УДК 004.4

В. Г. Сапега, М. В. Яснюк, Ю. Е. Горбач
Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь, daim777777@gmail.com

КИТАЙСКИЕ СТАНДАРТЫ ШИФРОВАНИЯ И КЛАССИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

В статье рассматриваются современные методы защиты информации в Республике Беларусь и криптографические стандарты, используемые в Китае. Анализируются ключевые особенности китайских SM-алгоритмов и их применение в национальных проектах. Также описаны классические методы шифрования, такие как шифр Цезаря, A1Z26 и шифр «Пляшущие человечки», рассмотрены принципы работы, достоинства и недостатки. Разработано веб-приложение для демонстрации шифрования этими методами, способствующее обучению основам криптографии и информационной безопасности.

Ключевые слова: криптография; SM-алгоритмы; шифрование.

V. G. Sapega, M. V. Yasnyuk, Y. E. Horbach
Institution of Education "Baranavichy State University", Baranavichy, the Republic of Belarus, daim777777@gmail.com

CHINESE ENCRYPTION STANDARDS AND CLASSICAL METHODS OF INFORMATION PROTECTION IN THE REPUBLIC OF BELARUS

The article discusses modern methods of information protection in the Republic of Belarus and cryptographic standards used in China. Key features of Chinese SM algorithms and their application in national projects are analyzed. Classic encryption methods, such as the Caesar cipher, A1Z26 and the Dancing Men cipher, are also described, their operating principles, advantages and disadvantages are considered. The web-application has been developed to demonstrate encryption using these methods, facilitating training in the basics of cryptography and information security.

Key words: cryptography; SM-algorithms; encryption.

Введение. В условиях современного цифрового мира защита личных данных и конфиденциальной информации становится одной из самых актуальных задач. Веб-приложение для шифрования

информации представляет собой инструмент, который позволяет эффективно обеспечивать безопасность данных в процессе их передачи и хранения в сети Интернет. Это значительно снижает риски утечек и несанкционированного доступа, что делает шифрование незаменимым элементом для защиты данных в различных сферах, включая финансовые, медицинские, правовые и корпоративные системы. Создание и использование веб-приложений для шифрования информации позволяет обеспечить высокий уровень конфиденциальности и безопасности для пользователей в цифровом пространстве.

Основная часть. Целью данного исследования являлась разработка веб-приложения для шифрования информации тремя методами: «Шифр Цезаря», «Шифр A1Z26», «Шифр пляшущих человечков».

Методы шифрования информации, используемые в Китае, охватывают широкий спектр технологий, включая международные стандарты и собственные разработки. Китай активно развивает криптографию, особенно в рамках кибербезопасности, чтобы обеспечить контроль над данными внутри страны. Китай разрабатывает собственные криптографические стандарты, известные как SM-алгоритмы, чтобы уменьшить зависимость от западных технологий:

SM2 — криптографическая система с открытым ключом (разновидность асимметричного шифрования, асимметричного шифра) для шифрования и/или электронной подписи [1]. SM2 разработан на основе эллиптических кривых. Криптография с эллиптической кривой — это важный тип шифрования в криптографии с открытым ключом, который использует эллиптическую кривую для шифрования и дешифрования [2].

Для удовлетворения требований приложений, таких как система электронной аутентификации, Государственное управление криптографии 17 декабря 2010 года выпустило криптографический алгоритм с открытым ключом SM2 и заявило о необходимости модернизации существующих систем [3].

SM3 — это криптографическая хэш-функция, используемая в китайском национальном стандарте. Она была опубликована Национальным управлением криптографии [4]. SM3 используется для реализации цифровых подписей, кодов аутентификации сообщений и генераторов псевдослучайных чисел [4].

SM3 применяется для хэширования данных в национальных проектах, таких как социальные кредиты и государственные базы данных.

SM4 — это блочный шифр, используемый в китайском национальном стандарте беспроводной локальной сети [5]. Алгоритм был разработан Центром обеспечения безопасности данных и связи Китайской академии наук и Центром тестирования коммерческой криптографии Национальной администрации криптографии [5]. SM4 применяется для шифрования данных в мобильных сетях, для безопасного хранения файлов и облачных сервисов.

Классические методы шифрования в Республике Беларусь:

1. Шифр Цезаря, также известный как шифр сдвига или код Цезаря, является одним из старейших и наиболее известных методов шифрования. Это вид шифра подстановки, при котором каждый символ исходного текста заменяется на символ, находящийся на фиксированном числе позиций влево или вправо в алфавите. Шифр называется шифром сдвига, поскольку основная идея заключается в сдвиге букв по алфавиту на определённое количество позиций [6].

Принцип работы шифра Цезаря: для шифрования текста с помощью шифра Цезаря используется ключ — число, которое указывает на количество позиций, на которые должны быть сдвинуты буквы. Например, если сдвиг равен 3, то буква «А» становится буквой «Г», «Б» — «Д», и так далее. Важно отметить, что после буквы «Я» (или «Z» в английском алфавите) сдвиг продолжается с первой буквы алфавита, что означает цикличность этого процесса [6].

Шифр получил своё название в честь римского императора и полководца Гая Юлия Цезаря, который использовал его для защищённой переписки с другими членами своей армии. Это позволило ему обеспечить секретность сообщений, отправляемых между различными военными частями. Цезарь использовал шифр с фиксированным сдвигом на 3 позиции, однако в те времена не существовало строгих стандартов безопасности, и защита сообщений была обеспечена только за счет сложности вскрытия шифра для того времени [6].

Несмотря на свою историческую значимость, шифр Цезаря имеет множество уязвимостей и считается очень простым для

взлома. Основная причина этого заключается в том, что существует всего 25 возможных вариантов сдвига (при использовании латинского алфавита), что делает его уязвимым к атакам с полным перебором [6].

Кроме того, шифр Цезаря является моноалфавитным шифром, то есть каждая буква исходного текста всегда заменяется на одну и ту же букву в зашифрованном сообщении. Это делает его уязвимым для криптоанализа, так как можно анализировать частотные характеристики символов (например, наиболее часто встречающиеся буквы в языке) и использовать это для расшифровки текста. Хотя шифр Цезаря не применяется в современных системах криптографии из-за своей уязвимости, он всё ещё находит применение в некоторых случаях. Например, шифр Цезаря используется в системе ROT13, которая представляет собой его модификацию с сдвигом на 13 позиций. ROT13 часто используется в Интернет-форумах и чатах для скрытия текста, который не является строго секретным, но не должен быть виден без дополнительного действия (например, при клике на ссылку). В современном мире шифр Цезаря уже не используется для серьёзных целей, но его концепции продолжают влиять на разработку более сложных алгоритмов шифрования [6].

2. Шифр A1Z26 представляет собой один из самых простых методов подстановки, в котором каждой букве латинского алфавита присваивается числовое значение, соответствующее её порядковому номеру. Например, букве A соответствует число 1, букве B — число 2, и так далее до Z, которое обозначается числом 26. Этот метод является разновидностью подстановочного шифра, так как для каждой буквы в тексте используется конкретное числовое значение, и преобразование текста заключается в замене букв на соответствующие им числа [7].

Этот метод шифрования достаточно примитивен и имеет ограничения, так как является линейным и не включает в себя никаких дополнительных элементов защиты. Однако он служит базовой моделью для понимания принципов шифрования и дешифрования, что делает его полезным для обучения основам криптографии [7].

Что касается криптографической стойкости, то шифр A1Z26 поддается дешифровке с высокой вероятностью, поскольку количе-

ство возможных подстановок ограничено [7]. Некоторые более сложные методы криптографии, такие как шифр Виженера, могут использовать идеи подстановки, но с дополнительным слоем сложности, который предотвращает дешифровку методом подбора [7].

«Пляшущие человечки» (англ. The Adventure of the Dancing Men) — один из 56 рассказов английского писателя Артура Конана Дойля о сыщике Шерлоке Холмсе и докторе Ватсоне, включённый писателем в сборник 13 рассказов «Возвращение Шерлока Холмса» [8]. Сам писатель включал этот рассказ в число 12 своих лучших произведений о Холмсе, поставив его на третье место. В рассказе великий сыщик Шерлок Холмс разоблачает загадку таинственного шифра, состоящего из изображений пляшущих человечков [8].

Разработанное в рамках данного исследования приложение позволяет осуществлять шифрование несколькими методами. При запуске веб-приложения пользователь попадает на страницу с шифром Цезаря. Сверху расположено удобное горизонтальное меню, благодаря которому можно перемещаться между различными шифрами. Для шифрования текста необходимо указать исходный текст, а также число, на которое нужно сдвигать символы в исходном тексте. Имеется возможность как шифровки, так и дешифровки текста. Для этого предусмотрены две соответствующие кнопки (рисунок 1).

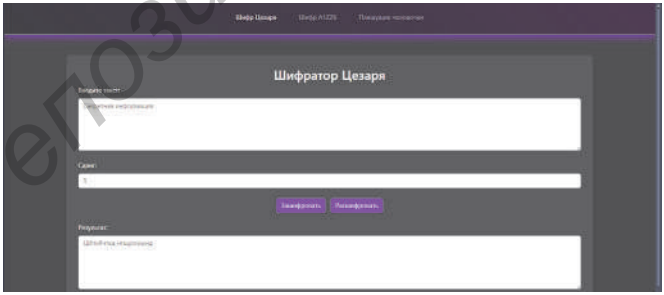

Рисунок 1 — Шифр Цезаря

Далее пользователь может перейти на страницу с шифром A1Z26, для этого необходимо выбрать соответствующий пункт

в верхнем горизонтальном меню. При переходе пользователь видит страницу, где может зашифровать информацию методом AZ126, для шифрования ему нужно ввести только текст и нажать кнопку «Зашифровать». Для расшифровки соответственно нужно в поле исходного текста ввести зашифрованный текст и нажать на кнопку «Расшифровать» (рисунок 2).

Далее опишем страницу «Пляшущие человечки». На ней пользователь точно так же может зашифровать информацию. Для этого ее необходимо ввести в соответствующее текстовое поле и нажать кнопку «Зашифровать». Результатом будут сменяющиеся друг за другом картинки человечка, образующие «танец». Так же на самой странице можно посмотреть саму последовательность этих картинок (рисунок 3).

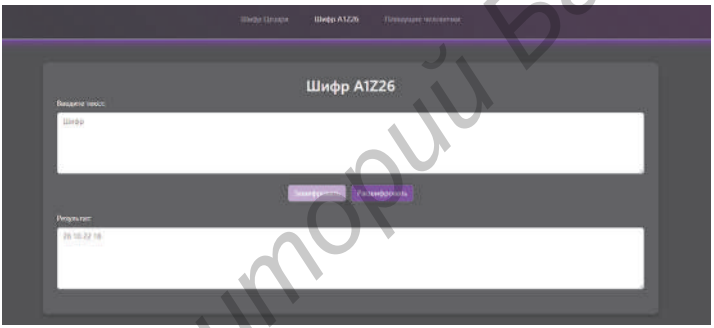

Рисунок 2 — Шифр A1Z26

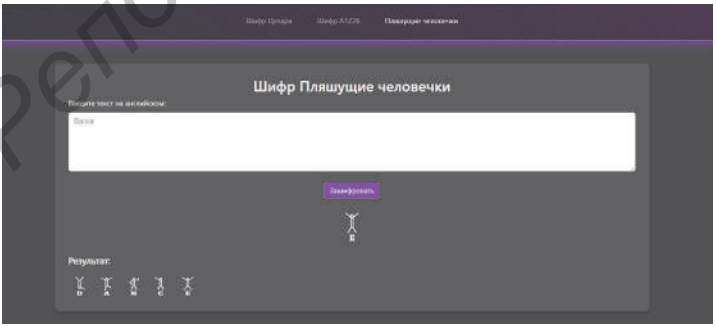

Рисунок 3 — Шифр пляшущих человечков

Заключение. В результате, благодаря удобному и понятному интерфейсу среды программирования Visual Studio Code с применением языка гипертекстовой разметки HTML и языка программирования Javascript удалось создать удобное веб-приложение для шифрования информации. Конечный продукт соответствует всем требованиям современного веб-приложения, имеет привлекательный и удобный пользовательский интерфейс, позволяет использовать три различных метода современной криптографии.

Список цитируемых источников

1. Криптосистема с открытым ключом : [сайт]. — 2024. — URL: https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом (дата обращения: 27.11.2024).
2. Криптография на основе эллиптических кривых (ECC) : [сайт]. — 2024. — URL: kriptografiya-na-osnove-ellipticheskih-krivyh-ecc.pdf (дата обращения: 27.11.2024).
3. Криптографический алгоритм с открытым ключом SM2 : [сайт]. — 2024. — URL: https://www.cnnic.com.cn/ScientificResearch/LeadingEdge/soea/SM2/201312/t20131204_43349.htm (дата обращения: 27.11.2024).
4. SM3 хэш-функция : [сайт]. — 2024. — URL: https://en.wikipedia.org/wiki/SM3_(hash_function) (дата обращения: 27.11.2024).
5. SM4 блочный шифр : [сайт]. — 2024. — URL: https://en.wikipedia.org/wiki/SM4_(cipher) (дата обращения: 27.11.2024).
6. Шифр Цезаря — Рувики : [сайт]. — 2024. — URL: https://ru.ruwiki.ru/wiki/Шифр_Цезаря (дата обращения: 27.11.2024).
7. Шифр A1Z26 : [сайт]. — 2024. — URL: https://poformule.ru/text/shifr-a1z26#:~:text=Шифр%20A1Z26%20 (дата обращения: 27.11.2024).
8. Шифр Пляшущие человечки — Рувики : [сайт]. — 2024. — URL: https://ru.ruwiki.ru/wiki/Пляшущие_человечки (дата обращения: 27.11.2024).