УДК 004.056.55

Студ. Е. Ю. Воронько
Науч. рук. ст. преп. П. Е. Сулим
(кафедра полиграфического оборудования и систем обработки информации, БГТУ)

ОБЗОР МЕТОДОВ ШИФРОВАНИЯ DES И AES

Необходимость скрывать сообщения и их значение от посторонних глаз, возникла вскоре после того, как человечество изобрело письменность. Шифрование используется в основном для обработки транзакций по небезопасным каналам связи, таким как Интернет.

Методы шифрования подразделяются на две категории – симметричные (AES, 3DES, CAST, DES, ГОСТ) и ассиметричные (RSA El-Gamal) методы. Рассмотрим основные алгоритмы симметричного шифрования: AES (Advanced Encryption Standard) и DES (Data Encryption Standard).

Стандарт шифрования данных (DES) представляет собой блочный шифр с симметричным ключом, основан на структуре Feistel, в которой открытый текст разделен на две половины. Для получения 64-битного зашифрованного текста требуется ввод в виде 64-битного открытого текста и 56-битного ключа. Перед обработкой весь обычный текст разделяется на две части по 32 бита каждая, и над каждой частью выполняются одни и те же операции. Каждый фрагмент проходит 16 раундов операций, прежде чем используется окончательная перестановка для получения 64-битного зашифрованного текста.

Расширенный стандарт шифрования (AES) также является блочным шифром с симметричным ключом. Национальный институт стандартов и технологий опубликовал AES в 2001 году. Поскольку DES использует относительно короткий ключ шифрования, а алгоритм был довольно медленным, для его замены был введен AES.

В AES обычный текст считается 126 битами, эквивалентными 16 байтам с 128-битным секретным ключом для генерации квадратной матрицы (имеющей 4 строки и 4 столбца). Затем он выполняет 10 раундов после этого шага. Из них 9 раундов содержат следующие этапы: суббайты, сдвиг строк, смешивание столбцов и добавления круглых ключей. Последний, $10^{-й}$ раунд включает в себя все вышеуказанные операции, за исключением «Смешивания столбцов», для получения 126-битного зашифрованного текста [1].

Рассмотрев основные алгоритмы симметричного шифрования, различия каждого из них отмечены в таблице.

Таблица – Сравнение алгоритмов симметричного шифрования DES и AES

Характеристики	Алгоритм DES	Алгоритм AES
Базовые модели	Блок данных в DES разделен на две половины.	Весь блок в AES обрабатывается как единая матрица.
Принцип	Работает на структуре шифра Фейстеля.	В AES используется принципы подстановки и перестановки.
Разработан	DES был разработан IBM.	AES был разработан Винсентом Раймоном и Джоаном Даеманом.
Раунды	16 раундов.	10 раундов для 128-битного алгоритма, 12 раундов для 192-битного алгоритма, 14 раундов для 256-битного алгоритма
Скорость	DES работает медленнее, чем AES.	AES быстрее.
Безопасность	Поскольку DES использует меньший ключ, он менее защищен.	Является более безопасным, благодаря большому секретному ключу.
Открытый текст	Состоит из 64 бит.	Может содержать 128,192 или 256 бит.
Размер блока	128 бит.	64 бита.
Происходят из	DES происходят из шифра Lucifer.	AES происходят из квадратного шифра.

Рассмотренные основные алгоритмы шифрования DES и AES, а также составлен небольшой сравнительный анализ алгоритмов по отношению друг к другу. В результате анализа можно сделать вывод, что DES – является более устаревшим алгоритмом, а AES – алгоритм, который безопаснее и быстрее.

ЛИТЕРАТУРА

1. Криптоалгоритмы. Классификация с точки зрения количества ключей [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/336578/ – Дата доступа: 15.03.2023.

УДК 004.413.5:665

Студ. Д.М. Пирейко
Науч. рук. ст. преп. П.Е. Сулим
(кафедра полиграфического оборудования и систем обработки информации, БГТУ)

ИЗУЧЕНИЕ ВОЗМОЖНЫХ СПОСОБОВ АВТОМАТИЗАЦИИ В ПОЛИГРАФИИ СРЕДСТВАМИ ПЛАТФОРМЫ ARDUINO

Автоматизация позволяет частично или полностью освободить человека от исполнения циклических процессов, или процессов, выполняющихся по строго заданному алгоритму. В настоящее время трудно себе представить производство, где вся или часть процессов