Идентификатор № 104-975-099

Гончарова Ирина Вячеславовна,

учитель информатики ГБОУ СОШ № 750 (СП № 2) СВОУО ДО г. Москвы

*Приложение 2*

*к статье* «**Проекты с применением компьютерных технологий (из опыта работы)».**

**Аннотации к работе "Гаммирование" и "Симметричное и асимметричное шифрование".**

*Из аннотации к работе "Гаммирование:*
1.*Теоретическая часть:*

Симметричное шифрование остаётся самым актуальным и криптографически гарантированным методом защиты информации, и поэтому **целью** работы выбрано исследование симметричного шифрования – одного из самых высокопроизводительных методов для защиты информации, изучение общей схемы, принципов работы. Разработка программного обеспечения по реализации алгоритмов шифрования, основанного на гаммировании.
*2. Методы проведения исследования:*

Для достижения цели исследования автором использовались общенаучные (теоретические и эмпирические) методы.

Из *теоретических* методов применялись: анализ известных данных о методах симметричного шифрования (метод классического шифрования Шеннона; блочные шифраторы - американский шифратор DES (Data Encryption Standard) и отечественный стандарт ГОСТ 28147-89, IDEA (International Data Encryption Algorithm), CAST, Шифр Skipjack, RC2 и RC4 и др.);изучение специальной литературы; синтез полученных данных для получения представлений об эффективности данного метода; сравнение классических шифров, выявление основных достоинств и недостатков, конкретизация общих методов и схемы симметричного шифрования, обобщение полученных данных.

Из *эмпирических* методов использовались: изучение симметричного шифрования на примере работ Шеннона и др., опытно-экспериментальная работа по разработке и реализации алгоритма шифрования, основанного на гаммировании ( разработка блок-схемы и программы на языке программирования QBASIC и языке объектно-ориентированного программирования VisualBasic).

*Из аннотации к работе "Симметричное и асимметричное шифрование".*

Симметричное и асимметричное шифрование остаются самыми актуальными и криптографически гарантированными методами защиты информации, и поэтому*целью* работы выбрано исследование симметричного и асимметричного шифрования – самых высокопроизводительных методов для защиты информации, изучение известных блочных шифраторов и методов двухключевой криптографии, схемы, принципов работы. Разработка программного обеспечения по реализации алгоритмов симметричного и асимметричного шифрования (схемы RSA). Продолжена работа по совершенствованию разработанного ранее автором программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании (блок-схемы и программы на языке объектно-ориентированного программирования Visual Basic –GAMMIR2-версия2). Планируется дальнейшая работа над проектом.

*Методы исследования:* Для достижения цели исследования автором использовались общенаучные (теоретические и эмпирические) методы. Из *теоретических* методов применялись: анализ известных данных о методах симметричного шифрования (метод классического шифрования Шеннона; блочные шифраторы - американский шифратор DES и отечественный стандарт ГОСТ 28147-89, IDEA (International Data Encryption Algorithm), CAST, Шифр Skipjack, RC2 и RC4 и др.); и методов двухключевой криптографии ( метод открытого распределения ключей Диффи-Хеллмана, криптосистема RSA и др.); изучение специальной литературы; синтез полученных данных для получения представлений об эффективности данных методов; сравнение классических шифров, методов шифрования с помощью симметричного и несимметричного ключей, выявление основных достоинств и недостатков, конкретизация общих методов и схем симметричного шифрования и асимметричного шифрования, обобщение полученных данных. Из *эмпирических* методов использовались: изучение симметричного шифрования на примере работ Шеннона , асимметричного шифрования на примере методов двухключевой криптографии, опытно-экспериментальная работа по разработке программного обеспечения по реализации алгоритмов симметричного и асимметричного шифрования (схемы RSA), по совершенствованию разработанного ранее программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании (разработка блок-схемы и программы на языке Visual Basic). *Данные работы опубликованы*:
1. «Симметричное шифрование» - сборник аннотаций научно-исследовательских работ участников X научной конференции молодых исследователей « Шаг в будущее, Москва», секция IV, системы безопасности, подсекция 1-информационная безопасность., стр. 84, М., МГТУ им. Н.Э.Баумана (разработка ПО по реализации алгоритма шифрования, основанного на гаммировании (программы на языке объектно-ориентированного программирования Visual Basic, демо-версия),(см. сборник «Программа-Шаг в будущее, Москва»);
2 «Симметричное и асимметричное шифрование», аннотация к работе, сборник аннотаций научно-исследовательских работ участников XI научной конференции молодых исследователей
«Шаг в будущее, Москва», секция IV, системы безопасности, подсекция 1.-информационная безопасность, (разработка ПО по реализации алгоритмов ассиметричного шифрования, криптосистемы RSA, программы на языке программирования QBasic и языке объектно-ориентированного программирования Visual Basic, демо-версия (см. сборник);
3 «Гаммирование» - тезисы, в материалах V Городской научно-практической технической конференции школьников «Исследуем и проектируем»ДО г. Москвы, ГОУ Многопрофильный технический лицей № 1501,сборник –программа и тезисы, Москва., Издательский Центр, ГОУ ВПО МГТУ «СТАНКИН»,стр.68-69;
4 «Симметричное шифрование (гаммирование)» - тезисы опубликованы в журнале «Сигма» № 6 , выпускаемом ФДП ГОУ ВППО «СТАНКИН» совместно с ОУМЦ СВАО, вся работа опубликована в сборнике материалов окружной научно-исследовательской конференции № 3 «Математика: знание и реальность”, СВОУ ДО г. Москвы;
5 Проектные работы, представленные на I и II Международные студенческие конференции по информационной безопасности «IT-security conference for new generation»- по теме «Криптография. Актуальность в современном обществе»; опубликованы в сборниках материалов конференций (тезисы на русском и английском языках) и на сайте.
6. Статья «Симметричное шифрование- гаммирование» , Электронный журнал «Наука и образование: электронное научно-техническое издание», Эл № ФС 77-30569, гос.регистрация № 0421100025.раздел «Информатика, Вычислительная техника и управление», фонд «Электронная библиотека».
7.Гончаров Н.О. Статья «Симметричное шифрование», сборник работ и тезисы конференции «Студенческая весна », МГТУ им. Н.Э. Баумана.

*Данные проекты стали победителями:*
1. I и II Международных студенческих конференций по информационной безопасности «IT-security conference for new generation», Лаборатория Касперского, получены Дипломы II степени в номинации «Криптография. Актуальность в современном обществе»;
2. X научная конференция молодых исследователей «ШАГ В БУДУЩЕЕ. Москва», МГТУ им. Баумана, сертификат-тема «Информационная безопасность»;
3.Лауреат I степени XI научной конференции молодых исследователей «Шаг в будущее, Москва», МГТУ им. Баумана, диплом и медаль за лучшую научную работу по направлению «системы безопасности», секция IV, системы безопасности, подсекция 1-информационная безопасность.
4. Окружная научно-исследовательская конференция «Математика: знание и реальность”, диплом I степени в области естественно-математических наук, МГУ ПС ( МИИТ);
5. Городская научно-практическая техническая конференции школьников «Исследуем и проектируем» ДО г. Москвы, МГТУ «СТАНКИН», диплом III степени, сертификат, направление: «информационные системы»;
6. Выставка "Дни Московского образования на ВВЦ", доклад по направлению естественно-математических наук.