Титков Е.В.
Научный руководитель: доцент каф. ФПМ, к.т.н. Р.А. Штыков
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: rm4life95@gmail.com

Обзор и анализ методов криптографии

С каждым годом компьютерная информация играет все более важную роль в нашей жизни, и все большую актуальность приобретают проблемы ее защиты. Каждый пользователь при общении хочет иметь защищённую сеть для обмена данными что бы передача данных была безопасной и не один злоумышленник не смог прочитать конфиденциальные данные. Для безопасной передачи данных криптография используется в беспроводных и проводных сетях, где простой текст преобразуется в шифр, а шифр преобразуется в простой текст.

Целью исследования является обзор и анализ методов крифтографии.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор методов криптографии.
2. Анализ выбранных криптосистем.
3. Результаты исследования.

Обзор методов криптографии

Криптография делится на симметричную и асимметричную. В симметричной один и тот же ключ используется обоими сторонами. Отправитель использует такой ключ для шифрования данных, а получатель для их расшифровки. В асимметричной используются два ключа, открытый и закрытый. Закрытый ключ хранится у получателя и защищен паролем, который известен только владельцу, а открытый ключ известен всем пользователям. Рассмотрим некоторые широко используемые асимметричные криптосистемы: RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA(Digital Signature Algorithm), ECC (Elliptic curve cryptography).

RSA

Алгоритм асимметричной криптосистемы с открытым ключом основанный на предполагаемой сложности факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложение числа на простые множители.

Diffie-Hellman

Данный алгоритм позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.

Digital Signature Algorithm (DSA)

Криптографический алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования (в отличие от RSA и схемы Эль-Гамаля). Подпись создается секретно, но может быть публично проверена. Это означает, что только один субъект может создать подпись сообщения, но любой может проверить её корректность. Алгоритм основан на вычислительной сложности взятия логарифмов в конечных полях.

Elliptic Curve Cryptography (ECC)

Раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день не известно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования.

Таблица 1. Анализ криптосистем

№	Криптосистема	Анализ
1	Rivest Shamir and Adleman (RSA)	RSA может использоваться в мобильной связи так как она уязвимая ко многим атакам.
		RSA не подходит для WSN (беспроводная сенсорная сеть) из за высокой сложности
2	Diffie-Hellman Algorithm	Ключи передаются между двумя пользователями неизвестными друг другу
		Преследуют две цели: проверка подлинности закрытого ключа и подтверждение открытого ключа
		Может использоваться в интернете и почти в каждой криптосистеме используемой в интернете (SSL, SSH, IPSec)
3	Digital Signature Algorithm (DSA)	Используется приемником для проверки отсутствия изменений в принятом сообщении. Цифровая подпись используется для этой задачи.
		Результат хеш-функции зависит от размера данных
4	Elliptic Curve Cryptography (ECC)	Алгоритмы с открытым ключом которые могут предоставлять более короткую длину ключа и имеют большую производительность над системами основанными на факторизации и дискретных логарифмах
		Производительность ECC в 5, 15, 20, 60, а иногда и в 400 раз быстрее чем у других.

Результаты исследования

После рассмотрения всех вышеперечисленных криптосистем, можно сделать вывод что ECC быстрее чем RSA, потому что используются меньшие ключи. Но математически его операция сложна как у RSA. В алгоритме Diffie-Hellman секретный ключ обменивается между двумя пользователями. В то время как цифровая подпись используется получателем в DSA для подтверждения отсутствия изменений в принятом сообщении.

Литература

1. RSA [Электронный ресурс] // wikipedia.org: интернет портал URL: https://ru.wikipedia.org/wiki/RSA (дата обращения: 7.04.2017).

2. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Триумф, 2002

.