TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN
ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

СОЗДАНИЕ ПРОГРАММЫ ДЛЯ ИМИТАЦИИ ШИФРОВАНИЯ МАШИНЫ ENIGMA НА ЯЗЫКЕ PYTHON

Tursunbek Sadriddinovich Jalolov
Asia International University
ts_jalolov@oxu.uz

Абстрактный: В данной статье представлен процесс создания программы для моделирования машинного шифрования Enigma на языке Python. «Enigma» — шифровальное устройство, использовавшееся немцами во время Второй мировой войны, и его было очень трудно взломать. Программа моделирования предназначена для воспроизведения функциональности реальной машины «Enigma» и предоставляет инструмент для понимания и экспериментирования с процессом шифрования.

Ключевые слова:

Машина «Enigma», шифрование, Python, симуляция, шифровальное устройство, Вторая мировая война

Машина «Enigma» — легендарное шифровальное устройство, сыгравшее значительную роль во Второй мировой войне. Разработанная немецким инженером Артуром Шербиусом машина использовалась для безопасной передачи конфиденциальной информации. Из-за сложности алгоритма шифрования союзным войскам было чрезвычайно сложно декодировать перехваченные сообщения, что в конечном итоге сделало его ключевым компонентом немецкой разведки.

В этой статье мы обсудим создание программы на Python, которая имитирует процесс шифрования машины Enigma. Цель программы — предоставить пользователям практический опыт понимания механики машины «Enigma» и ее криптографических функций. Благодаря этому моделированию пользователи смогут получить представление о проблемах, с которыми столкнулись взломщики кодов во время войны, и оценить значение шифрования в современной кибербезопасности.

Машина Enigma была одним из самых сложных шифровальных устройств времен Второй мировой войны, используемым немецкими вооруженными силами для шифрования и дешифрования сообщений. Эта машина использовала механические роторы для преобразования входящих букв в шифрованные символы, что делало ее очень сложной для взлома.

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

Сегодня программирование машины Enigma может быть увлекательным проектом для тех, кто интересуется историей шифрования и программированием. В этой статье мы рассмотрим, как создать программу для имитации работы машины Enigma на языке программирования Python.Для начала, мы должны понять, как работала машина Enigma. Основная идея заключалась в том, что каждое нажатие клавиши шифровалось с использованием простой замены буквы. Например, при вводе буквы "A" на машине Enigma она могла быть преобразована в букву "D", в зависимости от настроек роторов.Для создания программы имитации машины Enigma на языке Python, нам понадобится создать алгоритм, который будет преобразовывать входящие символы в соответствующие шифрованные символы. Мы также должны имитировать работу роторов, которые меняются при каждом нажатии клавиши.

Примерной программой для имитации машины Enigma на языке Python может быть:

```python
class EnigmaMachine:
    def __init__(self):
        self.rotors = ['EKMFLGDQVZNTOWYHXUSPAIBRCJ', 'AJDKSIRUXBLHWTMCQGZNPYFVOE',
'BDFHJLCPRTXVZNYEIWGAKMUSQO']
        self.reflector = 'YRUHQSLDPXNGOKMIEBFZCWVJAT'
        self.position = [0, 0, 0]

    def encrypt(self, letter):
        output = letter
        for rotor in self.rotors:
            output = rotor[(ord(output) - ord('A') + self.position[i]) % 26]
        output = self.reflector[ord(output) - ord('A')]
        for rotor in reversed(self.rotors):
            output = chr((rotor.index(output) - self.position[i] + 26) % 26 + ord('A'))
        return output

    def rotate(self):
        self.position[0] = (self.position[0] + 1) % 26
        if self.position[0] == 0:
            self.position[1] = (self.position[1] + 1) % 26
            if self.position[1] == 0:
                self.position[2] = (self.position[2] + 1) % 26
```

В этом примере программы мы создаем класс EnigmaMachine, который имеет методы для шифрования и вращения роторов. Мы также определили алгоритм для каждого ротора и для рефлектора, чтобы можно было преобразовать входящий символ в шифрованный и наоборот. После создания такой программы можно провести тесты, используя известные сообщения и различные комбинации настроек роторов, чтобы убедиться, что программа

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

правильно имитирует работу машины Enigma. Создание программы для имитации машины Enigma на языке Python - увлекательный проект, который не только позволяет изучить историю шифрования, но и улучшить навыки программирования на языке Python.

Создание программы моделирования:

Чтобы создать программу моделирования, нам сначала нужно понять основные принципы работы реальной машины «Enigma». Машина использовала ряд роторов, коммутационную панель и отражатель для шифрования и расшифровки сообщений. Эмулируя эти компоненты, мы можем воспроизвести процесс шифрования в нашей программе Python.

Мы начнем с определения основных функций машины «Enigma», таких как вращение ротора, замена букв и подключение коммутационной панели. Используя объектно-ориентированные возможности Python, мы можем инкапсулировать эти функции в классы, представляющие различные компоненты машины Enigma. Кроме того, мы реализуем пользовательские интерфейсы для ввода сообщений, настройки параметров компьютера и просмотра зашифрованных выходных данных.

На протяжении всего процесса разработки мы будем обращаться к историческим ресурсам и техническим документам, подробно описывающим работу машины Enigma. Это гарантирует, что наша программа моделирования точно отразит поведение исходного устройства и станет образовательным инструментом для изучения криптографических методов.

Машина «Enigma» остается увлекательной темой в истории криптографии, и ее влияние на современные методы шифрования неоспоримо. Создавая программу моделирования для машины «Enigma» на Python, мы стремились предложить практический и образовательный ресурс для энтузиастов и студентов, заинтересованных в понимании тонкостей криптоанализа. Благодаря этой программе пользователи смогут глубже понять проблемы, с которыми сталкиваются взломщики кодов во время войны, а также технологические достижения, которые сформировали сферу кибербезопасности. Моделируя процесс шифрования машины «Enigma», мы надеемся пробудить любопытство и исследования в области криптографии и внести свой вклад в сохранение исторических криптографических знаний.

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

Использованная Литература

1. Jalolov, T. S. (2023). PSIXOLOGIYA YO ‘NALISHIDA TAHSIL OLAYOTGAN TALABALARGA SPSS YORDAMIDA MATEMATIK USULLARNI O ‘RGATISHNING METODIK USULLARI. Educational Research in Universal Sciences, 2(10), 323-326.

2. Jalolov, T. S. (2023). PYTHON INSTRUMENTLARI BILAN KATTA MA’LUMOTLARNI QAYTA ISHLASH. Educational Research in Universal Sciences, 2(10), 320-322.

3. Jalolov, T. S., & Usmonov, A. U. (2021). “AQLLI ISSIQXONA” BOSHQARISH TIZIMINI MODELLASHTIRISH VA TADQIQ QILISH. Экономика и социум, (9 (88)), 74-77.

4. Sadriddinovich, J. T. (2023). Capabilities of SPSS Software in High Volume Data Processing Testing. American Journal of Public Diplomacy and International Studies (2993-2157), 1(9), 82-86.

5. Sadriddinovich, J. T. (2023, November). IDENTIFYING THE POSITIVE EFFECTS OF PSYCHOLOGICAL AND SOCIAL WORK FACTORS BETWEEN INDIVIDUALS AND DEPARTMENTS THROUGH SPSS SOFTWARE. In INTERNATIONAL SCIENTIFIC RESEARCH CONFERENCE (Vol. 2, No. 18, pp. 150-153).

6. Jalolov, T. S. (2023). TEACHING THE BASICS OF PYTHON PROGRAMMING. International Multidisciplinary Journal for Research & Development, 10(11).

7. Jalolov, T. S. (2023). Solving Complex Problems in Python. American Journal of Language, Literacy and Learning in STEM Education (2993-2769), 1(9), 481-484.

8. Jalolov, T. S. (2023). PEDAGOGICAL-PSYCHOLOGICAL FOUNDATIONS OF DATA PROCESSING USING THE SPSS PROGRAM. INNOVATIVE DEVELOPMENTS AND RESEARCH IN EDUCATION, 2(23), 220-223.

9. Jalolov, T. S. (2023). ADVANTAGES OF DJANGO FEMWORKER. International Multidisciplinary Journal for Research & Development, 10(12).

10. Jalolov, T. S. (2023). ARTIFICIAL INTELLIGENCE PYTHON (PYTORCH). Oriental Journal of Academic and Multidisciplinary Research, 1(3), 123-126.

11. Jalolov, T. S. (2023). SPSS YOKI IJTIMOIY FANLAR UCHUN STATISTIK PAKET BILAN PSIXOLOGIK MA’LUMOTLARNI QAYTA ISHLASH. Journal of Universal Science Research, 1(12), 207–215.

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

12. Jalolov, T. S. (2023). THE MECHANISMS OF USING MATHEMATICAL STATISTICAL ANALYSIS METHODS IN PSYCHOLOGY. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 138-144.

13. Jalolov, T. S. (2023). PROGRAMMING LANGUAGES, THEIR TYPES AND BASICS. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 145-152.

14. Jalolov, T. S. (2023). PYTHON TILINING AFZALLIKLARI VA KAMCHILIKLARI. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 153-159.

15. Jalolov, T. S. (2023). PYTHON DASTUR TILIDADA WEB-ILOVALAR ISHLAB CHIQISH. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 160-166.

16. Jalolov, T. S. (2023). SUN'IY INTELLEKTDA PYTHONNING (PYTORCH) KUTUBXONASIDAN FOYDALANISH. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 167-171.

17. Jalolov, T. S. (2023). WORKING WITH MATHEMATICAL FUNCTIONS IN PYTHON. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 172-177.

18. Jalolov, T. S. (2023). PARALLEL PROGRAMMING IN PYTHON. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 178-183.

19. Ikromova, S. (2023). INTERPRETATION OF THE PSYCHOLOGICAL SAFETY FACTOR IN RELATION TO DESTRUCTIVE INFORMATION IN ADOLESCENTS. Modern Science and Research, 2(9), 390-394.

20. Ikromova, S. (2023). CONCEPT OF IDEOLOGY AND FORMATION OF IDEOLOGICAL IMMUNITY IN YOUTH STUDENTS. Modern Science and Research, 2(6), 1223-1226.

21. Ikromova, S. (2023). FORMATION OF IDEOLOGICAL IMMUNITY TO DESTRUCTIVE INFORMATION IN TEENAGERS. Modern Science and Research, 2(5), 1009-1014.

22. Ikromova, S. A. (2022). MILLIY VA DINIY QADRIYATLARNING INSON TARBIYASIDAGI O'RNI. Экономика и социум, (12-2 (103)), 675-678.

23. Ikromova, S. A. (2023). SHAXS OG 'ISHGAN XULQINING KO 'RINISHLARI VA DESTRUKTIV AXBOROTLARNING KO 'RINISHLARI. Educational Research in Universal Sciences, 2(10), 528-532.

24. Akbarovna, I. S. (2023). YOSHLARDA DESTRUKTIV G'OYALARGA QARSHI IMMUNITET HOSIL QILISH OMILLARI.

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

25. Akbarovna, I. S. (2023). TALABA YOSHLARDA MAFKURA TUSHUNCHASI VA MAFKURAVIY IMMUNITETNI SHAKLLANTIRISH.

26. Akbarovna, I. S. (2023). O'SMIRLARDA DESTRUKTIV AXBOROTLARGA NISBATAN MAFKURAVIY IMMUNITET SHAKLLANTIRISH.

27. Akbarovna, I. S. (2023). DESTRUKTIV AXBOROTLARGA NISBATAN MAFKURAVIY IMMUNITET SHAKLLANTIRISH IJTIMOIY MUAMMO SIFATIDA. Barqaror Taraqqiyot va Rivojlanish Tamoyillari, 1(6), 26-29.

28. Akbarovna, I. S. (2023). MILLIY HARAKATLI O'YINLARNING BOLALAR TARBIYASIDAGI IJTIMOIY-PSIXOLOGIK XUSUSIYATLARI.

29. Sitora Akbarovna Ikromova. (2023). Formation of Ideological Immunity to Destructive Information. Intersections of Faith and Culture: American Journal of Religious and Cultural Studies (2993-2599), 1(9), 50–54.

30. Akbarovna, I. S. (2023). Study of the Formation of Ideological Immunity By Foreign and Russian Researchers. American Journal of Public Diplomacy and International Studies (2993-2157), 1(9), 235-239.

31. Akbarovna, I. S. (2023). Adolescence during Destructive Behavior Appearances the Problem Learning Condition. Intersections of Faith and Culture: American Journal of Religious and Cultural Studies (2993-2599), 1(9), 105-109.

32. Akbarovna, I. S. (2023). RESEARCH METHODS OF YOUTH PSYCHOLOGY. International Multidisciplinary Journal for Research & Development, 10(12).

33. Ikromova Sitora Akbarovna. (2023). NEUROPHYSIOLOGY BASIS OF HORMONES. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 68–77.

34. Akbarovna, I. S. (2023). Formation of Ideological Immunity to Destructive Information in Adolescents. American Journal of Public Diplomacy and International Studies (2993-2157), 1(10), 119-122.

35. Akbarovna, I. S. (2023). THE DEVELOPMENT OF CONSCIOUSNESS AND THE TEACHING OF CONCEPTS OF THE UNCONSCIOUS TO STUDENTS. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 107-114.

36. Ikromova, S. A. (2023). Cognitive processes and their description in psychology. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 115-133.

ISSN (E): 2992-9148
ResearchBib Impact Factor: 9.576 / 2023
VOLUME-1, ISSUE-5

37. Akbarovna, I. S. (2023). SOCIO-PSYCHOLOGICAL FACTORS OF BEHAVIOR FORMATION IN ADOLESCENTS. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 184-191.

38. Akbarovna, I. S. (2023). NEGATIVE AND POSITIVE CHANGES IN ADOLESCENT BEHAVIOR. TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN, 1(5), 192-197.

39. Ikromova, S. A. (2023). FACTORS IN THE DEVELOPMENT OF IMMUNITY TO DESTRUCTIVE IDEAS IN ADOLESCENTS. Innovation in Science, Education and Technology.

40. Malikovna, K. R. (2023). IQTISODIY MUSTAQILLIK–YANGILANAYOTGAN O ‘ZBEKISTON IJTIMOIY-IQTISODIY SALOHIYATINING MODDIY ASOSI. Scientific Impulse, 2(15), 18-22.

41. Karimova, R. N. M. (2018). DEVELOPMENT OF MOTIVATION IN HISTORY LESSONS USING ELEMENTS OF LOCAL LORE. In XLIII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE" INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS AND PROSPECTS OF MODERN SCIENCE AND EDUCATION" (pp. 121-123).

42. Karimova, R. M. (2020, March). The Participation of the Tajiks in the Development of Small and Medium-Sized Businesses in the Russian Far East. In International Scientific Conference" Far East Con"(ISCFEC 2020) (pp. 277-281). Atlantis Press.

43. Каримова, Р. М. (2020). ФИЛОСОФИЯ НЕЗАВИСИМОСТИ ЯВЛЯЕТСЯ ИДЕОЛОГИЧЕСКОЙ ОСНОВОЙ НАЦИОНАЛЬНОГО РАЗВИТИЯ СТРАНЫ. In EUROPEAN RESEARCH: INNOVATION IN SCIENCE, EDUCATION AND TECHNOLOGY (pp. 47-49).