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

контролируются без ведома человека, уведомляя его только в случае неисправности или предаварийной ситуации.

Развитие автоматика получила благодаря промышленно-техническому прогрессу. Даже автоматизация в быту берёт своё начало на промышленных производствах, где стремление к ускорению процесса и, соответственно, увеличение выручки способствовало внедрению новейших на тот момент наукоемких средств автоматизации.

Так же автоматизированные производства позволяли высвобождать большое количество рабочих рук, оптимизируя время и занятость персонала.

Arduino как платформа для разработки домашних средств автоматизации весьма успешна по ряду причин:

- небольшие размеры платы;
- гибкость программирования;
- скорость опроса;
- гигантское количество различных датчиков и модулей расширения;
- дешевизна платы.

Все те же плюсы актуальны и для промышленных объектов. В случае если проект в ходе эксплуатации будет изменен, его схему будет очень легко изменить, добавив или удалив необходимый компонент.

Неоспоримым плюсом станет наличие встроенного в плату программатора, который работает от USB кабеля, таким образом прошивку так же можно поменять на любой десктопной системе без каких-либо сложностей.

Важно отметить, что язык Arduino – видоизмененный C++, что позволит пользователям знакомым с ним быстрее адаптироваться под особенности платформы. Так, например, готовый к загрузке на плату код принято называть sketch-ем.

Еще одним плюсом станет крупное сообщество вокруг платформы. За время существования проекта вокруг него сформировалось крупное комьюнити, которое всегда подскажет разработчику в его начинаниях или же предостережет от ошибок. Не меньшую роль отводиться полной документации на официальном сайте https://arduino.ru.

Исходя из достоинств, рассмотрим возможные варианты применения платформы в промышленных целях. Первый и самый очевидный вариант – это богатое обилие модулей с датчиками. Плата запросто может отслеживать наличие и количество листов бумаги, количество краски (тонера) или любого другого красящего вещества. Также и отслеживание температуры отдельных объектов, таких как печатная пластина в контактно-копировальной установке. Сама плата предо-

ставляет пользователю возможность использования логических сигналов.

Для полиграфии это значит, что в случае превышения сенсорными датчиками определенных значений, программа платы позволяет подать логический аварийный сигнал в систему устранения или предотвращения неисправности. Например, аварийно включить систему вентиляции или перевести металлогалогенную (или любую другую) лампу в дежурный режим. То же можно сказать и о системе подачи запечатываемого материала: в случае нехватки плата спровоцирует пополнение [1, 2].

Другим плюсом станет возможность организации инфраструктуры из множества плат, которые объединены в единую сеть. Предположим, что одна отдельно взятая плата обслуживает датчики одного конкретного печатного станка.

Объединив несколько плат в одну сеть, состояние этих плат может считывать одна головная, которая, в случае неисправности дочерней, сообщит администратору о необходимости произведения ручного технического обслуживания.

Поле для возможных экспериментов крайне широко и требует изучения вопроса с точки зрения целесообразности с подробным изучением аналогов и подводных камней конечного проекта.

ЛИТЕРАТУРА

1. Грибков, А. В. Допечатное оборудование / А. В. Грибков, Ю. Н. Ткачук. – М.: МГУП, 2008. – 268 с.

2. Ефимов, М. В. Автоматизированное управление полиграфическим производством / М. В. Ефимов. – М.: МГУП «Мир книги», 1998.– 416 с.

УДК 676.01

Студ. И. В. Бадеев
Науч. рук. доц. О. П. Старченко
(кафедра полиграфических производств, БГТУ)

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ТЕХНОЛОГИЧЕСКИХ ПАРАМЕТРОВ НА КАЧЕСТВО ОПЕРАЦИИ РАЗРЕЗКИ НЕОТПЕЧАТАННЫХ ЛИСТОВ

Цель данной работы – изучить влияние плотности бумаги и высоты разрезаемой стопы на точность выполнения операции резки. Этот параметр будет оцениваться по максимальной величине косины листа из разрезанной стопы. Разрезке подвергается незапечатанная бумага, т. е. целью операции разрезки в данном случае служит подготовка бумаги к формату печатного оборудования.