Министерство образования Республики Беларусь

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.725.5

Шакалей
Марина Борисовна

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ЛОКАЛЬНОЙ СЕТИ

АВТОРЕФЕРАТ

на соискание степени магистра информатики и вычислительной техники по специальности 1-40-80-04 «Математическое моделирование, численные методы и комплексы программ»

_____

Научный руководитель
Липницкий Валерий Антонович
профессор, доктор технических наук

_____

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время первостепенным фактором, влияющим на политическую и экономическую составляющие безопасности, является степень защищенности информации и информационной среды. Поэтому важное значение приобретают вопросы обеспечения безопасности информационных технологий и гарантированной защиты данных в компьютерных сетях.

Для разработки современных средств защиты информации вопрос о необходимости применения криптографического преобразования информации стал очевидным. Надежная защита информации может быть обеспечена только на базе комплексного сочетания организационных мер с физическими, аппаратно-программными и криптографическими методами. При этом роль криптографических методов продолжает возрастать. Увеличение количества информации, обрабатываемой, передаваемой и хранимой в автоматизированных системах управления предприятий и организаций привело к повышению актуальности задач: обеспечения конфиденциальности, целостности, неотрицания авторства; создания защищенного электронного документооборота; обеспечения высокой скорости обработки и подписания.

В основу обеспечения безопасности электронного документооборота (ЭД) составляют системы электронной цифровой подписи (ЭЦП). Целью применения систем цифровой подписи является аутентификация информации - защита участников информационного обмена от навязывания ложной информации, установление факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений.

Система ЭЦП предусматривает, что каждый пользователь имеет свой секретный ключ, который используется для формирования подписи, а также соответствующий ему открытый ключ, предназначенный для проверки подписи и распространенный среди определенного круга пользователей, входящих в систему информационного обмена.

Если пользователи системы доверяют друг другу, то для защиты информации могут применяться методы, основанные на использовании итерированных симметричных криптографических алгоритмов. Отличительной чертой таких методов является наличие одинаковых возможностей у отправителя и получателя информации. Поэтому, если получатель утверждает, что получил защищенное сообщение от некоторого отправителя, а тот отрицает факт отправления данного сообщения, то виновную сторону установить средствами информационной системы невозможно.

В случае взаимного недоверия субъектов системы защита информации обеспечивается на основе криптографии с открытым ключом. Эти криптографические методы обеспечивают более широкие функциональные возможности. Другой отличительной чертой криптографии с открытым ключом является то, что она строится на основе узкого класса дискретных математических структур (конечные группы, кольца, поля и др.), удобных для выполнения вычислений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования.Целью диссертационной работы является повышение эффективности систем криптографической защиты информации, используяметод формирования и проверки электронной цифровой подписи на основе открытого ключа.Разработка подхода к созданию и строения системы защиты электронных документов от подделки, обеспечивающая повышение уровня защищенности документов от их фальсификации.

Главной задачей диссертационного исследования является разработка технических решений, обеспечивающих повышение безопасности передачи сообщений в алгоритмах, основанных на сложности задачи факторизации и проблемах дискретного логарифмирования, и посредством этого расширения областей их практической применимости в автоматизированных системах поддержания технологии криптографической защиты.

Для решения поставленной задачи в ходе выполнения диссертационных исследований решались следующие частные задачи:

1) изучить известные подходы к синтезу алгоритмов и протоколов аутентификации информации;
2) разобрать схемы потенциальных атак на известные схемы основанные на сложности задачи дискретного логарифмирования;
3) разобрать схемы потенциальных атак на известные схемы, основанные на сложности задач факторизации;
4) разработка подходов к сокращению размера ЭЦП в схемах, основанных на сложности задачи факторизации;
5) разработка подходов к повышению безопасности ЭЦП в схемах, основанных на преобразовании раундовой хэш-функции и системы сертифицирующегося открытого ключа;
6) разработка схем и алгоритмов реализации разработанных подходов;
7) реализация алгоритма на платформе .NetFramework;
8) анализ разработанной схемы и алгоритма.

Новизна полученных результатов. Новизна результатов диссертационногоисследования заключается в одновременном применении алгоритмов электронной цифровой подписи, основанных на различных вычислительных задачах в рамках исследованной технологии. Сегодня сложно найти информационную систему, которая бы не использовала криптографию. Коммерческие системы в большинстве своем используют криптографические примитивы, которые внесены уже в стандарты США, но возникают ситуации, когда такой вариант неприемлем. В данной работе представлен алгоритм внедрения разработанной криптографической схемы на языке C# на платформе .NetFramework. Основными результатами являются:

1. Способ повышения защищенности электронных документов от подделки, путем использования алгоритмов ЭЦП, основанных на двух независимых трудных вычислительных задачах.
2. Разработка подхода к повышению криптостойкости цифровой подписи, основанной на сложности задачи факторизации.
3. Разработка алгоритмов формирования и проверки подлинности цифровой подписи.
4. Оценка параметров разработанного алгоритма, обеспечивающий заданный уровень защищенности автоматизированной системы поддержания технологии криптографической защиты документов от подделки.
5. СредаCLRиспользует разработанный алгоритм по умолчанию.

Основным результатом работы является повышение уровня защищенности документов от подделки.

Положения,выносимыеназащиту.Повышение стойкости технологии криптографической защиты документов от подделки путем комбинирования двух ЭЦП сравнительно малого размера, стойкость которых основана на двух независимых трудных вычислительных задачах.

1. Подход к сокращению размера ЭЦП, основанной на сложности задачи факторизации.
2. Алгоритмы формирования ЭЦП сокращенного размера, основанные на сложности задачи факторизации.
3. Условия, накладываемые на выбор параметров разработанных алгоритмов ЭЦП, обеспечивающие их стойкость.

Апробация результатов диссертации. Основные результаты диссертационной работыдокладывались на 52-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР.

Опубликованностьрезультатовисследования.По теме диссертации опубликованы два тезиса,один из которых опубликован сборнике научной конференции БГУИР и второй в сборнике российской научно-техническойконференции.

Структура и объем диссертации.Диссертация состоит из введения, 5 глав,заключения и списка литературы. Диссертационная работа изложена на 72 страницах, работа содержит 5 рисунка, 1 таблицы, список литературы из 43 наименований и приложения.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Результаты проведённых исследований изложены в пяти главах.

В первой главе произведён обзор предметной области задач, решаемых в рамках данной работы. Рассмотрены системы защиты информации, а именно криптографические алгоритмы и протоколы аутентификации для защиты информации в информационных системах. Рассмотрены понятия электронной цифровой подписи и протокола распределения ключей. Обсуждаются современные методы аутентификации электронной информации на основе алгоритмов ЭЦП с открытым ключом. Детально рассматриваются и анализируются известные схемы ЭЦП, такие как RSA и Эль-Гамаля. Проводится анализ современных систем и выявляются их недостатки с позиций обеспечения информационной безопасности.

Во второй главе выполнена постановка научной задачи исследования. Определены цель проведения диссертационного исследования.

Третья глава диссертационной работы рассматриваетустройство криптографической подсистемы .NET Framework, представленной в пространстве имен System.Security.Cryptographi. Изучается устройство и преимущества языка программирования C#.

Четвертая глава посвящена детальному анализу алгоритма хэш-функции и система самосертифицирующего ключа; построению булевой алгебры; разрабатываются подходы, схемы и алгоритмы электронной цифровой подписи, обеспечивающие повышение безопасности ЭЦП при использовании задачи факторизации и проблемы дискретного логарифмирования в качестве базовой сложной задачи. Производится реализация алгоритма в .NET Framework.

В пятой главе произведен анализ временной сложности; анализ безопасности;анализ спроектированного алгоритма криптографической защиты H-S DSA, основанного на преобразовании хэш-функции и самосертифицирующегося ключа.

В заключении сформулированы основные результаты работы, кратко охарактеризована их новизна и практическая ценность. Сделан вывод о степени выполнения поставленных задач и достижении цели исследований.

ЗАКЛЮЧЕНИЕ

В данном диссертационном исследовании разработан подход к созданию схемы криптографической защиты, основанной на применении электронной цифровой подписи, как аутентификации и решен вопрос о повышении уровня защищенности от широкого спектра атак на систему, что определяет практическую важность темы диссертационного исследования. Детально изучены известные алгоритмы шифрования с открытым ключом. В соответствии с поставленными целями и задачами, в результате проведенных исследований и разработок были получены следующие результаты.

Проанализированы и обобщены некоторые цифровые алгоритмы подписи, которые являются относительно зрелыми и часто используемыми. В частности, более подробно рассмотрены схемы RSA и Эль-Гамаля. На этой основе были изучены алгоритмы циклической хэш-функции и система сертифицирующегося открытого ключа.

В результате цель работы была достигнута. Разработан и реализован алгоритм цифровой подписи аналогичный Эль-Гамаля (H-S DSA). Предложен способ реализации криптосистемы с открытым ключом, безопасность которого основывается отчасти на сложности факторизации чисел и задаче дискретного логарифмирования. Так же представлен алгоритм внедрения разработанной криптографической схемы на языке C# на платформе .NetFramework.

Сделана оценка эффективности схемы. Из анализа безопасности алгоритма, следует, что разработанный алгоритм обладает достаточной прочной безопасностью, она может эффективно противостоять всем видам атак на пароли, в том числе линейных и дифференциальных атак. H-S DSA алгоритм использует одностороннюю хэш-функцию, и её безопасность главным образом лежит на циклической хэш-функции, используемой в каждом раунде. В добавок к односторонней хэш-функции, безопасность H-S DSA так же зависит от следующих двух хорошо известных предположений: проблема дискретного логарифма и задачи факторизации. Из анализа временной сложности известно, что разработанный алгоритм имеет более низкую временную сложность. Безопасность H-S DSA лучше по сравнению с алгоритмом цифровой подписи Эль-Гамаля, и временная сложность H-S DSA не более, чем у алгоритма Эль-Гамаля. Таким образом можно считать, что алгоритм H-S DSA осуществим.

Алгоритм формирования и проверки электронной цифровой подписи H-S DSA, основанный на сложности задачи факторизации, проблеме дискретного логарифмирования, преобразовании раундовой хэш-функции и системе самосертифицирующегося ключа пригоден для применения в технологии криптографической защиты электронных документов от подделки.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1 - А.] Шакалей М.Б. Схема RSAна основе простого числа / М.Б. Шакалей // 52-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР: Тезисы доклада - Минск, 2016 - С. 25.

[2 - А.] Шакалей М.Б. Схема RSAна основе простого числа / М.Б. Шакалей // 52-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР: Тезисы доклада - Минск, 2016 - С. 24 - 25