Ministerul Educaţiei, Culturii şi Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere

Şef departament TSE: Sava Lilia conf. univ., dr.

„ _ ” _____ 2020

PROIECTAREA ŞI CERCETAREA DISPOZITIVELOR CRIPTOGRAFICE BAZATE PE ARDUINO UTILIZÎND LIMBAJUL DE PROGRAMARE VIZUAL XOD

РАЗРАБОТКА И ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ УСТРОЙСТВ НА ОСНОВЕ ARDUINO С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ВИЗУАЛЬНОГО ПРОГРАММИРОВАНИЯ XOD

Teză de master

Student: **Curlat Vitali, SISRC-191**

Conducator: **Puşneac Iurii conf. univ., dr.**

Consultant: **Şestacova Tatiana conf. univ., dr**

Chişinău – 2020

REZUMAT

CURLAT VITALI

Tema: Proiectarea și cercetarea dispozitivelor criptografice bazate pe Arduino utilizănd limbajul de programare vizual XOD.

Structura lucrării: Introducere, 3 Capitole, Concluzii, Bibliografie

Cuvinte-cheie: Criptografie, XOD, Arduino, Programare, Criptare, Generator, secvențe pseudo-aleatorii.

Scopul lucrării: Proiectarea și cercetarea dispozitivelor criptografice bazate pe Arduino utilizănd limbajul de programare vizual XOD.

Obiectivele lucrării: analiza capacităților tehnice ale Arduino, analiza mediului de programare a blocului XOD, analiza metodelor de criptografie cu rezistență acceptabilă, găsirea unui compromis pentru implementarea metodelor de criptografie cu rezistență acceptabilă în mediul de dezvoltare XOD pentru Arduino, crearea unui program de implementare a blocurilor criptografice în XOD, evaluarea rezistenței criptografice a algoritmului și a dispozitivului dezvoltat, asigurarea disponibilității unității criptografice create pentru utilizatorii mediului de dezvoltare XOD.

Metodele aplicate: În conformitate cu sarcina, au fost utilizate metode de programare a blocului XOD, programare C ++, generator de secvențe pseudo-aleatoare .

Rezultatele obținute: Pe parcursul lucrării, a fost găsit un compromis cu privire la implementarea dispozitivului criptografic pentru streamingul criptării datelor cu resurse limitate al Arduino. S-a realizat dezvoltarea elementului care lipsește (în limbajul de programare C ++). În mediul de dezvoltare XOD pentru Arduino, a fost implementat un generator de secvențe pseudo-aleatoare ca unitate separată. Blocul elaborat compilat și verificat în programul XOD pentru Arduino. A fost evaluată rezistența criptografică a algoritmului și a dispozitivului proiectat. Sunt identificate domeniile potențiale de aplicare a dispozitivului criptografic dezvoltat: criptarea datelor interne, criptarea fluxului de date pentru protocoale care se utilizeaza pentru comunicare intre dspozitive.

SUMMARY

CURLAT VITALI

Title: Elaboration and research of Arduino based cryptographic devices using the visual programming language XOD.

Thesis structure: Introduction, three chapters, Conclusions, Bibliography, Appendices.

Keywords: Cryptography, XOD, Arduino, Programming, Encryption, Generator, Pseudo-random sequence.

Thesis purpose: Elaboration and research of Arduino based cryptographic devices using the visual programming language XOD

Objectives: analysis of the technical capabilities of Arduino, analysis of the XOD block programming environment, analysis of cryptographic methods with acceptable strength, searching of a compromise for the implementation of cryptographic methods with acceptable strength in the XOD development environment for Arduino, developing a program for implementing a cryptographic block in XOD, evaluating the cryptographic strength of the algorithm and the developed device, ensuring the availability of the created cryptographic devices for users of the XOD development environment.

Applied methods: In accordance with the task, the methods of block programming XOD, C ++ programming, Pseudo-random number generator were used.

The Obtained Results: During design of the project, a compromise was found for the implementation of a cryptographic block for streaming data encryption with limited resources of Arduino devices. The development of the missing element was carried out (in the C ++ programming language). In the XOD development environment for Arduino, a pseudo-random sequence generator (PRS) was implemented as a separate block. The model was compiled in the XOD program for Arduino. The cryptographic strength of the algorithm and the developed device is assessed. Potential areas of application of the developed cryptographic device are identified: encryption of internal data, encryption of data flow for protocols that are used for communication between devices.

`

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……..….9

1. АНАЛИЗ СЕМЕЙСТВА КОНТРОЛЛЕРОВ ARDUINO, ХАРАКТЕРИСТИКИ, ДОСТОИНСТВА, ОГРАНИЧЕНИЯ……..10

1.1 Анализ технических характеристик Arduino UNO……...…10

1.2. Анализ технических характеристик Arduino Nano……..14

1.3. Анализ технических характеристик Arduino Pro Mini…….……...18

2. АНАЛИЗ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ ГРАФИЧЕСКОГО ЯЗЫКА XOD…….....…...23

2.1 Описание графического языка программированияXOD…….23

2.2 Особенности графического языка программирования XOD……..24

2.3 Создание нод для XOD в C ++……..25

3. МЕТОДЫ ШИФРОВАНИЯ ДАННЫХ НА ОСНОВЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ…….……...29

3.1 Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью……29

3.2 Поточные шифры…….……...35

3.3 Принцип побитного шифрования. Схема шифрования /расшифрования…….36

3.4 Генератор на основе регистра с линейной обратной связью……...……...39

3.5 Генератор псевдослучайных последовательностей и регистр с линейными обратными связями……..40

3.6 Примитивные полиномы……...…….41

4. РАЗРАБОТКА КРИПТОГРАФИЧЕСКИХ УСТРОЙСТВ НА ОСНОВЕ ARDUINO С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ВИЗУАЛЬНОГО ПРОГРАММИРОВАНИЯ XOD…….44

4.1 Разработка генератора Конфигурация – Галуа……44

4.2 Разработка генератора Конфигурация – Фибоначи……46

4.3 Реализация генератора псевдослучайных последовательностей на C++…….….48

`

4.4 Реализация генератора псевдо-случайных последовательностей в XOD.....55

ЗАКЛЮЧЕНИЕ ……65

БИБЛИОГРАФИЯ…….67

ПРИЛОЖЕНИЯ…….68

1 Код программы генератора псевдо-случайных последовательностей на 3 бита...68

2 Код программы генератора псевдо-случайных последовательностей на 5 бит….69

ВВЕДЕНИЕ

В настоящее время корректный анализ, обработка и достоверность данных как никогда актуальны. Сегодня , в период 4 индустриальной революции, когда мир делает новый шаг к автоматизации систем, как никогда важно обеспечить информационную безопасность.

Каждый из протоколов функционирует по определенным правилам , учитывает возможные сбои в процессе передачи данных. В основном своем большинстве протоколы использующиеся при коммуникации между микроконтроллерами просты и открыты так как аппаратно- вычислительный ресурс у них ограничен, что является минусом, так как не составляет большого труда злоумышленникам вмешаться в процессы работы управляемых систем.

Целью работы является: Разработка и исследование криптографических утройств на основе Arduino с использованием визуального программирования.

Поставлены следующие задачи:

1. Анализ технических характеристик различных плат Arduino, доступности в использовании. Ознакомление с графической платформой программирования XOD, общими принципами функционирования графического программирования.
3. Анализ особенностей, преимуществ и недостатков платформы XOD при программировании плат Arduino.
4. Изучение базовых принципов написание блоков нод для блочного языка програмирования XOD.
5. Анализ базовых принципов шифрования.
6. Разработка криптографического устройства и реализация программного кода блока шифрования, внедрение его в XOD

В качестве инструментов решено использовать среду блочного программирования XOD. На данный момент в библиотеках XOD не реализованы методы шифрования данных, что на сегодняшний день является одним из недостатков.

Созданный блок шифрования может применятся в качестве защиты канала связи от передатчика к приемнику, зашифровывая данные и не оставляя возможности перехвата и изменения информации.

БИБЛИОГРАФИЯ

Книги и публикации онлайн

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.
2. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.
4. Ростовцев А.Г., Макховенко Е.Б. Теоретическая криптография. - М., ред. Профессионал, 2005. - 490 р
5. Х.К.А.Ван Тилборг Основы криптологии. Профессиональное руководство и интерактивное руководство. - М., Мир, 2006. - 471 стр

Site web

1. Документация XOD, 1 octombrie 2018 [citat 11 iunie 2019].доступен: https://xod.io/ru/docs/tutorial
2. Документация , 3 noiembrie 2018 [citat 12 octombrie 2019].доступен: https://radioprog.ru/shop/merch/8
3. Документация Arduino, 18 iunie 2019 [citat 19 mai 2020].доступен: https://radioprog.ru/shop/merch/2
4. Визуальная среда разработки XOD ID, 10 august 2016 [citat 19 iunie 2019].доступен**:** https://amperka.ru/page/xod-ide
5. Семейство контроллеров Arduino, 25 iulie 2013 [citat 12 mai 2018].доступен: https://docplayer.ru/26007802-Glava-2-obzor-kontrollerov-semeystva-arduino-22.html.
6. Язык программирования XOD , 11 octombrie 2019 [citat 18 martie 2020].доступен: https://en.wikipedia.org/wiki/XOD_(programming_language)
7. Определения шифрования, 18 aprilie 2018 [citat 23 iunie 2019].доступен: https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5
8. Виды шифрования , 11 decembrie 2019 [citat 18 decembrie 2019].доступен: https://habr.com/ru/post/449552/
9. Гид по языку XOD, 4 ianuarie 2019 [citat 8 iulie 2019].доступен: https://xod.io/docs/guide/nodes-for-xod-in-cpp/
10. Список неприводимых и простых полиномов, 7 februarie 2015 [citat 5 mai 2017]. доступен: https://intuit.ru/studies/courses/553/409/lecture/17864
11. Создание ноды в XOD : https://xod.io/docs/guide/nodes-for-xod-in-cpp/