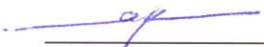


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект інтерактивного мобільного
застосунку для вивчення криптографічних алгоритмів»

Виконала: студентка 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Анастасія ПРУТ

Керівник: старший викладач кафедри КІ та КБ

 Наталія ЩУР

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олександр ПІРОГ

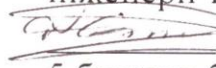
Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Прут Анастасія Олександрівна

Тема роботи: «Проект інтерактивного мобільного застосунку для вивчення
криптографічних алгоритмів»

затверджена Наказом університету від 5 березня 2024 р. № 97/с

Термін здачі студентом закінченої роботи 29 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес навчання криптографічних алгоритмів за допомогою інтерактивних мобільних додатків.

Предметом дослідження є методи та технології створення інтерактивних мобільних додатків для навчання криптоалгоритмів, зокрема використання онлайн-конструктора Wix для створення інтерактивних навчальних модулів, візуалізацій алгоритмів та інтерактивних вправ.

Обладнання та програмне забезпечення:

1. Конструктор сайтів Wix
2. Платформа WordPress
3. Конструктор Squarespace

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олександра ПОКОТИЛО	05.03.2024 	06.03.2024 
2	Олександра ПОКОТИЛО	26.04.2024 	26.04.2024 
3	Олександра ПОКОТИЛО	13.05.2024 	13.05.2024 

Студент  Анастасія ПРУТ

Керівник  Наталія ЩУР

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	7 березня	виконано
2	Аналіз літератури та збір інформації	27 березня	виконано
3	Розробка концепції застосунку	18 квітня	виконано
4	Вибір обладнання та технологій	30 квітня	виконано
5	Розробка дизайну інтерфейсу	15 травня	виконано
6	Реалізація функціоналу	22 травня	виконано
7	Тестування та відлагодження	28 травня	виконано
8	Оформлення кваліфікаційної роботи	23 червня	виконано
9	Підготовка перзентації до захисту	25 червня	

Студент  Анастасія ПРУТ

Керівник  Наталія ЩУР

АНОТАЦІЯ

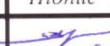
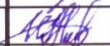
Пояснювальна записка до випускної кваліфікаційної роботи бакалавра на тему «Проект інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів» складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 50 сторінках друкованого тексту. Загальний обсяг роботи – 60 сторінок. Пояснювальна записка містить 42 рисунки та 2 таблиці. Список використаних літературних джерел налічує 21 найменування.

Метою випускної роботи є розробка інтерактивного мобільного застосунку тренажеру для вивчення криптографічних алгоритмів, який надасть користувачам можливість ознайомитись з основними методами та концепціями криптографії через інтерактивні навчальні модулі.

У процесі роботи було проаналізовано існуючі методи навчання криптографії та обрано оптимальні шляхи їх інтеграції в інтерактивному тренажері. Застосунок містить теоретичні матеріали, візуалізації алгоритмів та інтерактивні вправи, що допомагають користувачам краще зрозуміти та засвоїти складні концепції.

Кваліфікаційна робота демонструє можливість ефективного використання онлайн-конструкторів для створення освітніх застосунків в освітніх цілях.

Ключові слова: КРИПТОГРАФІЯ, МОБІЛЬНИЙ ТРЕНАЖЕР, ВІЗУАЛІЗАЦІЯ АЛГОРИТМІВ, ШИФРУВАННЯ

					ККІК.КР.Б – 123 – 24 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів	Літ.	Арк.	Аркушів
Розроб.		Прут А.О.		28.06.24				
Керівник		Щур Н.О.		28.06.24			4	60
Реценз.		Пірог О.В.		28.06.24				
Н. контр.		Щур Н.О.		28.06.24				
Затверд.		Єфіменко А.А.		28.06.24			ФІКТ, Гр. КІ-20-1	

ANNOTATION

The explanatory note for the bachelor's graduation qualification work on the topic «Project of an Interactive Mobile Application for Learning Cryptographic Algorithms» consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual part is presented on 50 pages of printed text. The total volume of the work is 60 pages. The explanatory note includes 42 figures and 2 tables. The list of used literary sources includes 21 titles.

The purpose of this graduation work is to develop an interactive mobile application trainer for learning cryptographic algorithms, which will provide users with the opportunity to familiarize themselves with the basic methods and concepts of cryptography through interactive learning modules.

During the course of the work, existing methods of teaching cryptography were analyzed and optimal ways of integrating them into the interactive trainer were selected. The application contains theoretical materials, algorithm visualizations, and interactive exercises that help users better understand and master complex concepts.

The qualification work demonstrates the possibility of effectively using online constructors for creating educational applications for educational purposes.

Keywords: CRYPTOGRAPHY, MOBILE TRAINER, ALGORITHM VISUALIZATION, ENCRYPTION

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ У СФЕРІ НАВЧАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ.....	10
1.1. Аналіз сучасного стану проблеми та обґрунтування актуальності теми роботи.....	10
1.2. Порівняння існуючих аналогів програмного продукту	13
1.3. Архітектура та укрупнена структура майбутнього тренажеру	14
1.4. Інструментальні засоби реалізації програмного продукту та вимоги до апаратних засобів.....	16
Висновок до першого розділу	19
РОЗДІЛ 2. РОЗРОБКА ТА РЕАЛІЗАЦІЯ МОБІЛЬНОГО ЗАСТОСУНКУ	20
2.1. Варіанти використання мобільного застосунку	20
2.2. Структура модулів та класів програми	22
2.3. Опис реалізації функціоналу мобільного застосунку	24
2.4. Опис компонентної будови мобільного застосунку	32
Висновок до другого розділу	38
РОЗДІЛ 3. ОПИС ІНТЕРФЕЙСУ, ПОРЯДОК РОБОТИ ТА НАЛАШТУВАННЯ ЗАСТОСУНКУ, ТЕСТУВАННЯ РЕАЛІЗОВАНИХ АЛГОРИТМІВ.....	40
3.1. Структура та основні елементи інтерфейсу застосунку	40
3.2. Порядок роботи із мобільним застосунком та тестовий приклад	50
Висновки до третього розділу	51
ВИСНОВКИ	53
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	54
ДОДАТКИ	56

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

UI – (user interface), інтерфейс користувача

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі захист інформації стає все більш важливим аспектом діяльності як окремих осіб та організацій. Кількість кібератак зростає з кожним роком, що підкреслює потребу в глибоких знаннях методів шифрування для захисту даних.

Розробка інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів надзвичайно важлива з кількох причин. Зростання важливості інформаційної безпеки перед обличчям постійно зростаючої кількості кібератак підкреслює необхідність глибокого розуміння способів захисту зашифрованих даних. Мобільні технології стали невід’ємною частиною нашого повсякденного життя, і їх використання в навчанні зростає завдяки їх доступності та зручності. Традиційні методи навчання часто не дають достатнього рівня практичних знань, тоді як інтерактивні навчальні модулі дозволяють значно покращити навчальний процес завдяки активній взаємодії з матеріалом.

Ця робота може вирішити багато важливих завдань. По-перше, не вистачає інтерактивних навчальних матеріалів з криптографії. Багато існуючих ресурсів не забезпечують належного рівня взаємодії та практичного керівництва, що призводить до труднощів у вивченні матеріалу. По-друге, складність розуміння теоретичних криптографічних концепцій можна зменшити за допомогою інтерактивних візуалізацій алгоритмів і вправ. По-третє, проблему обмеженого доступу до якісних освітніх ресурсів можна вирішити за допомогою мобільного застосунку на платформі Wix, який надасть широкій аудиторії доступ до зашифрованих навчальних матеріалів.

Тому розробка інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів є важливою та своєчасною ініціативою, яка сприятиме підвищенню рівня освіти у сфері інформаційної безпеки та забезпеченню доступності знань для широкого кола користувачів.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Метою кваліфікаційної роботи є розробка інтерактивного мобільного тренажера для вивчення криптографічних алгоритмів, який надасть користувачам можливість вивчати основні методи та концепції криптографії за допомогою інтерактивних навчальних модулів.

Визначена мета обумовлює наступні завдання:

- Аналіз літератури та існуючих рішень;
- Визначення вимог до застосунку;
- Проєктування застосунку;
- Розробка застосунку;
- Тестування та оптимізація.

Об’єктом дослідження є процес навчання криптографічних алгоритмів за допомогою інтерактивних мобільних додатків.

Предметом дослідження є методи та технології створення інтерактивних мобільних додатків для навчання криптоалгоритмів, зокрема використання онлайн-конструктора Wix для створення інтерактивних навчальних модулів, візуалізацій алгоритмів та інтерактивних вправ.

У процесі виконання кваліфікаційної роботи було розроблено проєкт інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів, який містить теоретичні матеріали, візуалізації алгоритмів та інтерактивні вправи, які полегшують розуміння та вивчення складних понять у галузі криптографії.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ У СФЕРІ НАВЧАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

1.1. Аналіз сучасного стану проблеми та обґрунтування актуальності теми роботи

В умовах стрімкого розвитку інформаційних технологій та збільшення кількості кіберзагроз забезпечення інформаційної безпеки стає дуже актуальним завданням. Шифрування є одним з основних методів захисту інформації, що забезпечує конфіденційність, цілісність і достовірність даних. Однак для ефективного використання криптографічних алгоритмів необхідні глибокі знання та розуміння їх принципів і механізмів.

Зростаюча кількість кібератак і зростаючі вимоги до безпеки ІТ-систем зумовлюють потребу у високоякісному навчанні фахівців з криптографії. За даними аналітичних компаній, кількість кібератак щорічно зростає на 20-30%, що свідчить про постійну еволюцію загроз у кіберпросторі. У цьому сенсі компанії та організації активно інвестують у розробку та впровадження нових методів захисту даних, а також у підвищення кваліфікації своїх співробітників. Традиційні методи навчання, засновані на лекціях і підручниках, часто не забезпечують достатнього рівня практичних знань і навичок. Вони можуть бути ефективними для передачі теоретичних знань, але не завжди сприяють розвитку практичних навичок, необхідних для роботи з реальними криптосистемами. Крім того, студенти та спеціалісти часто стикаються з відсутністю інтерактивних та практичних навчальних матеріалів, що ускладнює процес навчання та знижує мотивацію. У цьому сенсі інтерактивні мобільні додатки, які поєднують теоретичні знання з практичними вправами, стають все більш популярними.

Інтерактивні мобільні додатки, які поєднують теоретичні знання з практичними вправами, стають все більш важливими і все більш затребуваними. Згідно з дослідженнями, використання мобільних технологій в освіті дозволяє значно підвищити ефективність навчальних матеріалів завдяки можливості інтерактивної взаємодії та миттєвого зворотного зв'язку.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Мобільні додатки мають ряд переваг (Рис. 1.1):

- **Доступність:** Можливість навчання в будь-який час і в будь-якому місці.
- **Інтерактивність:** використання анімації, візуальних елементів та інтерактивних завдань для покращення розуміння матеріалу.
- **Персоналізація:** Адаптація навчального процесу до потреб і рівня підготовки кожного користувача.
- **Мотивація:** застосування навчального процесу сприяє підвищенню мотивації та зацікавленості користувачів.



Рисунок 1.1 - Переваги мобільних додатків

Враховуючи вищезазначене, інтерактивні мобільні тренажери для вивчення криптографії можуть стати ефективним інструментом підвищення кваліфікації професіоналів у цій сфері. Це дозволяє не лише отримати теоретичні знання, а й закріпити їх практично за допомогою вправ та інтерактивних завдань.

Основними перевагами інтерактивних мобільних додатків у навчанні криптографії є (Рис. 1.2):

- **Візуалізація алгоритмів:** програми дозволяють візуалізувати процеси шифрування та дешифрування, допомагаючи користувачам краще зрозуміти, як працюють алгоритми.
- **Практичні завдання:** Інтерактивні вправи та завдання дозволяють користувачам закріпити отримані знання та розвинути практичні навички.

- Зворотний зв'язок: миттєвий зворотний зв'язок дозволяє користувачам відразу бачити результати своїх дій і виправляти помилки.
- Гнучкість навчання: здатність вчитися в потрібний час і в потрібному місці підвищує ефективність засвоєння матеріалу.

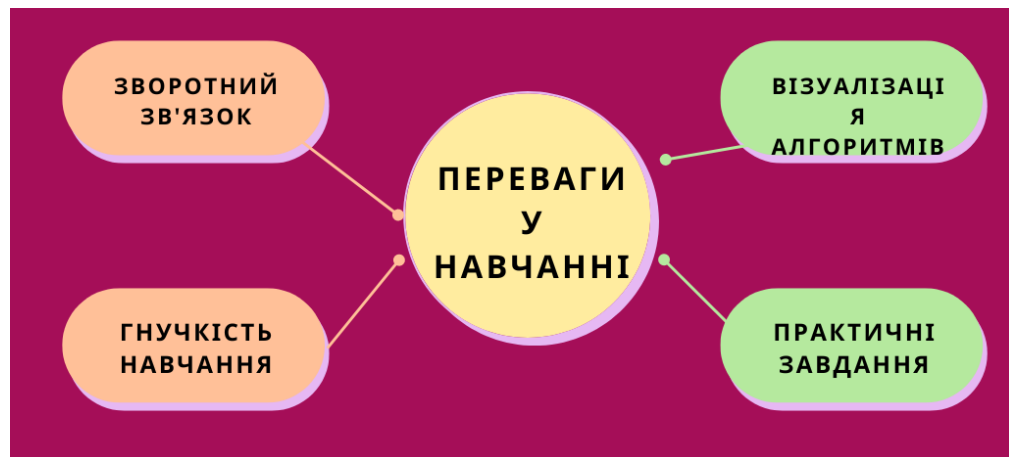


Рисунок 1.2 - Переваги інтерактивних мобільних додатків у навчанні кодуванню

Мета роботи – створити інтерактивний мобільний застосунок, який допоможе користувачам вивчати криптографічні алгоритми за допомогою інтерактивних навчальних модулів. Такий підхід сприятиме глибшому розумінню складних криптографічних концепцій та підвищенню рівня кваліфікації спеціалістів у цій галузі.

Тому тема цієї кваліфікаційної роботи виникає у зв'язку зі зростанням кількості кіберзагроз та необхідністю підвищення кваліфікації спеціалістів із криптографії. Інтерактивні мобільні додатки, які поєднують теоретичні знання з практичними вправами, є ефективним інструментом для навчання криптографії та сприяють кращому розумінню та засвоєнню складних концепцій. Розробка такого застосунку забезпечить доступність, інтерактивність та ефективність навчального процесу, що підвищить рівень знань та навичок у сфері криптографічного захисту даних.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2. Порівняння існуючих аналогів програмного продукту

У цьому розділі виконано детальний аналіз та порівняння існуючих програмних аналогів, спрямованих на навчання криптографічних алгоритмів за допомогою інтерактивних мобільних додатків. Результати аналізу (Табл. 1.1) дозволили зрозуміти сильні та слабкі сторони кожного з виявлених аналогів, що важливо для подальшого вдосконалення та розвитку нового продукту.

Проаналізуємо функціональність інших програм:

- CryptoAR – ця програма надає базову інформацію про криптографію та основні алгоритми шифрування. Він містить інтерактивні завдання, які перевіряють знання користувачів, але охоплення більш складних криптографічних концепцій, таких як асиметричне шифрування та електронні цифрові підписи, обмежене.
- CryptoLearn – ця програма спрямована на глибше розуміння алгоритмів шифрування та підпису за допомогою візуальних та інтерактивних елементів. Однак його інтерфейс може стати проблемою для тих, хто новачок у світі криптовалют.
- KryptoBuddy – ця програма пропонує широкий спектр вправ і тестів для вивчення криптографічних алгоритмів, але має обмежені можливості для інтерактивного навчання та візуалізації складних алгоритмів.

У результаті аналізу було встановлено, що жоден із протестованих аналогів повністю не відповідає потребам глибокого інтерактивного навчання криптографії через мобільні додатки. Більшість існуючих програм мають обмежені можливості для підтримки складних алгоритмів і не забезпечують достатньої інтерактивності для ефективного навчання.

Розробка нового інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів має на меті заповнити ці прогалини. Нова програма включатиме широкий спектр візуалізацій, вправ та інтерактивних тестів для забезпечення ефективного навчання користувачів.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Порівняння існуючих аналогів програмного продукту

ПОРІВНЯННЯ ІСНУЮЧИХ АНАЛОГІВ					
НАЗВА	ОПИС	ПЕРЕВАГИ	НЕДОЛІКИ	ЦІНА	ПЛАТФОРМА
CRYPTOMANIAC	ІНТЕРАКТИВНИЙ ДОДАТОК ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЇ З ВІКТОРИНАМИ, ІГРАМИ ТА СИМУЛЯТОРАМИ.	- ВЕЛИКА БАЗА ДАНИХ АЛГОРИТМІВ - ПРОСТИЙ ТА ЗРОЗУМЛИЙ ІНТЕРФЕЙС - ЦІКАВИЙ ТА ЗАХОПЛЮЮЧИЙ КОНТЕНТ	- НЕМАЄ РОЗДІЛУ ПРО ПРАКТИЧНЕ ЗАСТОСУВАННЯ	БЕЗКОШТОВНО З ВНУТРІШНІМИ ПОКУПКАМИ	IOS, ANDROID
KHAN ACADEMY CRYPTOGRAPHY	БЕЗКОШТОВНИЙ ОНЛАЙН-КУРС З КРИПТОГРАФІЇ, ЯКИЙ ВКЛЮЧАЄ ВІДЕО, СТАТТІ ТА ІНТЕРАКТИВНІ ВПРАВИ.	- БЕЗКОШТОВНИЙ ТА ДОСТУПНИЙ - ДЕТАЛЬНИЙ ТА ҐРУНТОВНИЙ КОНТЕНТ - ПІДХОДИТЬ ДЛЯ ПОЧАТКІВЦІВ ТА ДОСВІДЕНИХ КОРИСТУВАЧІВ	- НЕМАЄ МОБІЛЬНОГО ДОДАТКУ - НЕМАЄ ІГРОВИХ ЕЛЕМЕНТІВ	БЕЗКОШТОВНО	ВЕБ
CYPHER	МОБІЛЬНИЙ ДОДАТОК, ЯКИЙ ДОЗВОЛЯЄ ШИФРУВАТИ ТА ДЕШИФРУВАТИ ТЕКСТ ЗА ДОПОМОГОЮ РІЗНИХ АЛГОРИТМІВ.	- ПРОСТИЙ У ВИКОРИСТАННІ - ПІДТРИМУЄ ДЕКІЛЬКА АЛГОРИТМІВ - ДОЗВОЛЯЄ ДІЛИТИСЯ ЗАШИФРОВАНИМИ ПОВІДОМЛЕННЯМИ	- НЕМАЄ РОЗДІЛУ ПРО ТЕОРІЮ КРИПТОГРАФІЇ - НЕМАЄ ІГРОВИХ ЕЛЕМЕНТІВ	БЕЗКОШТОВНО	IOS, ANDROID
CRYPTOCURRENCY TRADING ACADEMY	ОНЛАЙН-КУРС З ТОРГІВЛІ КРИПТОВАЛЮТАМИ, ЯКИЙ ВКЛЮЧАЄ РОЗДІЛ ПРО КРИПТОГРАФІЧНІ АЛГОРИТМИ.	- ДЕТАЛЬНИЙ ОПИС КРИПТОГРАФІЧНИХ АЛГОРИТМІВ, ЩО ВИКОРИСТОВУЮТЬСЯ В КРИПТОВАЛЮТАХ	- НЕ ЗОСЕРЕДЖЕНИЙ НА ВИВЧЕННІ КРИПТОГРАФІЇ ЯК НАУКИ - ДОРОГИЙ КУРС	300 USD	ВЕБ
COURSERA CRYPTOGRAPHY COURSE	ОНЛАЙН-КУРС З КРИПТОГРАФІЇ ВІД СТЕЙНФОРДСЬКОГО УНІВЕРСИТЕТУ.	- ВИСОКИЙ РІВЕНЬ НАВЧАННЯ - ВИКЛАДАЮТЬ ЕКСПЕРТИ З КРИПТОГРАФІЇ	- ДОРОГИЙ КУРС - НЕМАЄ ІГРОВИХ ЕЛЕМЕНТІВ	400 USD	ВЕБ
НАШ ПРОЕКТ	ІНТЕРАКТИВНИЙ МОБІЛЬНИЙ ЗАСТОСУНОК-ТРЕНАЖЕРУ ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ	- ГЛИБОКЕ ІНТЕРАКТИВНЕ НАВЧАННЯ, - ПОКРИТТЯ СКЛАДНИХ АЛГОРИТМІВ	НЕОБХІДНІСТЬ В РОЗРОБЦІ ТА ВПРОВАДЖЕННІ	БЕЗКОШТОВНО	ВЕБ

1.3. Архітектура та укрупнена структура майбутнього тренажеру

У цьому підрозділі обговорюється архітектурний підхід і загальна структура майбутнього симулятора, призначеного для навчання криптографічним алгоритмам через інтерактивну мобільну програму. Описує основні компоненти системи, їх функції та взаємодію між ними для забезпечення ефективного навчання користувачів.

Розроблюваний мобільний застосунок матиме модульну архітектуру (Рис. 1.3), що дозволить легко додавати нові функціональні можливості та оновлювати існуючі компоненти. Основні модулі застосунку включатимуть:

- Теоретичний модуль: міститиме навчальний матеріал з основ криптографії, включаючи опис загальних алгоритмів та їх застосування.

- Модуль візуалізації: забезпечує візуалізацію роботи алгоритмів шифрування, дозволяючи користувачам контролювати процес шифрування та дешифрування даних.
- Інтерактивний модуль: міститиме рішення та практичні завдання, які допоможуть користувачам покращити свої знання та навички.

Теоретичний модуль ляже в основу навчальної частини програми, надаючи користувачам доступ до основних концепцій шифрування. Він міститиме детальний матеріал про основи шифрування, включаючи опис основних алгоритмів шифрування та його застосування в різних сферах інформаційної безпеки. Користувачі зможуть вивчати теоретичний матеріал у вигляді текстових описів, схем та інших візуальних форм, які полегшують розуміння складних концепцій шифрування.

Модуль візуалізації дозволить інтерактивно проілюструвати роботу криптографічних алгоритмів. Це дозволить користувачам бачити процеси шифрування та дешифрування даних у реальному часі. Цей модуль включатиме візуалізації, які пояснюють кожен крок алгоритму, покращуючи розуміння користувачами закулісних процесів захисту криптографічної інформації.

Інтерактивний модуль спрямований на закріплення знань і навичок, отриманих під час виконання вправ і практичних завдань. Це надасть користувачам можливість самостійно застосовувати теоретичні знання в різних сценаріях. Цей модуль включатиме інтерактивні завдання з шифрування та дешифрування даних, аналіз криптографічних атак та перевірку знань з криптографічних тем.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

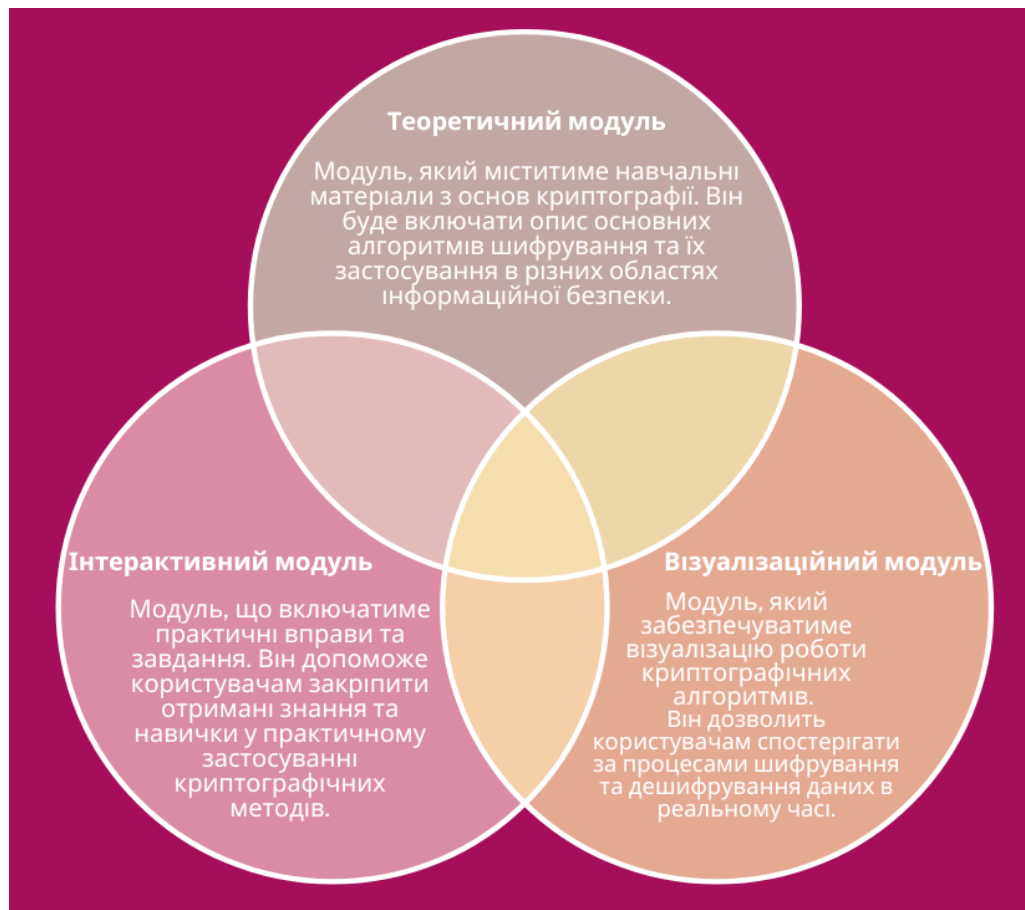


Рисунок 1.3 - Модульна архітектура застосунку

Кожен з цих модулів буде інтегрований в єдину платформу, що забезпечить зручний доступ до навчального матеріалу та практичних завдань через мобільний застосунок, що підтримується на різних платформах.

Ця архітектура дозволить ефективно впроваджувати і підтримувати нові можливості застосунку, забезпечуючи високий рівень користувацького досвіду та якість навчання з криптографії через мобільний застосунок.

1.4. Інструментальні засоби реалізації програмного продукту та вимоги до апаратних засобів

При виборі інструменту для створення мобільного застосунку було проведено порівняльний аналіз кількох конструкторів сайтів (Табл. 1.2):

- WordPress: Відомий своєю гнучкістю і широким спектром плагінів, але вимагає додаткових знань для налаштування і підтримки.
- SquareSpace: Має візуально привабливі шаблони, але обмежений в можливостях налаштування і розширення функціоналу.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Weebly: Простий у використанні, але має менше можливостей для розширення функціоналу порівняно з Wix.

Таблиця 1.2

Порівняльна таблиця конструкторів сайтів

ПОРІВНЯННЯ КОНСТРУКТОРІВ				
	WORDPRESS	SQUARESPACE	WEEBLY	WIX
ЦІНА	БЕЗКОШТОВНО (З ПЛАТНИМИ ПЛАНАМИ)	ПЛАТНІ ПЛАНИ	ПЛАТНІ ПЛАНИ	БЕЗКОШТОВНО (З ПЛАТНИМИ ПЛАНАМИ)
ПРОСТОТА ВИКОРИСТАННЯ	СЕРЕДНІЙ	ВИСОКИЙ	ВИСОКИЙ	ВИСОКИЙ
ГНУЧКІСТЬ	ВИСОКИЙ	СЕРЕДНІЙ	СЕРЕДНІЙ	ВИСОКИЙ
ДИЗАЙН	ШИРОКИЙ СПЕКТР ТЕМ	СТИЛЬНІ ТА СУЧАСНІ ШАБЛОНИ	ПРОСТІ ТА ЕЛЕГАНТНІ ШАБЛОНИ	СТИЛЬНІ ТА СУЧАСНІ ШАБЛОНИ
ФУНКЦІОНАЛЬНІСТЬ	ШИРОКИЙ СПЕКТР ПЛАГІНІВ ТА РОЗШИРЕНЬ	ОБМЕЖЕНА, АЛЕ ПОТУЖНА	ОБМЕЖЕНА	ШИРОКИЙ СПЕКТР ВБУДОВАНИХ ФУНКЦІЙ
ПІДТРИМКА КЛІЄНТІВ	АКТИВНА СПІЛЬНОТА ТА ФОРУМ	ВІДМІННА	ХОРОША	ВІДМІННА

Для розробки мобільного застосунку «Проект інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів» був обраний онлайн-конструктор Wix (Рис. 1.4), який надає широкі можливості для створення та редагування веб-сайтів і веб-застосунків без потреби в програмуванні.

Інструменти Wix, які можуть бути використані в процесі розробки:

- Wix Editor: Інтуїтивно зрозумілий інтерфейс для розміщення і редагування контенту, включаючи текст, зображення, відео та інші елементи.
- Wix Code (Corvid): Платформа для створення динамічних веб-сайтів і додатків з використанням JavaScript. Це дозволяє додавати власний код для реалізації спеціалізованих функцій та взаємодії з базою даних.
- Wix App Market: Магазин додатків Wix, де можна знайти різноманітні розширення і плагіни для покращення функціональності застосунку без програмування.

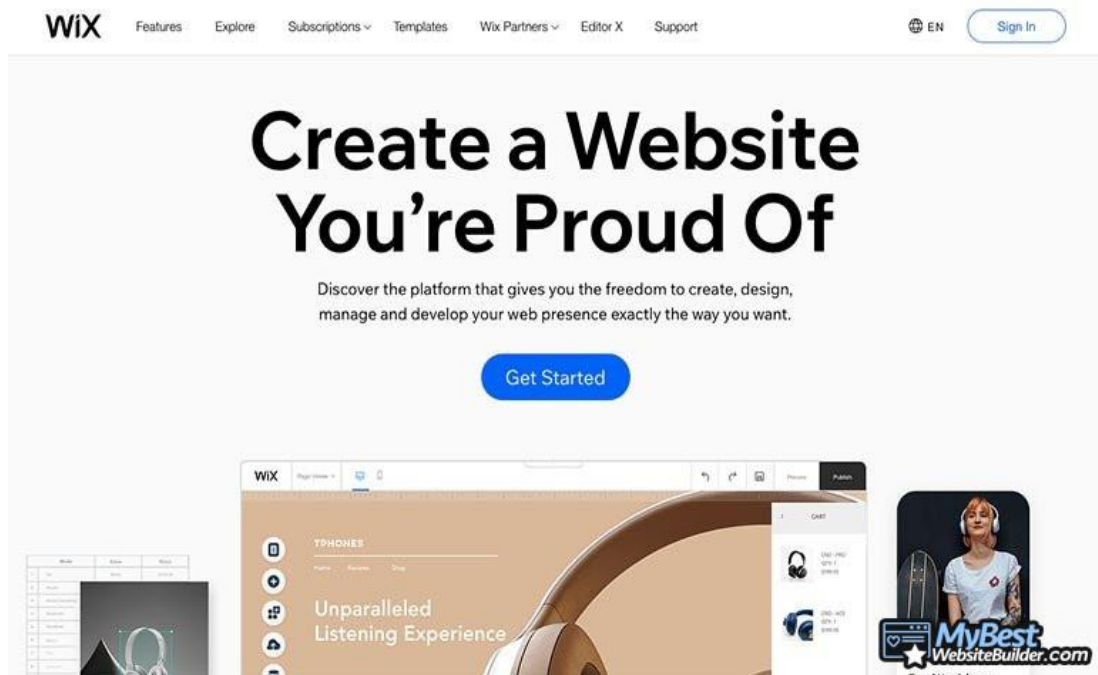


Рисунок 1.4 - Середовище конструктора сайтів WIX

Розглянемо детальніше основні переваги Wix (Рис. 1.5):



Рисунок 1.5 - Переваги Wix

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок до першого розділу

Виконання першого розділу кваліфікаційної роботи «Проект інтерактивного мобільного застосунку для вивчення криптографічних алгоритмів» відображає основні аспекти дослідження в процесі аналізу та планування розробки програмного комплексу.

У цьому розділі розглядається поточний стан і важливість теми, а також наголошується на необхідності створення інтерактивного інструменту для навчання програмуванню з урахуванням сучасних тенденцій в освіті та технологіях. Аналіз існуючих порівнянь підсистем кібербезпеки показав необхідність удосконалення та інтеграції інноваційних підходів у навчальні процеси.

Визначено концептуальну структуру майбутнього програмного комплексу, що складається з теоретичних, наочних та інтерактивних модулів, як основоположну для реалізації навчальних цілей і завдань. Вибір Wix Builder для розробки інструменту був виправданий його потужною функціональністю, простим у використанні інтерфейсом і розширюваністю за допомогою Wix Code.

Потім у першій частині було висвітлено необхідність, доцільність та принципи системного впровадження проєкту, метою якого є створення високоефективного інтерактивного інструменту для вивчення криптографії, який відповідає сучасним освітнім та безпековим вимогам інформації.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. РОЗРОБКА ТА РЕАЛІЗАЦІЯ МОБІЛЬНОГО ЗАСТОСУНКУ

2.1. Варіанти використання мобільного застосунку

У цьому розділі розглядаються різні сценарії використання інтерактивної мобільної програми для вивчення криптографічних алгоритмів (Рис. 2.1). Основна мета – показати, чим застосунок може бути корисним для різних категорій користувачів і які функції він пропонує.

2.1.1. Навчальні заклади та студенти.

Мобільні додатки можна інтегрувати в навчальний процес у школах, коледжах та університетах для вивчення програмування. Основними можливостями використання програми в навчальних закладах є:

1) Самоосвіта:

Теоретичні матеріали: завдяки застосунку студенти можуть вивчити основи криптографії, історію та принципи роботи різноманітних алгоритмів.

2) Практичні заняття:

Інтерактивні вправи: виконання завдань, які сприяють закріпленню теоретичних знань на практиці.

Візуалізація та симуляція алгоритмів: можливість використовувати алгоритми шифрування в реальному часі та контролювати процес шифрування та дешифрування.

Виконання завдань: студенти можуть виконувати вправи через застосунок, використовуючи моделювання та вбудовані інструменти.

Автоматична перевірка результатів: програма може автоматично перевіряти виконані завдання та надавати відгуки.

Тому мобільний застосунок є універсальним інструментом для вивчення криптографії, що забезпечує комплексний підхід до вивчення теорії та практики. Використання додатків у навчальних закладах покращує якість навчання та робить процес більш інтерактивним та цікавим для учнів чи студентів.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

2.1.2. Курси та тренінги

Для професійного розвитку та підвищення кваліфікації працівників у сфері кібербезпеки та ІТ застосунок може бути використаний у проведенні тренінгів та курсів з основ криптографії з метою ознайомлення працівників чи бажаючих з основними та найцікавішими алгоритмами криптографії, організації семінарів з використанням інтерактивних завдань та різноманітних кейсів.

2.1.3. Самоосвіта для ентузіастів

Для людей, які цікавляться криптографією та кібербезпекою та не мають офіційної освіти в цій галузі, програма пропонує:

- 1) Доступ до навчальних матеріалів: ознайомлення з основними поняттями та алгоритмами криптографії у зручному форматі.
- 2) Інтерактивні практичні завдання та отримання негативного відгуку.
- 3) Симуляції: виконання симуляції реальних сценаріїв криптододатків.



Рисунок 2.1 - Сценарії використання інтерактивної мобільної програми для вивчення криптографічних алгоритмів

Різноманітність можливостей використання системи підкреслює її універсальність і корисність для широкого кола користувачів. Інтерактивний мобільний застосунок стане цінним інструментом як для навчальних закладів і професійних курсів, так і для окремих ентузіастів і компаній.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2. Структура модулів та класів програми

Розглянемо архітектуру створеного мобільного застосунку для навчання криптографії, а також його окремих підсистем. Мета полягає в тому, щоб описати загальну структуру системи і взаємодії користувача з системою.

Загальна структура системи.

Мобільний застосунок, що створюється, матиме модульну архітектуру, яка дозволить легко додавати нові функції та оновлювати існуючі компоненти. До основних елементів системи відносяться:

1. Інтерфейс користувача (UI). Інтерфейс користувача є одним із ключових елементів системи, оскільки саме через нього користувачі взаємодіють із додатком. Основне призначення інтерфейсу користувача – забезпечити зручний та інтуїтивно зрозумілий доступ до функцій і можливостей програми. Інтерфейс складається з кількох основних розділів (Рис. 2.2):



Рисунок 2.2 – Схема модульної архітектури застосунку

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

1) Головна сторінка:

- Привітання та вступна інформація. Домашня сторінка містить коротке привітання та опис основних функцій програми. Вступна інформація допомагає користувачам швидко зрозуміти, що пропонує застосунок і як ним користуватися.
- Навігаційне меню – меню, яке дозволяє користувачам легко переміщатися між різними розділами програми. Він має бути зручно розташований і містити посилання на всі основні модулі, такі як теоретичний модуль, модуль візуалізації, інтерактивний модуль та модуль тестування.

2) Теоретичний модуль:

- Навчальні матеріали: сторінки з текстовими та мультимедійними матеріалами, що пояснюють основні концепції криптографічних алгоритмів. Матеріали можуть включати статті, презентації, відео та інші форми вмісту.
- Навігація по розділах: зручна навігація, яка дозволяє користувачам швидко знаходити те, що їм потрібно.

3) Візуалізаційний модуль:

- Схеми, зображення та пояснення роботи шифрів, особливості їх застосування, демонстрація роботи криптографічних алгоритмів.

4) Інтерактивний модуль:

- Практичні завдання, що дають можливості зашифрувати власний обраний текст або фразу, побачити як працює шифрувальний алгоритм, налаштування ключів або кодових фраз.

5) Тестовий модуль:

- Набір вправ та завдань для закріплення отриманих знань. Завдання варіюються за рівнем складності та охоплюють різні аспекти криптографії.
- Автоматична перевірка: Система автоматично перевіряє результати виконаних завдань та надає користувачам зворотний зв'язок. Це допомагає швидко виявити та виправити помилки.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Тести для перевірки знань користувачів з різних тем криптографії. Тести можуть включати питання з вибором правильної відповіді, так і задачі з різними типами складності.
- Відсутність оцінки результатів. Користувач зможе спробувати свої сили в тестах та задачах, але процесу оцінювання не буде оскільки це тренажер який несе за собою пізнавальну та навчальну функцію.

Інтерфейс користувача має бути розроблений з урахуванням принципів юзабіліті, щоб забезпечити максимальну зручність та ефективність роботи із застосунком. Важливо, щоб інтерфейс був адаптивним, тобто забезпечував зручний доступ до всіх функцій як на великих екранах (наприклад, планшетах), так і на смартфонах.

2.3. Опис реалізації функціоналу мобільного застосунку

Створюючи мобільний застосунок для вивчення криптографічних алгоритмів, ми обрали шифри Цезаря, Плейфера, Віженера та шифр частого колу, оскільки кожен із цих алгоритмів дозволяє користувачам зрозуміти основи криптографії та принцип роботи методів шифрування. Кожен із цих алгоритмів має своє власне історичне значення, легкість впровадження та освітню цінність, що робить їх ідеальними для освітніх цілей. У цьому розділі ми пояснимо причини вибору кожного з цих алгоритмів та їх практичне застосування в мобільному застосунку.

Шифр Цезаря.

Шифр Цезаря є одним із найпростіших і найвідоміших методів шифрування, який використовується для вивчення криптографії. У ньому виконується переміщення кожної літери простого тексту на певну кількість позицій в алфавіті, що полегшує пояснення основних принципів шифрування (Рис. 2.3).

У застосунку шифр Цезаря використовується для ознайомлення користувачів із концепцією шифрування. Користувачі можуть вводити звичайний текст і ключ, спостерігаючи за процесом шифрування та дешифрування в реальному часі. Це дозволяє зрозуміти, як прості зміни можуть призвести до зашифрованих повідомлень.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

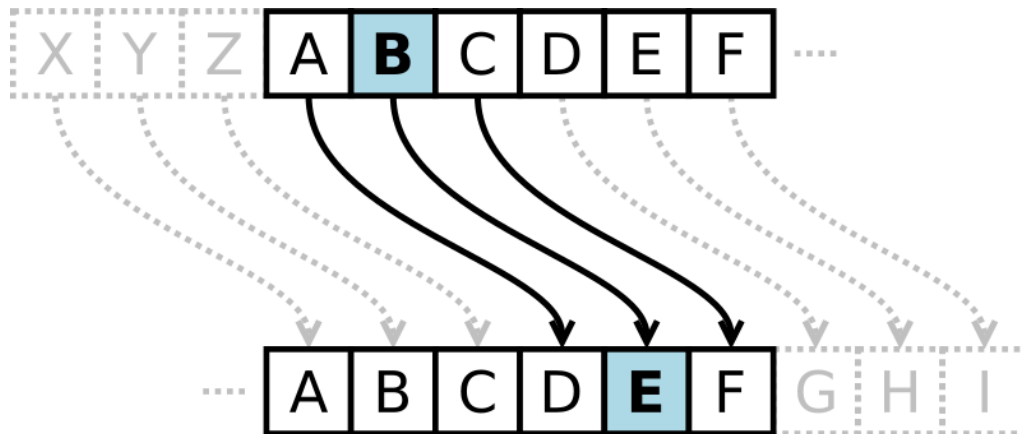


Рисунок 2.3 – Система шифрування Цезаря

Шифр Цезаря є одним з найпростіших та найвідоміших алгоритмів шифрування. Він полягає у зсуві кожної букви відкритого тексту на задану кількість позицій вниз по алфавіту. Наприклад, при ключі 3 буква А стає D, В стає Е і так далі.

Реалізація шифру Цезаря у застосунку:

```
$w.onReady(function () {

    // Функція для шифрування Цезаря
    function caesarCipher(str, shift) {
        const alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'.split("");
        return str.toUpperCase().split("").map(char => {
            const index = alphabet.indexOf(char);
            if (index === -1) return char;
            return alphabet[(index + shift) % 26];
        }).join("");
    }

    // Обробка натискання кнопки
    $w.onReady(function () {
        $w(«#button2»).onClick(() => {
            const message = $w(«#input1»).value;
            const key = parseInt($w(«#slider1»).value, 10);
            const encryptedMessage = caesarCipher(message, key);
            $w(«#text41»).text = encryptedMessage;
        });
    });
});
```

Шифр Плейфера.

Шифр Плейфера є складнішим, ніж шифр Цезаря, і використовує ключову матрицю (Рис. 2.4) для шифрування біграм (пар букв). Це ілюструє, як більш складні методи можуть забезпечити кращу безпеку.

У програмі користувачі можуть створити таблицю ключів на основі ключового слова, розділити текст на біграми та зашифрувати їх на основі позиції в таблиці. Інтерактивні вправи допомагають користувачам зрозуміти, як різні позиції букв у таблиці впливають на результат шифрування. [14]

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Рисунок 2.4 – Система шифрування Плейфера

Реалізація шифру Плейфера у застосунку:

```
//шифр плейфера
$w.onReady(function () {
  // Призначення обробника події для кнопки #button3
  $w(«#button4»).onClick(() => {
    // Отримання тексту з поля введення #input2
    let text = $w(«#input5»).value;
    // Отримання ключа з поля введення #input3
    let key = $w(«#input4»).value;

    // Перевірка, чи текст і ключ не пусті
    if (text && key) {
      // Виклик функції шифрування і отримання зашифрованого тексту
      let encryptedText = playfairEncrypt(text, key);

      // Виведення зашифрованого тексту в поле #text43
      $w(«#text44»).text = encryptedText;
    } else {
      // Виведення повідомлення про помилку
      $w(«#text44»).text = »Please enter both text and a valid key.«;
    }
  });
});
```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

```

// Функція для створення матриці ключів для шифру Плейфера
function generateKeyMatrix(key) {
    key = key.toUpperCase().replace(/[^A-Z]/g, "").replace(/J/g, 'I');
    let matrix = [];
    let seen = new Set();
    let alphabet = »ABCDEFGHIJKLMNOPQRSTUVWXYZ»; // 'J' is omitted

    for (let char of key) {
        if (!seen.has(char)) {
            matrix.push(char);
            seen.add(char);
        }
    }

    for (let char of alphabet) {
        if (!seen.has(char)) {
            matrix.push(char);
            seen.add(char);
        }
    }

    return Array.from({ length: 5 }, (_, i) => matrix.slice(i * 5, i * 5 + 5));
}

// Функція для шифрування тексту шифром Плейфера
function playfairEncrypt(plaintext, key) {
    let matrix = generateKeyMatrix(key);
    plaintext = plaintext.toUpperCase().replace(/[^A-Z]/g, "").replace(/J/g, 'I');

    // Розбиваємо текст на біграми
    let bigrams = [];
    for (let i = 0; i < plaintext.length; i += 2) {
        let a = plaintext[i];
        let b = (i + 1 < plaintext.length) ? plaintext[i + 1] : 'X';
        if (a === b) {
            b = 'X';
            i--;
        }
        bigrams.push([a, b]);
    }

    // Шифрування біграм
    let ciphertext = "";
    for (let [a, b] of bigrams) {
        let [rowA, colA] = findPosition(matrix, a);

```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

```

let [rowB, colB] = findPosition(matrix, b);

if (rowA === rowB) {
    ciphertext += matrix[rowA][(colA + 1) % 5] + matrix[rowB][(colB + 1) % 5];
} else if (colA === colB) {
    ciphertext += matrix[(rowA + 1) % 5][colA] + matrix[(rowB + 1) % 5][colB];
} else {
    ciphertext += matrix[rowA][colB] + matrix[rowB][colA];
}
}

return ciphertext;
}

// Функція для знаходження позиції символу в матриці
function findPosition(matrix, char) {
    for (let row = 0; row < 5; row++) {
        for (let col = 0; col < 5; col++) {
            if (matrix[row][col] === char) {
                return [row, col];
            }
        }
    }
    return [-1, -1]; // Символ не знайдено (що не повинно трапитись)
}

```

Шифр Віженера.

Шифр Віженера є прикладом багатоалфавітного шифру, який використовує ключове слово для шифрування кожної літери відкритого тексту (Рис. 2.5). Це забезпечує більш складне шифрування, оскільки кожна літера відкритого тексту може бути змінена по-різному залежно від відповідної літери ключового слова.

У програмі користувачі можуть вводити звичайний текст і ключове слово, спостерігаючи, як кожна літера тексту змінюється залежно від ключа. Інтерактивні вправи дозволяють експериментувати з різними ключами та повідомленнями, спостерігаючи за процесом шифрування та дешифрування. [14]

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок 2.5 – Система шифрування Віженера

Реалізація шифру Віженера у застосунку:

```

$w.onReady(function () {
    // Призначення обробника події для кнопки #button5
    $w(«#button5»).onClick(() => {
        // Отримання тексту з поля введення #input7
        let text = $w(«#input7»).value;
        // Отримання ключа з поля введення #input6
        let key = $w(«#input6»).value;

        // Перевірка, чи текст і ключ не пусті
        if (text && key) {
            // Виклик функції шифрування і отримання зашифрованого тексту
            let encryptedText = vigenereEncrypt(text, key);

            // Виведення зашифрованого тексту в поле #text46
            $w(«#text46»).text = encryptedText;
        } else {
            // Виведення повідомлення про помилку
            $w(«#text46»).text = »Please enter both text and a valid key.»;
        }
    });
});

```

```
// Функція для шифрування тексту шифром Віженера
function vigenereEncrypt(plaintext, key) {
    plaintext = plaintext.toUpperCase().replace(/[^A-Z]/g, "");
    key = key.toUpperCase().replace(/[^A-Z]/g, "");

    let ciphertext = "";
    for (let i = 0, j = 0; i < plaintext.length; i++) {
        let letter = plaintext[i];
        let keyLetter = key[j % key.length];
        let letterPos = letter.charCodeAt(0) - 65; // Позиція літери в алфавіті (A=0, B=1, ..., Z=25)
        let keyPos = keyLetter.charCodeAt(0) - 65; // Позиція літери ключа в алфавіті (A=0, B=1, ..., Z=25)
        let encryptedChar = String.fromCharCode((letterPos + keyPos) % 26 + 65); // Шифрування літери

        ciphertext += encryptedChar;
        j++;
    }
    return ciphertext;
}
```

Шифр частоколу.

Шифр частоколу використовує концепцію перестановки символів у повідомленні (Рис. 2.6). Це дозволяє нам продемонструвати інший підхід до шифрування, заснований не на заміні символів, а на їх перестановці.

У програмі можна ввести звичайний текст і ключ (кількість рядків або стовпців), спостерігаючи за тим, як текстові символи розташовані в сітці і як змінюється їх порядок після зміни порядку. Це допомагає зрозуміти, як шифри на основі перестановки можуть ефективно приховувати вміст повідомлення.

Original Message: Hello World

H				o				r				
	e		l					o		l		
		l					W					d

Encrypted Message: Horel ollWd

Рисунок 2.6 – Система шифрування частоколу

Шифр частоколу є представником шифрів перестановки. Ключем є ціле число K – висота частоколу. При шифруванні літери повідомлення записуються як степені (їх кількість висота частоколу), а потім отримані літери в степенях переписуються по рядках зверху донизу. [15]

Реалізація шифру частоколу у застосунку:

```
$w.onReady(function () {
  // Призначення обробника події для кнопки #button3
  $w(«#button3»).onClick(() => {
    // Отримання тексту з поля введення #input2
    let text = $w(«#input2»).value;
    // Отримання ключа з поля введення #input3
    let key = parseInt($w(«#input3»).value);

    // Перевірка, чи текст і ключ не пусті
    if (text && key) {
      // Виклик функції шифрування і отримання зашифрованого тексту
      let encryptedText = railFenceEncrypt(text, key);

      // Виведення зашифрованого тексту в поле #text43
      $w(«#text43»).text = encryptedText;
    } else {
      // Виведення повідомлення про помилку
      $w(«#text43»).text = »Please enter both text and a valid key.«;
    }
  });
});

// Функція для шифрування тексту шифром частоколу
function railFenceEncrypt(text, key) {
  if (key <= 1) return text; // Якщо ключ <= 1, повертаємо текст без змін

  let fence = Array.from({ length: key }, () => []);
  let rail = 0;
  let direction = 1;

  for (let char of text) {
    fence[rail].push(char);
    rail += direction;

    if (rail === 0 || rail === key - 1) {
      if (key % 2 === 0) {
        direction *= -1;
      }
    }
  }
}
```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

```

    } else {
        direction = direction === 1 ? -1 : 1;
    }
}

let encryptedText = "";
for (let i = 0; i < key; i++) {
    encryptedText += fence[i].join("");
}
return encryptedText;
}

```

Вибір даних чотирьох алгоритмів базувався на їхній здатності пояснювати різні аспекти криптографії, від простих методів підстановки до більш складних методів перестановки та шифрування. Інтерактивні завдання та модулі програми дозволяють користувачам не лише вивчити теоретичні основи криптографії, а й побачити ці принципи в дії, експериментуючи з різними алгоритмами та ключами. Це сприяє глибшому розумінню та закріпленню знань у практичному контексті.

2.4. Опис компонентної будови мобільного застосунку

Наш сайт-тренажер для вивчення криптографічних алгоритмів розроблений на платформі Wix і складається з чотирьох основних сторінок, кожна з яких виконує свою функцію для зручного і ефективного навчання та тестування користувачів.

Сторінка «Головна»

На сторінці «Головна» нашого сайту-тренажера знаходиться інформація, яка спрямована на введення користувача в тему та основні можливості застосунку (Рис. 2.7).

1) Вітання та основна інформація про застосунок:

- Коротке вітання користувачеві з оглядом нашого сайту-тренажера для вивчення криптографічних алгоритмів.
- Пояснення цілей застосунку: надання можливостей для навчання і практичного застосування криптографічних шифрів.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

- Викладення переваг використання сайту-тренажера: доступність, зручність і ефективність для вивчення складних криптографічних концепцій.
- 2) Загальна інформація про криптографічні шифри, які вивчаються:
- Огляд основних криптографічних шифрів, які доступні для вивчення на сайті.
 - Вказівка на те, що детальніше вони розглядаються на сторінці «Навчальні матеріали».
- 3) Меню з усіма сторінками:
- Навігаційне меню, що містить посилання на всі інші сторінки сайту.
 - Зручний доступ до основних розділів: «Навчальні матеріали», «Візуалізації», «Практичний тест».
- 4) Огляд чотирьох обраних криптографічних шифрів:
- Короткий опис кожного з чотирьох обраних криптографічних шифрів.
 - Кожен опис супроводжується кнопкою, яка спрямовує користувача на сторінку «Навчальні матеріали» для докладнішого вивчення.

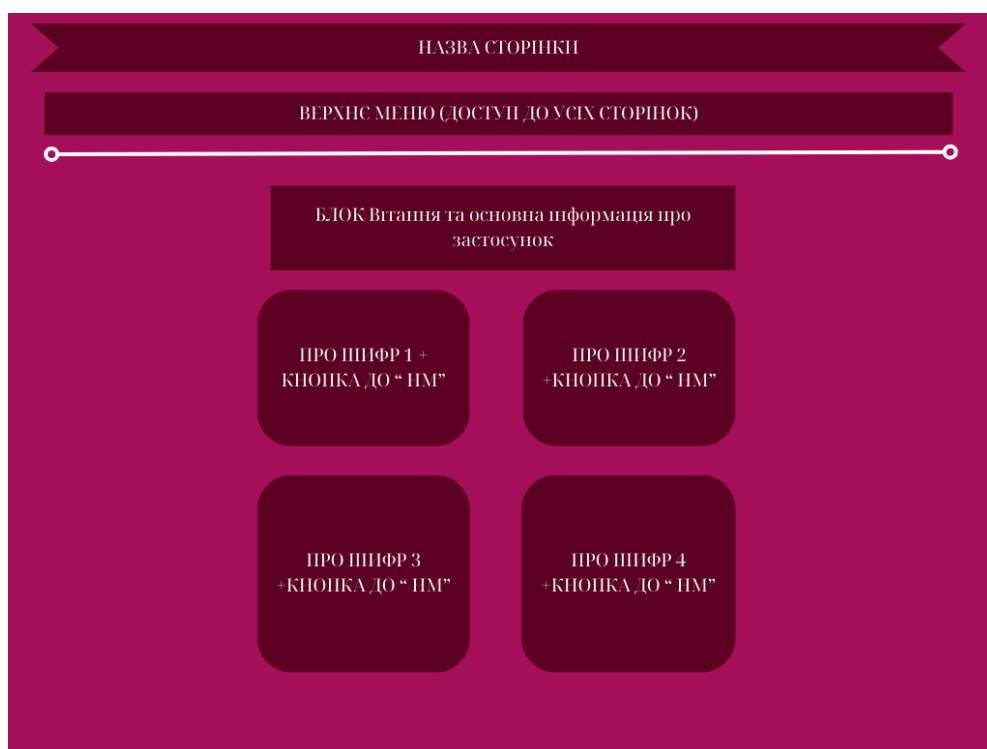


Рисунок 2.7 – Проектування майбутньої сторінки «Головна»

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Ця сторінка створена для забезпечення першого контакту користувача з сайтом-тренажером, яка дозволяє швидко та зрозуміло ознайомитися з основними функціями та можливостями нашого застосунку.

Сторінка «Навчальні матеріали»

На сторінці «Навчальні матеріали» детально розглянуті основні криптографічні алгоритми, доступні для вивчення нашими користувачами (Рис. 2.8).

1) Детальний опис криптографічних алгоритмів:

- Шифр Цезаря:
 - Повний аналіз принципу дії алгоритму.
 - Відображення схеми шифрування.
 - Приклади з конкретними текстами та ключами.
 - Ілюстрації, що демонструють процес шифрування та дешифрування.
- Шифр Плейфера:
 - Докладне пояснення структури алгоритму.
 - Відображення основних етапів шифрування.
 - Приклади з використанням конкретних ключів та текстів.
 - Графічні схеми для наглядності процесу шифрування.
- Шифр Віженера:
 - Аналіз криптографічних принципів, на яких базується алгоритм.
 - Ілюстрації ключових аспектів шифру.
 - Зразки шифрування та дешифрування для різних ключів.
 - Графічні візуалізації для кращого розуміння процесу роботи алгоритму.
- Шифр частоколу:
 - Повне пояснення структури та принципу дії шифру.
 - Відображення відмінностей від інших шифрів.
 - Реальні приклади застосування в різних сценаріях.
 - Малюнки та діаграми для кращого усвідомлення основних концепцій.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

2) Кнопка під кожним шифром для переходу на наступну сторінку «Візуалізації»:

- Зручні посилання для користувачів, які бажають детальніше ознайомитися з візуальними аспектами кожного криптографічного шифру.
- Це дозволяє користувачам переходити на наступний етап навчання з легкістю та без зайвих зусиль.

Ця сторінка призначена для глибокого вивчення криптографічних алгоритмів, надання ясного та комплексного огляду їхньої роботи, що сприяє покращенню розуміння користувачами принципів криптографії.

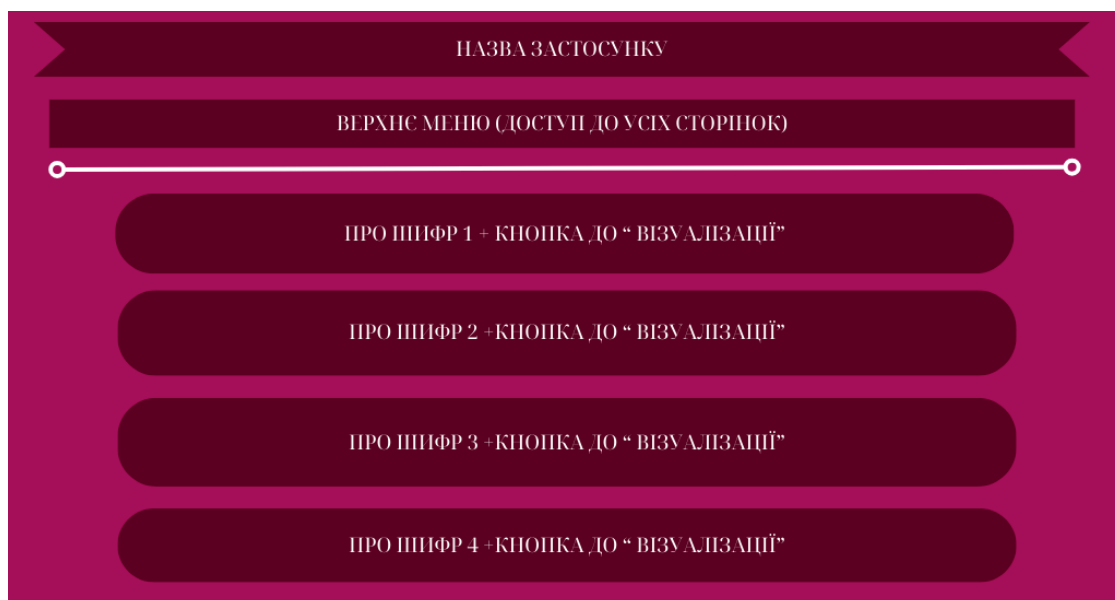


Рисунок 2.8 – Проектування майбутньої сторінки «Навчальні матеріали»
Сторінка «Візуалізації»

На сторінці «Візуалізації» ми надаємо докладне пояснення та візуалізацію роботи кожного криптографічного алгоритму, що вивчається у нашому тренажері (Рис. 2.9). Ця сторінка спрямована на глибше розуміння принципів шифрування та їхнього практичного застосування.

1) Детальне пояснення та візуалізація кожного шифру:

- Шифр Цезаря:
 - Пояснення основних кроків шифрування і дешифрування.
 - Візуалізація зміщення символів на задану кількість позицій.

- Ілюстрації, що демонструють процес зміни тексту після шифрування.
- Шифр Плейфера:
- Опис структури таблиці для шифрування.
- Відображення процесу заміни символів на пари за допомогою таблиці.
- Приклади шифрування та дешифрування з реальними текстами.
- Шифр Віженера:
- Розгляд ключового слова та його використання для шифрування.
- Графічні діаграми, що показують послідовність дій у шифруванні.
- Приклади застосування з різними ключами та текстами.
- Шифр частоколу:
- Огляд принципу побудови шифру та його основних характеристик.
- Графічні схеми для наглядності процесу шифрування.
- Реальні сценарії застосування шифру в практичних випадках.

2) Реалізація тренажерів для кожного алгоритму:

Для кожного з розглянутих криптографічних алгоритмів ми реалізували тренажер, що дозволяє користувачам:

- Ввести фразу чи слово для шифрування.
- Обрати ключ або кодову фразу, необхідну для кожного конкретного шифру.
- Після натискання кнопки «шифр» отримати результат шифрування.

Це дозволяє користувачам не лише ознайомитися з теоретичними аспектами кожного шифру, але й набути практичних навичок у їх застосуванні.

3) Кнопка для переходу на сторінку «Практичний тест»:

На кінцевому етапі сторінки «Візуалізації» розміщено кнопку, що дозволяє користувачам перевірити свої знання та навички, переходячи на наступну сторінку «Практичний тест». Тут доступні теоретичні питання та завдання, які допомагають закріпити засвоєні матеріали і перевірити їх розуміння.

Ця сторінка спрямована на повністю інтерактивне навчання з криптографічних алгоритмів, роблячи навчання цих складних концепцій доступним і зрозумілим для користувачів будь-якого рівня підготовки.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				36
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.9 – Проектування майбутньої сторінки «Візуалізації»

Сторінка «Практичний тест»

На цій сторінці представлені теоретичні питання, спрямовані на перевірку знань користувачів з криптографії. Кожне питання супроводжується можливістю користувача ввести свою відповідь.

1) Постановка теоретичних питань:

- Пояснення основних понять
- Визначення криптографії та її основних завдань.
- Розбіжність між симетричними та асиметричними криптосистемами.
- Шифрування та дешифрування
- Основні етапи процесу шифрування та дешифрування.
- Приклади застосування шифрів у реальних ситуаціях.
- Криптографічні алгоритми
- Огляд основних криптографічних алгоритмів (Шифр Цезаря, Шифр Плейфера, Шифр Віженера, шифр частоколу).
- Опис особливостей кожного з них та сфер їхнього застосування.

2) Реалізація завдань:

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Кожне теоретичне питання супроводжується можливістю користувача ввести свою відповідь у відповідне поле на сайті-тренажері. Після введення відповіді, користувач може перевірити її на правильність за допомогою кнопки «Перевірити». Система надає зворотний зв'язок щодо правильності відповіді та деталізацію правильної відповіді у випадку помилки.

Ця сторінка спрямована на те, щоб перевірити рівень розуміння користувачами основних концепцій криптографії, а також допомогти закріпити теоретичні знання через інтерактивні завдання та миттєву перевірку результатів.

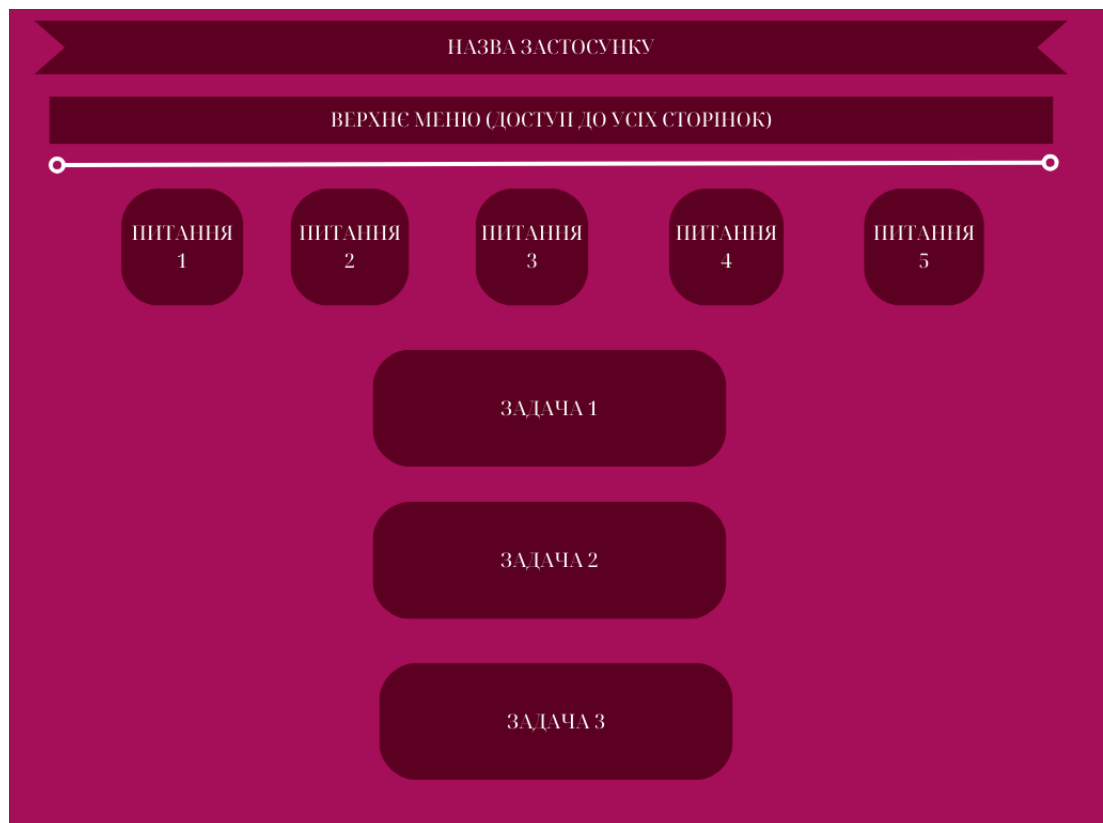


Рисунок 2.10 – Проектування майбутньої сторінки «Практичний тест»

Висновок до другого розділу

У другому розділі нашої роботи детально розглядаються аспекти розробки та впровадження інтерактивного мобільного застосунку для тестування криптографічних алгоритмів. Департамент складається з кількох ключових відділів, кожен з яких відіграв важливу роль у формуванні нашого проєкту та його реалізації.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Параметри використання системи дозволяють користувачам вивчати основні поняття шифрування та використовувати нашу програму для навчання, самостійної роботи чи підготовки до іспитів. Завдяки зручному інтерфейсу та організованому представленню матеріалу користувачі можуть ефективно вивчати складні криптографічні концепції.

Опис реалізації функцій системи включає розробку та впровадження криптографічних алгоритмів у мобільних додатках. Кожен із обраних шифрів (шифр Цезаря, шифр Плейфера, шифр Вігенера, шифр Палісад) детально описано та реалізовано з урахуванням деталей його роботи та сценаріїв практичного застосування.

Опис архітектури програми надає повну інформацію про архітектурні компоненти системи, їх взаємодію та залежності. Використання платформи Wix для створення навчального веб-сайту сприяло легкості та швидкості розробки, одночасно забезпечуючи високий рівень зручності та доступності для користувачів.

Висновки та перспективи подальшого вдосконалення свідчать про успіх у досягненні цілей, викладених у другому розділі. Розроблений мобільний застосунок не тільки відповідає вимогам сучасних технологій, але й відкриває нові можливості для подальшого розвитку у сфері навчання кодуванню. Перспективи включають розширення функціональності, покращення безпеки та інтеграцію з іншими платформами для забезпечення більшої доступності та простоти використання.

Таким чином, друга частина нашої роботи демонструє нашу здатність проєктувати та впроваджувати складні ІТ-системи, спрямовані на ефективне навчання та розвиток у сфері криптографії.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

РОЗДІЛ 3. ОПИС ІНТЕРФЕЙСУ, ПОРЯДОК РОБОТИ ТА НАЛАШТУВАННЯ ЗАСТОСУНКУ, ТЕСТУВАННЯ РЕАЛІЗОВАНИХ АЛГОРИТМІВ

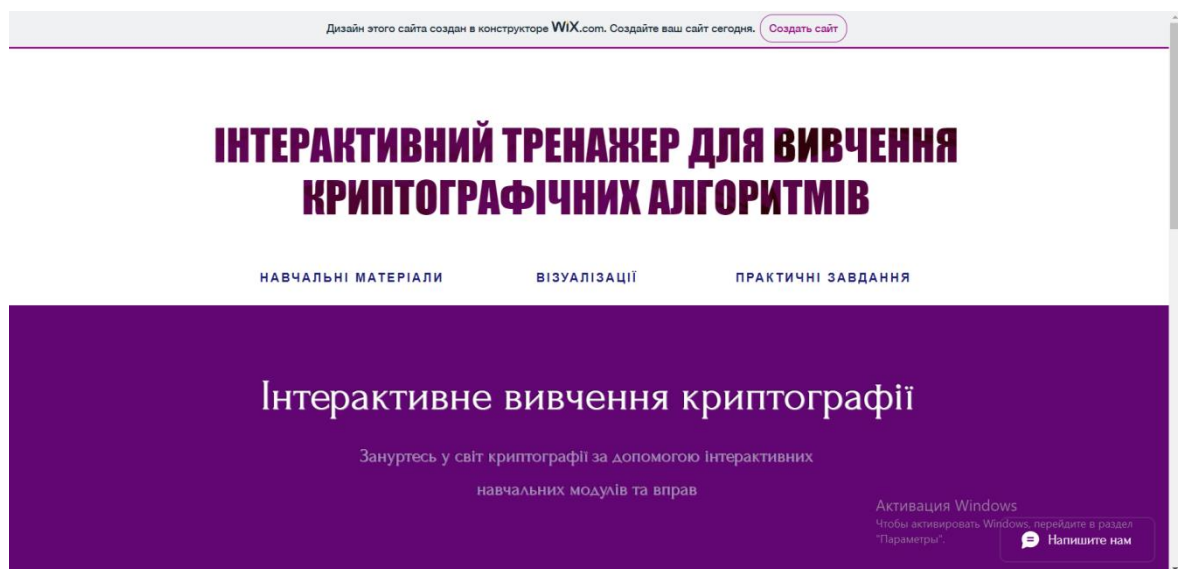
3.1. Структура та основні елементи інтерфейсу застосунку

У цьому розділі детально описано інтерфейс мобільного застосунку, розробленого для вивчення криптографічних алгоритмів. Описано основні елементи інтерфейсу, їх функціональні можливості та способи взаємодії з користувачем.

Основні елементи інтерфейсу (Рис. 3.1-3.3)

Головний екран (Home):

1. Привітання та загальна інформація: коли користувач переходить на головний екран, його вітають і надають загальну інформацію про програму та її призначення.
2. Навігаційне меню: меню з кнопками для переходу до інших сторінок програми, таких як «Дослідження», «Візуалізації», «Треновий тест» тощо.
3. Основна інформація про представлені шифри та кнопки «Детальніше» біля кожного що посилають до сторінки «Навчальні матеріали» індивідуально під кожную секцію.



		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Наш мобільний застосунок пропонує унікальний підхід до вивчення криптографічних алгоритмів. Ви зможете ознайомитися з теорією, спостерігати за візуалізацією алгоритмів та закріпити знання через інтерактивні вправи.

↓ Спробуйте зараз ↓



ШИФР ЦЕЗАРЯ
Один з найдавніших та найбільш поширених шифрів простої (моноалфавітної) заміни, названий на честь римського імператора Гая Юлія Цезаря

Дізнатися більше



ШИФР ЧАСТОКОЛУ
Транспозиційний шифр, який полягає в написанні тексту зигзагом по кількох рядках і потім зчитуванні його по рядках

Дізнатися більше



ШИФР ПЛЕЙФЕРА
Метод шифрування, який використовує матрицю (5x5), заповнену ключовим словом і рештою алфавіту, для шифрування біграм (пар літер) шляхом заміни їх на інші пари літер за певними правилами.

Дізнатися більше



ШИФР ВІГЕНЕРА
Шифр, що складається з послідовності декількох шифрів Цезаря з різними значеннями зсуву, що визначаються літерами ключового слова.

Дізнатися більше

Активация Windows
"Чтобы активировать Windows, перейдите в меню 'Параметры'."

Напишите нам

Рисунки 3.1-3.3 – Інтерфейс головної сторінки

Сторінка «Навчальні матеріали» (Рис. 3.4-3.11):

1. Опис криптографічних алгоритмів: докладний опис кожного криптографічного алгоритму, наприклад шифр Цезаря, шифр Плейфера, шифр Вігенера, шифр пікету, із діаграмами, прикладами та зображеннями.
2. Кнопки переходу: під кожним алгоритмом розташована кнопка, за допомогою якої можна перейти до наступної сторінки «Візуалізації».

ІНТЕРАКТИВНИЙ ТРЕНАЖЕР ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ



		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Принцип роботи

Шифрування в шифрі Цезаря здійснюється за допомогою формули:
$$C = (P + K) \bmod 26$$
$$P = (C - K) \bmod 26$$
де CCC – це зашифрована літера,
PPP – початкова літера,
KKK – ключ (кількість позицій для зміщення).
Для дешифрування використовується формула:
$$P = (C - K) \bmod 26$$
$$P = (C - K + 26) \bmod 26$$

ВІЗУАЛІЗАЦІЯ

Приклад шифрування та дешифрування

Приклад: зашифруємо слово "HELLO" з ключем 3.

- H → K
- E → H
- L → O
- L → O
- O → R

Зашифроване повідомлення: "KHOOR"

ПЕРЕВАГИ :

- Простота реалізації.
- Швидкість шифрування та дешифрування.

Недоліки:

- Легкість розшифрування без ключа.
- Вразливість до частотного аналізу.

Активация Windows

Чтобы активировать Windows, перейдите на сайт "Параметры".

Напишите нам

Шифр Частоголу

Шифр Частоголу – це античний метод шифрування, використовуваний у давнину для конфіденційності повідомлень.

Принцип роботи

Шифрування в шифрі Частоголу здійснюється за допомогою спеціального кругового пристрою, де кожна літера тексту замінюється на відповідну літеру на колі, зміщену на певну кількість позицій.

ВІЗУАЛІЗАЦІЯ

Приклад шифрування та дешифрування:

Приклад: зашифруємо слово "SECRET" з ключем 3

- S → V
- E → H
- C → F
- R → U
- E → H
- T → W

Зашифроване повідомлення: "VHFUHW"

Переваги та недоліки:

Переваги:

- Складний для розшифрування без спеціального пристрою.
- Використовується для забезпечення високого рівня конфіденційності.

Недоліки:

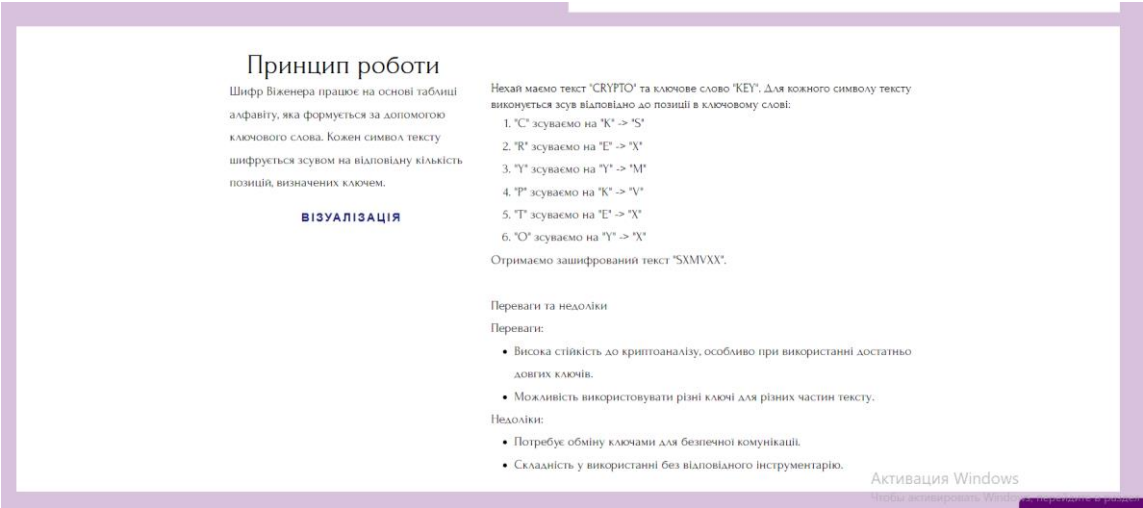
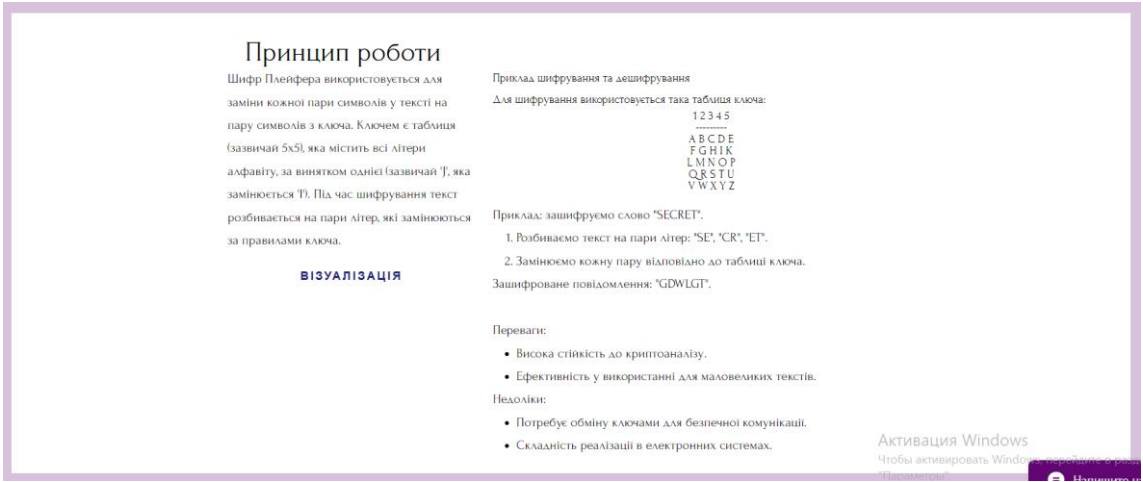
- Слабкість перед сучасними криптографічними атаками
- Відсутність застосування в сучасних умовах.

Активация Windows

Шифр Плейфера

Шифр Плейфера — це поліалфавітний шифр заміни, який використовується для шифрування пар символів. Вперше використовувався в кінці XIX століття для військових потреб. Названий на честь свого винахідника — Шарля Плейфера.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				42
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунки 3.4-3.11 – Інтерфейс сторінки «Навчальні матеріали»

Сторінка «Візуалізації» (Рис. 3.12-3.21):

1. Детальне пояснення алгоритмів: демонстрація та опис роботи кожного криптографічного алгоритму з ілюстраціями та прикладами шифрування.
2. Реалізація симуляторів: для кожного алгоритму реалізовано симулятор, у якому користувач може ввести фразу або слово, яке потрібно зашифрувати, вибрати ключ або кодову фразу та після натискання кнопки «зашифрувати» отримати результат шифрування.

3. Кнопка «Практичний тест»: внизу сторінки є кнопка, яка переведе вас на сторінку «Практичний тест».

Дизайн этого сайта создан в конструкторе **WIX.com**. Создайте ваш сайт сегодня.

Создать сайт

ІНТЕРАКТИВНИЙ ТРЕНАЖЕР ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

НА ГОЛОВНУ

ШИФР ЦЕЗАРЯ

Візуалізація роботи Шифру Цезаря

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

У цьому шифрі кожна літера повідомлення зсувається в алфавіті на K позицій вперед від символу, що замінюється. При досягненні кінця алфавіту виконується циклічний перехід до його початку. При необхідності розділові знаки та пробіли ігноруються. Таким чином, наприклад, літери алфавіту відповідатимуть числові позиції

Ключем шифрування є деяке фіксоване секретне число K – від 1 до 25 для англійського (латинського) алфавіту та K – від 1 до 32 для українського. При дешифруванні літери зашифрованого тексту замінюються на літери розташовану в алфавіті на K позицій назад.

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Напишіть нам

Розглянемо приклад:

Відома, що Цезарь для шифрування використовував ключ K=3, тобто відбувся зсув символів повідомлення на три позиції вперед у латинському алфавіті. Отже, повідомлення римського імператора ALEA IACTA EST обереть кінцевий після зашифрування буде мати вигляд DONDMDFWDMVV

Спробуйте Шифр Цезаря самостійно

ВВЕДІТЬ СВОЄ ПОВІДОМЛЕННЯ АНГЛІЙСЬКОЮ *

ОБЕРНІТЬ КЛЮЧ

ШИФР

Ваш шифр:

ШИФР ЧАСТОКОЛУ

Візуалізація роботи Шифру Частоколу

Original Message: Hello World

H	e	l	o	W	r	l	d

Encrypted Message: Horel ollWd

Шифр частоколу є представником шифрів перестановки. Ключем є шле число K – висота частоколу. При шифруванні літери повідомлення записуються як степені (ix кількість висота частоколу), а потім отримані літери в степенях переплітаються по рядках зверху донизу.

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Розглянемо приклад:

Зашифруємо повідомлення Я ОТРИМАЮ ІСПИТ АВТОМАТОМ із ключем K=3. Записавши по три літери зверху догори, а потім зверху до низу по рядках, отримаємо шифротекст

Я	О	Т	М	І	Н	В	М	О
О	Н	Ю	П	А	О	Т		
Я	Р	А	С	Т	Т	А	М	

поблизу підраховувати кількість літер шифротексту, поділити їх на ключ та записати літери по K штук (K – ключ) в порядку зверху донизу.

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Спробуйте Шифр Частокоту самостійно

ВВЕДІТЬ СВОЄ ПОВІДОМЛЕННЯ АНГЛІЙСЬКОЮ *

ВВЕДІТЬ ЗНАЧЕННЯ КЛЮЧА *

ШИФР

Ваш шифр:

ШИФР ПРЕЙФЕРА

Візуалізація роботи Шифру Преїфера

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Шифр Преїфера є біграмним, тобто текст повідомлення розбивається на біграми (групи з двох символів). Таким чином, шифр Преїфера є більш стійкий до зламів у порівнянні із шифром Цезаря, так як ускладнюється його частотний аналіз. Він може бути проведений, але не для 26 можливих символів (англійський алфавіт), а для $26 \times 26 = 676$ можливих біграм.

Для шифрування шифр Преїфера використовує матрицю 5x5 (для англійського алфавіту), яка містить ключове слово або фразу. Щоб скласти ключову матрицю, в першу чергу потрібно заповнити порожні клітинки матриці літерами ключового слова (виключаючи літери, що повторюються), потім заповнити клітинки, що лишилися символами алфавіту, що не зустрічаються в ключовому слові, по порядку. В англійських текстах зазвичай пропускається символ «Q», щоб зменшити алфавіт, в інших версіях «i» та «j» об'єднуються в одну клітинку.

Для того щоб зашифрувати повідомлення, необхідно розбити його на біграми (групи з двох символів) та відшукати ці біграми в матриці. Якщо кількість літер повідомлення непарна, то для формування останньої біграми додається символ «X».

Активация Windows
Чтобы активировать Windows, перейдите в раздел
"Параметры".

Для того щоб зашифрувати повідомлення, необхідно розбити його на біграми (групи з двох символів) та відшукати ці біграми в матриці. Якщо кількість літер повідомлення непарна, то для формування останньої біграми додається «X».

Два символи біграми відповідають кутам прямокутника в ключовій матриці. Визначаємо положення кутів цього прямокутника відносно один одного. Потім, керуючись наступними 4 правилами, зашифрувати пари символів вихідного тексту.

Правила шифрування біграм

1. Якщо дві літери біграми однакові – додаємо після першого символу «X».
2. Якщо літери біграми знаходяться в різних стовпцях і різних рядках – заміняємо їх на літери, що знаходяться в тих самих рядках (стовпцях), але відповічно в інших кутах прямокутника.
3. Якщо літери біграми зустрічаються в одному рядку – заміняємо їх на літери, розташовані в найближчих стовпцях праворуч від відповічних літер. Якщо літера остання у рядку, то вона заміняється на перший символ цього ж рядка.
4. Якщо літери біграми зустрічаються в одному стовпці – перетворюємо їх в літери того ж стовпця, що знаходяться безпосередньо під ними. Якщо літера є нижньою в стовпці – вона заміняється на першу літеру цього ж стовпця.

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Розглянемо приклад:

Зашифруємо повідомлення HIDE THE GOLD IN THE TREE STUMP із використанням ключової фрази PLATFAIR EXAMPLE. Матрицю шифрування буде матрицю описана на малюнку.

Для шифрування розіємо текст на біграми HI DE TH EG OL DI NT HE TR EX ES TU ME. Знаємо літери першої біграми у матриці та заміняємо їх на літери, що знаходяться у протилежних кутах прямокутника.

Далі, користуючись правилами шифрування біграм, отримуємо шифротекст: BM ND ZB XD KY BE JV DM UI XM MN LV JE.

Активация Windows
Чтобы активировать Windows, перейдите в раздел
"Параметры".

Нажмите на

		Прут А.О.		
		Щур Н.О.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 123 – 24 – ПЗ

Арк.

45

Спробуйте Шифр Прейфера самостійно

ВВЕДІТЬ СВОЄ ПОВІДОМЛЕННЯ АНГЛІЙСЬКОЮ *

ВВЕДІТЬ ЗНАЧЕННЯ КЛЮЧА *

ШИФР

Ваш шифр:

ШИФР ВІЖЕНЕРА

Визуалізуйте роботу Шифру Віженера

Чтобы активировать Windows, перейдите в раздел "Параметры".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

На протязі століть використання простого моноalfавітного шифру зміни було достатнім, щоб забезпечити таємність. Подальший розвиток частотного криптоаналізу, спочатку арабами, а потім і в Європі, зруйнував його стійкість. Таким чином криптографи мали придумати новий, більш стійкий шифр. Вчений епохи Відродження Леона Батіста Альберті вперше запропонував замість одного секретного алфавіту, використовувати два або більше, послідовно або циклічно змінюючи їх за певним правилом. Грунтуючись на ідеях попередників, свій шифр створив французький посол в Римі Блез де Віженер. Шифр Віженера складається з послідовності декількох шифрів Цезаря з різними значеннями зсуву, що визначаються літерами ключового слова. Кожна літера відкритого тексту зсувається вперед на позицію відповідално літери ключа. Якщо ключове слово менше за повідомлення, то воно циклічно повторюється. Для зашифрування може використовуватися й таблиця Віженера

Активация Windows

Чтобы активировать Windows, перейдите в раздел "Параметры".

Напишите нам

A	T	T	A	S	K	A	T	D	A	W	N
L	E	M	O	N	L	E	M	O	N	L	E
0	19	19	0	2	10	0	19	3	0	22	13
11	4	12	14	13	11	4	12	14	13	11	4
11	23	5	14	15	21	4	5	17	13	7	17
L	X	F	O	R	V	E	F	R	N	H	R

Розглянемо приклади:

Повідомлення ATTACK AT DAWN зашифровано ключем LEMON. В результаті чого отримаємо шифротекст LXOFVEFRNHR.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Розглянемо приклади:

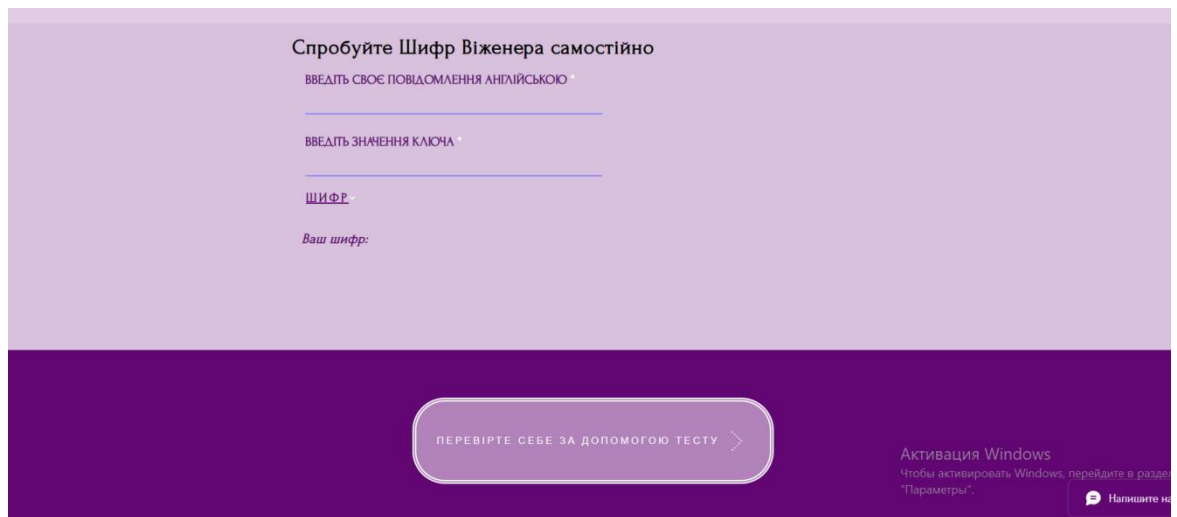
Повідомлення PURPLE зашифровано ключем SMART за допомогою таблиці Віженера, перетвориться у шифротекст HGRGEW.

При дешифруванні потрібно відшукати у першому стовпчику літеру ключа і за літерами шифротексту визначити, в якому стовпчику зверху знаходиться літера відкритого тексту.

Активация Windows

Чтобы активировать Windows, перейдите в раздел "Параметры".

Напишите нам



Рисунки 3.12-3.21 - Інтерфейс сторінки «Візуалізації»

Сторінка «Практичний тест» (Рис. 3.22-3.26)

На сторінці «Практичний тест» розглядаються теоретичні аспекти криптографії через постановку питань та виконання завдань, які дозволяють користувачам перевірити свої знання та навички.

Вміст сторінки включає:

1. Теоретичні питання з криптографії:
2. Формулювання теоретичних запитань, які покривають ключові аспекти криптографічних алгоритмів, такі як принципи роботи, основні характеристики, застосування тощо.
3. Включення можливості перевірки правильності відповідей, що дозволяє користувачам самостійно оцінити свої знання.
4. Представлення конкретних завдань, до яких включені практичні аспекти використання криптографічних алгоритмів.
5. Можливість введення відповідей користувачами і перевірка їх на правильність.
6. Включення можливості повернутися до інших розділів застосунку для подальшого вивчення або тренування.

Ця сторінка спрямована на практичне застосування теоретичних знань з криптографії, що надає користувачам можливість перевірити свої знання через виконання завдань та перевірку правильності відповідей.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

ІНТЕРАКТИВНИЙ ТРЕНАЖЕР ДЛЯ ВИВЧЕННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

НА ГОЛОВНУ

НАВЧАЛЬНІ МАТЕРІАЛИ

ВІЗУАЛІЗАЦІЇ



Практичний тест

Після ознайомлення з навчальним матеріалом, ми запрошуємо вас пройти практичний тест для закріплення отриманих знань. Цей тест дозволить вам випробувати свої вміння застосовувати криптографічні алгоритми в реальних умовах та підготуватися до використання їх у практичних завданнях.

Активация Windows

Чтобы активировать Windows, перейдите в раздел «Получить ключ»

Питання №1

Шифр, в якому літери тексту циклічно замінюються на літери в алфавіті на k позицій вперед (праворуч), де k – ключ, називається шифром...

- a) Полубія
- б) Цезаря
- в) Хула
- г) Плейфера
- д) Вікенера

Перевірити

Привітання відоміадам:

Питання №2

Який вигляд буде мати повідомлення CAESAR після зашифрування за допомогою шифру Цезаря з ключем 3?

- a) BZDRZQ_
- б) FDHVDU
- в) HFJXFW
- г) HZJZHY
- д) ECGUCT

Перевірити

Привітання відоміадам:

Питання №3

Який вигляд буде мати повідомлення CRYPTOGRAPHY після зашифрування за допомогою шифру частотного з ключем 3?

- a) YQWRTIRHCFQF
- б) KTRHVNQNSCFQF
- в) FUSBNYRUSQXS
- г) CRPYTGORPHYU
- д) YRCARGOTRYUR

Перевірити

Привітання відоміадам:

Питання №4

У шифру Плейфера, для того, щоб зашифрувати повідомлення необхідно спочатку... 30

- a) розбити його на діпаграми
- б) визначити координати кожної літери в квадраті
- в) знайти порядковий номер кожної літери за таблицею
- г) розбити його на триграми
- д) літери повідомлення записати як степені

Перевірити

Привітання відоміадам:

Активация Windows

Чтобы активировать Windows, перейдите в раздел «Получить ключ»

Напи

Питання №5

Який шифротекст буде у результаті шифрування слова CAR за допомогою шифру Плейфера із заданою ключовою матрицею?

- a) HSER
- б) SHER
- в) XVSE
- г) ORKD
- д) BDAN

Перевірити

Привітання відоміадам:

B	A	K	K	H
O	S	E	B	C
F	G	I	T	M
N	P	Q	U	V
V	W	X	Y	Z

Питання №6

Відкритий текст APRICOT зашифровано за допомогою шифру Цезаря як FUWNHTY. Яку довжину ключа використано?

- a) 10
- б) 7
- в) 3
- г) 23
- д) 5

Перевірити

Привітання відоміадам:

Питання №7

Шифр Вікенера є шифром...

- a) моноалфавітної заміни
- б) поліалфавітної заміни
- в) моноалфавітної перестановки
- г) поліалфавітної перестановки
- д) моноалфавітної підстановки

Перевірити

Привітання відоміадам:

Питання №8

Якщо слово WISDOM зашифрувати за допомогою шифру Вікенера з ключем GREAT, то отримаємо шифротекст...

- a) CQVMAFU
- б) KXMFPS
- в) CZWDHS
- г) DZWDIS
- д) BYVCHR

Перевірити

Привітання відоміадам:

Активация Windows

Чтобы активировать Windows, перейдите в раздел «Получить ключ»

Напи

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				48
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунки 3.22-3.26 - Інтерфейс сторінки «Практичний тест»

Функціонал і способи взаємодії з користувачем.

Кожен елемент інтерфейсу розроблено з урахуванням простоти використання та навігації користувача.

Навігаційне меню забезпечує легкий доступ до всіх функцій і розділів програми.

Кнопки на кожній сторінці дозволяють інтуїтивно зрозуміло переходити до потрібного вмісту.

Симулятори дозволяють користувачам не тільки вивчати теорію, але й отримати практичний досвід використання криптографічних методів.

У цій частині детально описано структуру та основні елементи інтерфейсу мобільного застосунку, розробленого для дослідження криптографічних алгоритмів, його функціональні можливості та способи взаємодії з користувачем.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2. Порядок роботи із мобільним застосунком та тестовий приклад

У цьому підрозділі описано послідовність дій користувача при використанні розробленої системи для вивчення криптографічних алгоритмів. Процес взаємодії з додатком детально розглядається крок за кроком, включаючи введення вхідних даних, вибір параметрів шифрування та отримання результату.

Порядок роботи із мобільним застосунком

1) Запуск застосунку:

Користувач запускає мобільний застосунок для вивчення криптографічних алгоритмів.

2) Головна сторінка:

На головній сторінці відображається вітання та основна інформація про застосунок.

Користувач отримує доступ до меню з усіма розділами застосунку, включаючи «Навчальні матеріали», «Візуалізації», та «Практичний тест».

3) Навчальні матеріали:

Користувач переходить на сторінку «Навчальні матеріали», де детально описані криптографічні алгоритми (Шифр Цезаря, Шифр Плейфера, Шифр Віженера, шифр частого колу) зі схемами, прикладами та малюнками.

Під кожним алгоритмом розміщені кнопки для переходу до сторінки

4) «Візуалізації»:

На сторінці «Візуалізації» користувач може ознайомитися з детальним поясненням та візуалізацією кожного криптографічного алгоритму.

Реалізовані тренажери для кожного алгоритму, де користувач може ввести фразу чи слово для шифрування, обрати ключ або кодову фразу, а після натискання кнопки «шифр» отримати результат шифрування.

Кнопка для переходу на сторінку «Практичний тест».

5) Практичний тест:

На сторінці «Практичний тест» користувач виконує теоретичні питання з криптографії та розв'язує практичні завдання.

Користувач вводить свої відповіді і перевіряє їх на правильність.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Після завершення тесту користувач може переглянути правильні відповіді і аналізувати результати.

Тестовий приклад

Для ілюстрації роботи системи наведемо тестовий приклад використання одного з криптографічних алгоритмів, наприклад, Шифру Цезаря (Рис. 3.27):

1. Введення вхідних даних:

Користувач вводить текстову фразу для шифрування.

2. Вибір параметрів шифрування:

Вибір ключа або зсуву для Шифру Цезаря.

3. Отримання результату:

Після натискання кнопки «шифр» система виводить результат шифрування.

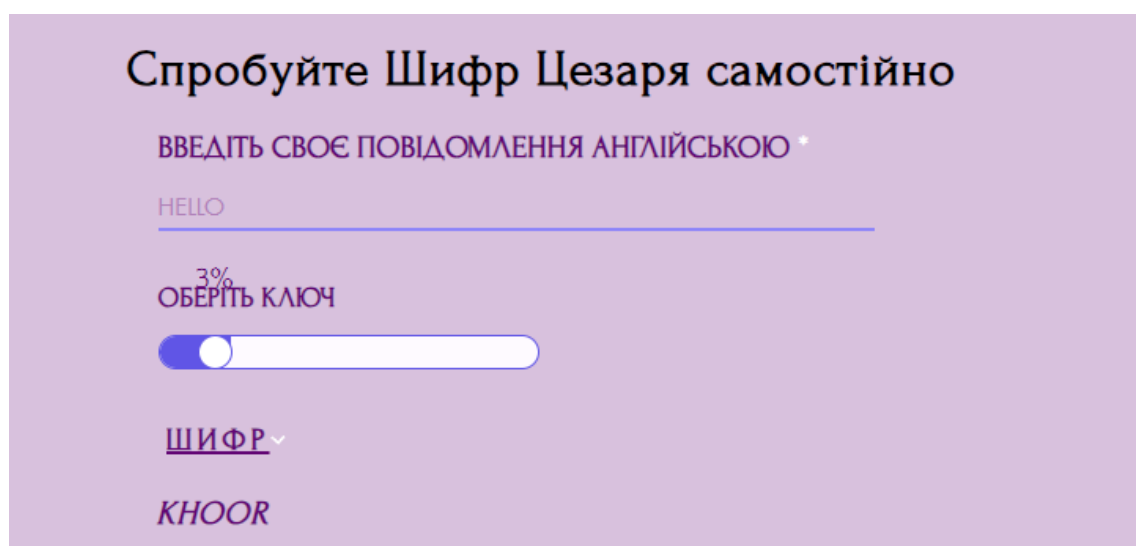


Рисунок 3.27 – Вдалий результат шифрування Цезаря

Таким чином, описаний порядок роботи демонструє як користувач може взаємодіяти з розробленим застосунком, використовуючи різні криптографічні алгоритми для навчання та практичного тестування своїх знань.

Висновки до третього розділу

Третій розділ цієї роботи є ключовим кроком у вивченні та впровадженні мобільного застосунку для вивчення криптографічних алгоритмів. Він містить детальний опис усіх аспектів системи, від опису інтерфейсу до тестування реалізованих алгоритмів.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

У цьому розділі представлено детальний аналіз інтерфейсу користувача, включаючи всі основні компоненти та їхні функції. Описано структуру програми, її елементи та способи взаємодії з користувачем, що забезпечують комфортне та інтуїтивно зрозуміле використання програми.

Представлена послідовність дій користувача при роботі з системою: від введення вхідних даних до отримання результату шифрування. Кожен крок процесу ретельно аналізується та документується, що сприяє чіткому розумінню функціональних можливостей програми.

Тестування реалізованих алгоритмів підтвердило їх ефективність та надійність відповідно до сучасних криптографічних стандартів. Отримані результати демонструють високу якість програмного комплексу та його придатність у реальних умовах.

Цей розділ визначає ключові параметри успіху та функціональності мобільного застосунку, що створюється. Це основа для постійного вдосконалення та оптимізації системи, що стимулює її розвиток у майбутньому. Отримані результати дозволяють зробити висновки про готовність програмного забезпечення до впровадження на практиці та його корисність для кінцевих користувачів.

Наприкінці можна відзначити, що загалом були не тільки представлені технічні аспекти реалізації програми, а й підкреслюється її важливість у контексті вимог сучасного програмного забезпечення. Отримані результати підтверджують успішність обраного підходу до створення мобільного застосунку для дослідження криптографії, що відкриває широкі перспективи для його розвитку та подальшого використання.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

ВИСНОВКИ

Метою даної кваліфікаційної роботи була розробка та впровадження мобільного застосунку для вивчення криптографічних алгоритмів. Процес розробки включав впровадження кількох базових шифрів, створення інтерактивного інтерфейсу користувача, впровадження симуляторів і практичних тестів для перевірки знань користувачів. У підсумку проаналізуємо отримані результати та надані відповіді на завдання.

Розроблений застосунок має інтуїтивно зрозумілий і дружній інтерфейс, який дозволяє користувачам легко вивчати та використовувати криптографічні алгоритми. Інтерфейс забезпечує зручний доступ до всіх функцій програми, що є важливим аспектом ефективного навчання.

У роботі за допомогою сучасних методів програмування реалізовано шифр Цезаря, шифр Плейфера, шифр Віженера та шифр частоколу. Кожен алгоритм було ретельно перевірено, щоб підтвердити, що він працює правильно та відповідає вимогам криптографії.

Розроблені тренажери дозволяють користувачам відпрацьовувати навички шифрування в реальному часі. Практичний іспит дає вам можливість перевірити набуті знання та провести самооцінку, допомагаючи поглибити ваше розуміння криптографічних алгоритмів.

Проведені дослідження підтвердили високу ефективність і надійність реалізованих алгоритмів. Вони продемонстрували стабільну продуктивність і відповідність криптографічним стандартам, підтвердивши свою придатність для навчальних цілей і практичного використання.

Загальною метою цієї роботи було створення комплексного інструменту, який допоможе користувачам оволодіти основами криптографії через практичне застосування. Отримані результати демонструють успішність запропонованих завдань і підготовку програми для майбутніх удосконалень і використання в освітніх цілях.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bruce Schneier, «Applied Cryptography: Protocols, Algorithms, and Source Code in C,» Wiley, 1996.
2. [Електронний ресурс] – Режим доступу: <https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+2nd+Edition-p-9780470068526>
3. William Stallings, «Cryptography and Network Security: Principles and Practice,» Pearson, latest edition.
4. Simon Singh, «The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography,» Fourth Estate, 1999.
5. [Електронний ресурс] – Режим доступу: <https://link.springer.com/book/10.1007/978-3-319-21936-4>
6. [Електронний ресурс] – Режим доступу: <https://ieeexplore.ieee.org/document/1055638>
7. Н.О. ЩУР, О.А. ПОКОТИЛО, “ ОСНОВИ КРИПТОЛОГІЇ Навчальний посібник”, 2021
8. [Електронний ресурс] – Режим доступу: <https://link.springer.com/book/10.1007/978-3-319-21936-4>
9. Васильченко І.І., Шидловський В.В. «Криптографія: теорія та практика». Київ: Видавничий дім «Слово», 2006.
10. [Електронний ресурс] – Режим доступу: <https://crypto.stanford.edu/~dabo/cryptobook/>
11. Сергієнко І.А., Лазаренко В.П., Гнатенко Л.В. «Основи криптографії». Київ: Видавничий дім «Академія», 2015.
12. Корягін В.В., Кричевський П.В., Мельничук А.О. «Комп’ютерна безпека та криптографія». Київ: Видавництво НТУУ «КПІ», 2010.
13. Городний М. М. «Криптографія: основи захисту інформації» — Навчальний посібник для студентів вищих навчальних закладів. Київ: Видавництво «Академія», 2016.

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

14. Грицай І. М. «Основи криптографії та захисту інформації» — Навчальний посібник. Львів: Видавництво «Львівська політехніка», 2017.
15. Шапіровський Ю.В., Ткачук В.Г. «Криптографія і захист інформації». Київ: Видавничий дім «Ін Юре», 2008.
16. Мельничук А.О., Титенко В.Г. «Криптографія та захист інформації». Київ: Видавничий дім «Логос», 2012.
17. [Електронний ресурс] — Режим доступу: <https://www.wiley.com/en-us/Cryptography%3A+Theory+and+Practice%2C+3rd+Edition-p-9781118080913>
18. [Електронний ресурс] — Режим доступу: <https://link.springer.com/book/10.1007/978-3-662-49896-5>
19. [Електронний ресурс] — Режим доступу: <https://crypto101.io/>
20. [Електронний ресурс] — Режим доступу: <https://link.springer.com/book/10.1007/978-3-662-07324-1>
21. [Електронний ресурс] — Режим доступу: <https://link.springer.com/book/10.1007/978-1-4757-5678-9>

ДОДАТКИ

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Кодинг реалізації задач та теоретичних питань на сторінці «Практичний тест»:

```
$w.onReady(function () {

//питання 1
// Додаємо обробник події onClick до кнопки з ідентифікатором button1
$( '#button1' ).onClick((event) => {
    // Встановлюємо текст, який хочемо відобразити
    const outputText = «Правильна відповідь: б) Цезаря»;

    // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
    $( '#text41' ).text = outputText;
});
})
```

```
//питання 2
// Додаємо обробник події onClick до кнопки з ідентифікатором button1
$( '#button2' ).onClick((event) => {
    // Встановлюємо текст, який хочемо відобразити
    const outputText = «Правильна відповідь: б) FDHVDU»;

    // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
    $( '#text42' ).text = outputText;
});
```

```
//питання 3
// Додаємо обробник події onClick до кнопки з ідентифікатором button1
$( '#button3' ).onClick((event) => {
    // Встановлюємо текст, який хочемо відобразити
    const outputText = «Правильна відповідь: г) CRPYTGORPANY»;

    // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
    $( '#text45' ).text = outputText;
});
```

```
//питання 4
// Додаємо обробник події onClick до кнопки з ідентифікатором button1
$( '#button4' ).onClick((event) => {
    // Встановлюємо текст, який хочемо відобразити
```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

const outputText = «Правильна відповідь: б) визначити координати кожної літери в квадраті Плейфера.»;

```
// Виводимо текст у текстовому полі за його ідентифікатором (#text39)
$w('#text48').text = outputText;
});
```

// питання 5

// Додаємо обробник події onClick до кнопки з ідентифікатором button1

```
$w('#button5').onClick((event) => {
  // Встановлюємо текст, який хочемо відобразити
  const outputText = «Правильна відповідь: б) SHER.»;
```

```
  // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
  $w('#text51').text = outputText;
});
```

//питання 6

// Додаємо обробник події onClick до кнопки з ідентифікатором button1

```
$w('#button8').onClick((event) => {
  // Встановлюємо текст, який хочемо відобразити
  const outputText = «Правильна відповідь: д) 5»;
```

```
  // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
  $w('#text60').text = outputText;
});
```

//питання 7

// Додаємо обробник події onClick до кнопки з ідентифікатором button1

```
$w('#button7').onClick((event) => {
  // Встановлюємо текст, який хочемо відобразити
  const outputText = «Правильна відповідь: б) поліалфавітної заміни»;
```

```
  // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
  $w('#text57').text = outputText;
});
```

//питання 8

// Додаємо обробник події onClick до кнопки з ідентифікатором button1

```
$w('#button6').onClick((event) => {
  // Встановлюємо текст, який хочемо відобразити
  const outputText = «Правильна відповідь: а) QRMAFU»;
```

```
  // Виводимо текст у текстовому полі за його ідентифікатором (#text39)
```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```
$w('#text54').text = outputText;
});
```

//задача 1

```
$w.onReady(function () {
    // Додати обробник події натискання кнопки
    $w('#button9').onClick(() => {
        // Отримати введені значення користувача з #input1
        let userInput = $w('#input1').value.trim().toLowerCase();

        // Очікуване значення відповіді
        let expectedAnswer = «wfmnsgbt»; // Замініть це на вашу очікувану відповідь

        // Порівняти введені значення з очікуваною відповіддю
        if (userInput === expectedAnswer) {
            // Якщо відповідь правильна
            $w('#text66').text = «Ваша відповідь - Правильна!»;
        } else {
            // Якщо відповідь неправильна
            $w('#text66').text = «Ваша відповідь - Неправильна!»;
        }
    });
});
```

//задача 2

```
$w.onReady(function () {
    // Додати обробник події натискання кнопки
    $w('#button10').onClick(() => {
        // Отримати введені значення користувача з #input1
        let userInput = $w('#input2').value.trim().toLowerCase();

        // Очікуване значення відповіді
        let expectedAnswer = «gb ut sd al ut up bg bm tg d»; // Замініть це на вашу
        очікувану відповідь

        // Порівняти введені значення з очікуваною відповіддю
        if (userInput === expectedAnswer) {
            // Якщо відповідь правильна
            $w('#text67').text = «Ваша відповідь - Правильна!»;
        } else {
            // Якщо відповідь неправильна
            $w('#text67').text = «Ваша відповідь - Неправильна!»;
        }
    });
});
```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

});

//задача 3
$w.onReady(function () {
    // Додати обробник події натискання кнопки
    $w('#button11').onClick() => {
        // Отримати введені значення користувача з #input1
        let userInput = $w('#input3').value.trim().toLowerCase();

        // Очікуване значення відповіді
        let expectedAnswer = «wntc hhrpn cktr»; // Замініть це на вашу очікувану
        відповідь

        // Порівняти введені значення з очікуваною відповіддю
        if (userInput === expectedAnswer) {
            // Якщо відповідь правильна
            $w('#text70').text = «Ваша відповідь - Правильна!»;
        } else {
            // Якщо відповідь неправильна
            $w('#text70').text = «Ваша відповідь - Неправильна!»;
        }
    }
});
});

```

		Прут А.О.			ККІКБ.КР.Б – 123 – 24 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		60