются на блоки между потоками.
- 2) Каждый поток запускает алгоритмом шифрования.
- 3) Далее результаты шифрования записываются в отдельный блок каждого потока.
- 4) В итоге происходит сбор всех данных в один общий блок.

Алгоритм дешифрование происходит аналогично.



Рис. 3 Распараллеливание алгоритма

Работа алгоритмов на различных устройствах.

В процессе работы алгоритмы были запущены на следующих устройствах.

- 1) ПК 4 GB q9400 266 gHZ, ОС Windows 7.
- 2) ноутбук dell 4GB core i7 255gHZ, ОС Windows 8.
- 3) планшет Nexus 7, 2GB четырехъядерный процессор Nvidia Tegra 3 1.5ГГц под ОС Android 5.0 lolipop.

Алгоритмы были реализованы на языке Java с использованием многопоточности. На рисунках 4 и 5 демонстрируется время выполнения алгоритмов шифрования с различным количеством потоков. По горизонтали - количество потоков, по вертикали – время выполнения задачи. Как видно из гистограмм с увеличением количества потоков время выполнения становится меньше.



Рис. 4. Гистограмма работы параллельного алгоритма AES128 с 10 МБ данных

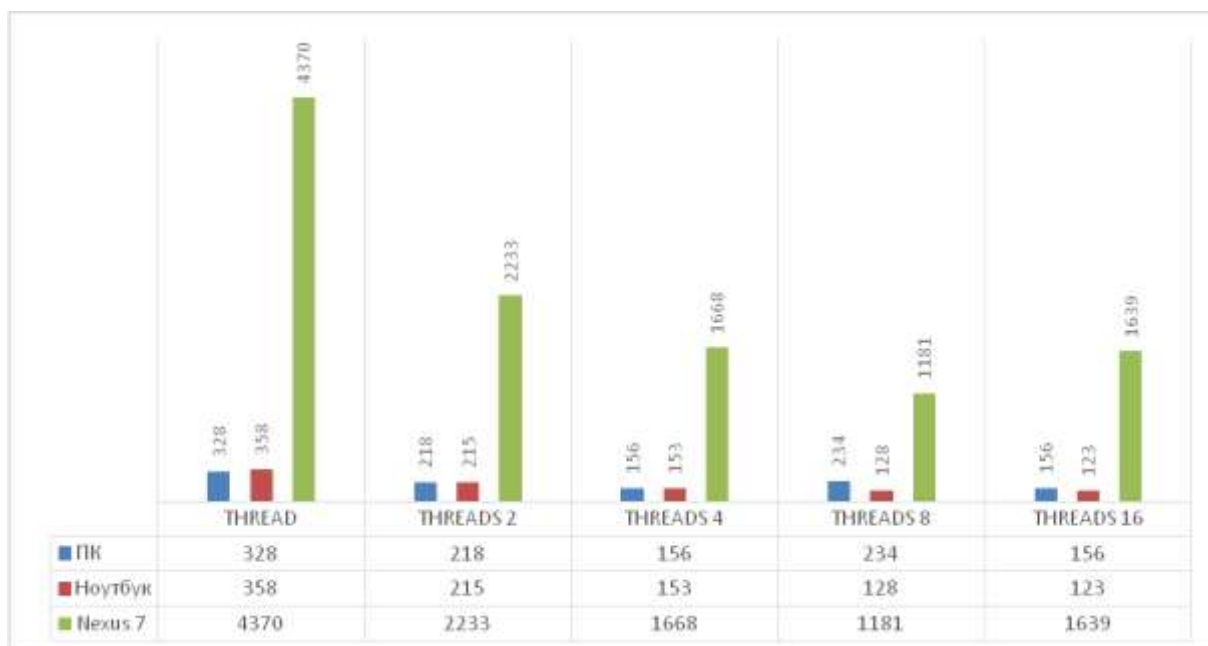


Рис. 5. Гистограмма работы параллельного алгоритма Blowfish с 10 МБ данных

На стационарных устройствах с ОС Windows 8 и 7 никаких проблем в реализации не возникло. На Android устройствах были проблемы следующего характера:

1) В процессе реализации алгоритмов возникла проблема нехватки памяти на Nexus 7. Поток не мог полностью работать с цельным блоком данных, вследствие чего пришлось разделить блок на подблоки в каждом потоке, что уменьшило производительность алгоритма, но обеспечило устойчивую работу при небольших объемах памяти.

2) Исходя из гистограмм 4 и 5 видно, что AES128 проигрывает по скорости алгоритму Blowfish. Это связано с использованием памяти и множественным

**ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ ӘДІСТЕМЕСІ.
БІЛІМ БЕРУДІ АҚПАРАТТАНДЫРУ
ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ
ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ**

дублированием данных в алгоритме AES128. С решением данной проблемы возможно не только ускорение алгоритма, но и оптимизация данного алгоритма для Android системы.

В результате проведенного исследования и анализа возникших проблем было установлено, что одним из способов увеличения производительности является использование технологии Intel Threading Building Blocks, которая позволяет оптимизировать алгоритм и упрощает некоторые процессы, однако требует переноса алгоритма на язык программирования C++.

Закключение. В процессе работы были рассмотрены проблемы реализации алгоритмов шифрования Blowfish и AES128, проблемы работы с Android устройствами и пути их решения, а также сделаны предположения по применению методов, которые увеличат производительность алгоритма на Android устройствах.

В результате было разработано программное приложение для персональных и мобильных устройств. Версия для персонального компьютера была реализована в среде разработки NetBeans на языке Java. Приложение способно шифровать и расшифровывать данные в текстовом варианте, используя алгоритмы шифрования Blowfish и AES128.

Приложение для мобильных устройств было разработано в среде Android studio. Мобильная версия выполняет аналогичные функции, что и версия для персональных компьютеров. Приложение совместимо со всеми системами Android 4.0 и выше.

1. Breeze A. Blowfish, ресурс для IT-специалистов. // <http://habrahabr.ru/post/140394>
2. Костюхин К. AES-128. Детали и реализация на Python, ресурс для IT-специалистов. // <http://habrahabr.ru/post/212235>
3. Fundamentals of Cryptology. // A Professional Reference and Interactive Tutorial by Henk C.A. van Tilborg Eindhoven University of Technology The Netherlands. - Boston/Dordrecht/London: KLUWER ACADEMIC PUBLISHERS, 2006. - 503с.
4. Форузан Б.А. Криптография и безопасность сетей. – М.: Бином, Лаборатория знаний, 2010. - 784с.

Аңдатпа. Ақпаратты қорғау мәселесі әрқашан маңызды. Қазіргі қоғамның жоғары деңгейдегі автоматтандыруы ақпаратты қорғау, қауыпсыздық мәселесінің маңыздылығын арттыра түседі. Компьютерлік жүйені жаппай қолдану ақпараттың өңделуін ұлғайтты, бірақ ақпаратты қорғау мәселесінің өзектілігін арттыра түсуде. Бұл мәселе стационарлы компьютерлер бойынша шешіліп келе жатыр. Ал мобильді құрылғылардың қолданысқа енгені криптографиялық қорғауда жаңа шешімдерді талап етеді.

Бұл мақалада екі түрлі криптографиялық алгоритмдердің салыстырмалы талдау құрылғыларда жұмыс істеу, жүзеге асыру мәселелері талқыланды : Blowfish және AES128, параллельденген.

Түйін сөздер: Ақпараттық қорғау, Blowfish және AES128, шифрование, параллельді алгоритмдер, талдау.

Abstract. Information security has always been relevant. Highest degree of automation, sought by modern society, puts it in dependence on the level of security in information technology. The massive use of computer systems, would allow solving the problem of automating the processing of ever-increasing volumes of information, made these processes are extremely vulnerable to aggressive and put in front of consumers of information technologies a new problem - the problem of information security. The problem of information security has long been solved for desktop computers, but with the advent of mobile applications with their own specific features created a need for new solutions in the field of encryption.

This article discusses the implementation and comparative analysis of cryptographic algorithms work on two different devices: Blowfish and AES128, which have been parallelized.

Keywords: information security, Blowfish and AES128, encryption, parallel algorithms, analysis.

ҚҰРМЕТТІ ОҚЫРМАНДАР!

ҚР БЖҒМ Білім және ғылым саласындағы бақылау комитетінің 2012 жылы 10 шілдедегі № 1082 Шешімімен Қазақстан Республикасының Білім және Ғылым министрлігінің Білім және ғылым саласындағы бақылау комитетінің ұсынысымен Абай атындағы Қазақ ұлттық педагогикалық университетінің «Физика-математика ғылымдары» сериясы бойынша Хабаршы журналы ғылыми қызметтерінің негізгі нәтижелерін жариялау үшін келесі мамандықтар бойынша ұсынылатын басылымдар Тізіміне енгізілгенін хабарлаймыз:

- 01.01.00 топ мамандықтары бойынша – физика-математика ғылымдары (математика);
- 01.02.00 (01.02.01, 01.02.04, 01.02.06) мамандықтары бойынша – физика-математика ғылымдары (механика);
- 05.00.00 (05.02.18) мамандықтары бойынша – техникалық ғылымдар;
- 13.00.00 (13.00.02) мамандықтары бойынша – педагогика (оқыту және тәрбиелеу теориясы мен әдістемесі /математика, физика, информатика/) ғылымдары;
- 01.04.00 топ мамандықтары бойынша - физика-математика ғылымдары (физика).

2009 жылдан бастап Инженеринг және Технология Институтымен (Ұлыбритания) ақпараттық-қолдау қызмет көрсетуге жасалған келісім-шарттың (№2, 12.01.2009ж.) негізінде Абай атындағы ҚазҰПУ «Физика-математика сериясы» бойынша Хабаршы журналында жарияланатын мақалалардың реферативті ақпараты INSPEC электронды мәлімтер қорына енгізіледі.

Редакция ғылыми мақала материалдарын толығымен немесе жекелеп ғылыми дәйексөз индексімен қамтамасыз ететін қазақстандық және шетелдік мекемелерге беруге, сонымен қатар осы материалдарды журналдың интернет сайтына орналастыруға құқылы.

«ХАБАРШЫ. ФИЗИКА-МАТЕМАТИКА ҒЫЛЫМДАРЫ СЕРИЯСЫ» ЖУРНАЛЫНА БАСЫЛАТЫН МАҚАЛАЛАРДЫ БЕЗЕНДІРІЛУГЕ ҚОЙЫЛАТЫН ТАЛАПТАР

I. Қажетті материалдар

- 1.Парақтары төменгі жағында қарандашпен нөмірленген мақаланың қатты көшірмесі (2 дана), барлық авторлар мақала мәтінінің бір данасына қол қоюлары керек;
2. Мақаланың аты, мақалаға үш түрде (қазақ, орыс, ағылшын тілдерінде) жазылған аңдатпалардың, түйін сөздердің қатты көшірмесі (1 дана). Аңдатпада зерттеудің мақсаты мен әдіснамасын, негізгі жетістігі мен қорытындысын көрсету қажет. Аңдатпада 5-7 сөйлем болуы керек. Түйін сөздер саны электрондық іздеу жүйесінде мақала табылатындай 5-10 сөзден (сөз тіркесінен) тұруы керек.
- 3 Автор (авторлар – 4 адамнан артық болмау керек) жайында мәліметтердің қатты көшірмесі (1 дана): Ф.А.Ә. толығымен, жұмыс орны (ұжым аты, жоғары оқу орынның толық аты), атқаратын қызметі, жұмыс телефоны, үйдің мекен-жайы, үй телефоны, ғылыми дәрежесі, ғылыми атағы, e-mail.
4. Мақаланың, мақалаға жазылған аңдатпаның және түйін сөздердің электрондық түрі;

II. Мақаланы безендіру ережесі

- 1.Мақала мәтіні Word редакторында бірлік интервал арқылы терілу керек;
- 2.Парақ пішімі : 210 x 297 mm (A4);
3. Жоғары, төменгі, оң жақтағы, сол жақтағы өрістер: – 2,5 см;
- 4.Мақала беттері нөмірленбейді;
- 5.Шрифт: Times New Roman (қазақ, орыс, ағылшын тілдері үшін), өлшемі - 12 пт; Абзацтық жылжу– 1 см.;
6. Кестелер мен графикалық материалдар (суреттер, графикалар, фотосуреттер және т.б.) толассыз нөмірленулері және атаулары (кегль №11) болуы керек. Барлық кестелер мен графикалық материалдарға мақала мәтінінде сілтемелер болуы керек. Берілген нысандар сілтемелерден кейін орналасуы қажет. Word редакторында орындалған суреттер нысан ретінде қойылуы керек;
7. Мақала мәтіні ені бойынша форматталуы керек.

III. Формула жазуға қойылатын талаптар

Формулалардағы (Equation) символдар өлшемдері : Обычный – 11 пт, Крупный индекс – 6 пт, Мелкий индекс – 5 пт, Крупный символ – 24 пт, Мелкий символ – 4 пт; формулалар беттің ортасы бойынша орналастырылады. Сілтеме жасалатын формулаларды ғана нөмірлеу керек. Формулалар толассыз нөмірленеді. Формулалар нөмірлері оң жақ шетімен тегістеледі де, дөңгелек жақшаға алынады. Мәтінде де формулаларға сілтемелерді дөңгелек жақшаға жазады.

IV. Әдебиеттер тізімі

мақалада пайдаланылған әдебиеттер мәтінде пайдалану ретіне сәйкес қолжазбаның соңында келтіріледі. Мақаладағы әдебиетке сілтеу квадраттық жақшада беріледі, мысалы, [1], [2,3], [4-7].

V. Мақаланың түрі

1. Сол жақ жоғарғы бұрышта бас әріптермен ӘОК (кегль №13);
2. Жартылай қарайтылған кіші әріптермен (кегль №13) ортада автордың (авторлардың саны 4 адамнан аспауы керек) фамилиясы және аты-жөні;
3. Бір бос жолдан кейін жартылай қарайтылған бас әріптермен (кегль №13) мақала аты;
4. Бір бос жолдан кейін дөңгелек жақшада автор (авторлар) жұмыс істейтін немесе оқитын қала және ұжымның аты; егер автор (авторлар) білім алушы болса, * (жұлдызша) белгісінен кейін білім алушының статусы (студент, магистрант, докторант) жазылады (кегль №11);
5. Бос жолдан кейін мақала жазылған тілде 5-7 сөйлем көлемінде аңдатпа және 5-10 сөздер болатындай түйін сөздер (кегль №11, курсив);
6. . Бір бос жолдан кейін мақала мәтіні (кегль №12);
7. Пайдаланылған әдебиеттер тізімі мәтіннен кейін екі бос жол тастап (кегль №11) кіші әріптермен келтіріледі. Бірлік интервал.
8. Бос жолдан кейін 2 тілде мақалаға аңдатпа және 5-10 сөздер (сөз тіркесі) болатындай түйін сөздер (кегль №11, курсив).

1-мысал. Мақаланы безендіру

ӘОЖ

ФИО, ФИО*

МАҚАЛАНЫҢ АТЫ

(қала, мекеменің аты, * - студент/магистрант/ докторант)

Аңдатпа. Мақала тілінде (5-7 сөйлем).

Түйін сөздер: Мақала тілінде (5-10сөз, сөз тіркесі)

Мақала мәтіні (5-7 бет)

Пайдаланылған әдебиеттер тізімі

Аңдатпа. Мақала тілінен өзге 2 тілде (5-7 сөйлем).

Түйін сөздер: Мақала тілінен өзге 2 тілде (5-10 сөз, сөз тіркесі)

VI. Мақалаларды жариялау тілдері – қазақ, орыс, ағылшын тілдері.

Редакцияға түскен мақалаларға білім саласы бойынша мамандар мен ғылымдар пікір береді. Пікір негізінде редакция алқасы авторға мақаланы тағы да толықтыруға (түзетуге) ұсыныс жасауы, не мүлдем қайтарып беруі мүмкін. Бұрын жарияланған немесе басқа баспаға жіберілген мақалалар қабылданбайды.

Мақала көлемі 5-7 бет. Көлемі 7 беттен артық болған жағдайда журнал редакциясымен хабарласып келісулері қажет. Мақала мәтініне енетін иллюстрациялардың, сұлбалардың және кестелердің көлемі мәтіннің жалпы көлеміне кіреді.

Мақаланы дайындау және жариялау бойынша пайда болған барлық сұрақтар бойынша журнал редакциясына хабарласыңыздар.

Мекен-жайы: Алматы қаласы, Төле би 86 көшесі, Абай атындағы ҚазҰПУ, Математика, физика және информатика институты, жұмыс телефоны - 8(727) -2 61-68-69, e-mail Vestnik_KazNPU@mail.ru

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Информируем Вас, что Решением Комитета по контролю в сфере образования и науки МОН РК от «10» июля 2012 года № 1082 «Вестник Казахского национального педагогического университета имени Абая, Серия физико-математические науки» включен в Перечень изданий, рекомендуемых Комитетом по контролю в сфере образования и науки Министерства образования и науки Республики Казахстан для публикации основных результатов научной деятельности по следующим направлениям:

- по специальностям группы 01.01.00 – физико-математические науки (математика);
- по специальности 01.02.00 (01.02.01, 01.02.04, 01.02.06) – физико-математические науки (механика);
- по специальности 05.00.00 (05.02.18) – технические науки;
- по специальности 13.00.00 (13.00.02) – педагогические науки (теория и методика обучения и воспитания /математика, физика, информатика);
- по специальностям группы 01.04.00 – физико-математические науки (физика).

С 2009 г. действует Договор с Институтом Инжиниринга и Технологий (Великобритания), (№2 от 12.01.2009 г.) на оказание информационно-сопроводительных услуг, согласно которому реферативная информация о статьях, публикуемых в Вестнике КазНПУ имени Абая, вносится в электронную базу данных INSPEC.

Редакция имеет право частично или полностью предоставлять материалы научных статей в казахстанские и зарубежные организации, обеспечивающие индекс научного цитирования, а также размещать данные материалы на Интернет-сайте журнала.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ СТАТЕЙ ПУБЛИКУЕМЫХ В ЖУРНАЛЕ «ВЕСТНИК. СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ»

I. Представление необходимых материалов

1. Текст статьи в твердой копии с пронумерованными, внизу по центру карандашом, страницами (2 экз.), один экземпляр текста статьи должен быть подписан всеми авторами.
2. Название статьи, аннотации к статье, ключевые слова (на 3-х языках: казахском, русском, английском) в твердой копии (1 экз.). В аннотации необходимо указывать цель и методологию исследования, основные достижения и выводы. Объем аннотации – 5-7 предложений. Ключевые слова: 5–10 слов (словосочетаний), по которым статьи могут быть найдены в электронных поисковых системах.
3. Сведения об авторе (авторах – не более 4 человек) в твердой копии на 3-х языках (1 экз.): фамилия, имя, отчество, место работы (город, название организации/вуза без сокращений), ученая степень и звание, должность, e-mail, контактный телефон.
4. Статья, аннотации к статье, ключевые слова в электронном виде.

II. Правила оформления статей.

1. Текст статьи должен быть набран в редакторе Word через одинарный интервал;
2. Формат листа: 210 x 297 mm (A4);
3. Поля: верхнее, нижнее, правое, левое – 2,5 см;
4. Страницы статьи не нумеруются;
5. Шрифт: Times New Roman (для каз., рус. и англ. языков), размер - 12 пт; Абзацный отступ – 1 см.
6. Таблицы и графические материалы (рисунки, графики, фотографии и др.) должны иметь сквозную нумерацию и названия (кегль №11). На все таблицы и графические материалы должны быть сделаны ссылки в тексте статьи. При этом расположение данных объектов должно быть после ссылок на них. Рисунки, выполненные в редакторе Word, должны быть вставлены как объект.
7. Текст статьи должен быть отформатирован по ширине.

III. Требования к написанию формул

Размеры символов в формулах (Equation): обычный – 11 пт, крупный индекс – 6 пт, мелкий – 5 пт, крупный символ – 24, мелкий – 4 пт; формулы располагают по центру страницы, Нумеровать следует только те формулы, на которые приводятся ссылки. Нумерация формул должна быть сквозной. Номер формулы располагают по правому краю страницы и заключают в круглые скобки. В тексте ссылку на формулу также приводят в круглых скобках.

IV. Список литературы, использованной в статье, составляется по ходу упоминания ее в тексте и приводится в конце рукописи. Ссылки на литературу в тексте указываются в квадратных скобках, например, [1], [2,3], [4-7].

V. Вид статьи

1. УДК в левом верхнем углу прописными буквами (кегель №13);
2. Полуужирными строчными буквами (кегель №13) по центру инициалы и фамилия автора (авторов не более 4 человек);
3. Через пустую строку полуужирными прописными буквами (кегель №13) название статьи;
4. Через пустую строку в круглых скобках, город и название организации, где работает или учится автор (авторы). Если автор (авторы) обучающиеся, то после знака * (звездочка) – указать статус обучающегося (студент, магистрант, докторант) (кегель №11);
5. Через пустую строку аннотация на языке публикации в 5-7 кратких предложениях (кегель №11);
6. Через пустую строку текст статьи (кегель №12);
7. Используемые источники, указываются после текста статьи, через две пустые строки строчными буквами (кегель №11). Интервал – одинарный;
8. Через пустую строку аннотации к статье на 2-х языках, ключевые слова: 5–10 слов (словосочетаний) (кегель №11, курсив).

Образец. Оформление статьи

УДК

ФИО, ФИО*

НАЗВАНИЕ СТАТЬИ

(город, название организации, *- студент/магистрант/докторант)

Аннотация. На языке статьи (5-7 предложений).

Ключевые слова: на языке статьи

Текст статьи (не менее 5 и не более 7 стр.)

Список литературы

Библиографический список

Аңдатпа.

Түйін создер:

Abstract.

Keywords:

VI. Языки издания статей – казахский, русский, английский.

Поступившие в редакцию статьи рецензируются ведущими специалистами и учеными по отраслям знаний. На основании рецензии редколлегии может рекомендовать автору доработать статью или отказать в публикации. Рукописи статей, опубликованных ранее или переданных в другие издания, не принимаются.

Рекомендуемый объем статьи – не менее пяти и не более семи страниц. В ином случае вопрос по объему статьи необходимо согласовать с редакцией журнала. Иллюстрации, схемы, таблицы, включаемые в текст статьи, учитываются в общем объеме текста.

По всем вопросам, связанным с подготовкой, представлением и публикацией материалов, необходимо обращаться в редакцию журнала.

Адрес: г.Алматы, ул.Толе би 86, КазНПУ им.Абая, Институт математики, физики и информатики
рабочий телефон 8(727) -2 61-68-69, e-mail Vestnik_KazNPU@mail.ru