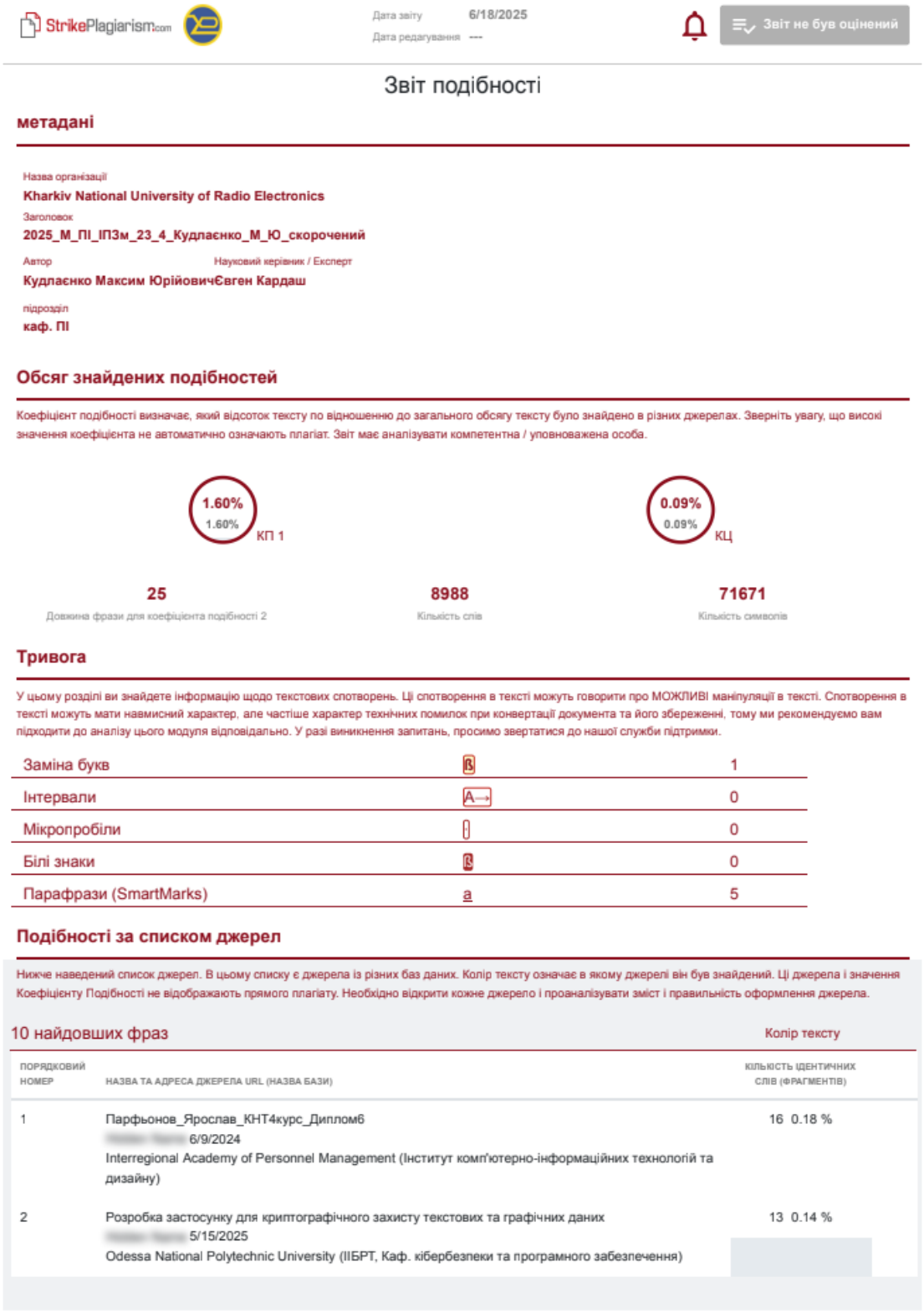
ДОДАТОК А

ЗВІТ РЕЗУЛЬТАТІВ ПЕРЕВІРКИ НА УНІКАЛЬНІСТЬ ТЕКСТУ В БАЗІ ХНУРЕ



StrikePlagiarism.com

Дата звіту 6/18/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Kharkiv National University of Radio Electronics
Заголовок
2025_М_ПІ_ІПЗм_23_4_Кудлаєнко_М_Ю_скорочений
Автор
Кудлаєнко Максим Юрійович
Науковий керівник / Експерт
Євген Кардаш
підрозділ
каф. ПІ

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

1.60% 1.60% КП 1

0.09% 0.09% КЦ

25	8988	71671
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	1
Інтервали	A→	0
Мікропробіли	¶	0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	5

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Парфьонов_Ярослав_КНТ4курс_Диплом6 6/9/2024 Interregional Academy of Personnel Management (Інститут комп'ютерно-інформаційних технологій та дизайну)	16 0.18 %
2	Розробка застосунку для криптографічного захисту текстових та графічних даних 5/15/2025 Odessa National Polytechnic University (ІІБРТ, Каф. кібербезпеки та програмного забезпечення)	13 0.14 %

Рисунок А.1 – Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ

3	https://elartu.tntu.edu.ua/bitstream/lib/48168/1/Master_Thesis__SBm-61_Hurskiy_V_B_2024.pdf	11 0.12 %
4	https://metod.vntu.edu.ua/getfile.php/9821.pdf	10 0.11 %
5	Магістр групи КП-31мн Бабак Артем Андрійович [redacted] 5/9/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФПМ, К-ра програмного забезпечення комп'ютерних систем)	10 0.11 %
6	ФКНТ_2024_122_ТроцькийЯВ [redacted] 11/20/2024 Ukrainian national aviation university (ФКНТ Кафедра комп'ютерних інформаційних технологій)	9 0.10 %
7	https://metod.vntu.edu.ua/getfile.php/9821.pdf	8 0.09 %
8	С 91_Вавровський_магістр [redacted] 11/26/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ІС33І, Спецjальна кафедра №1)	7 0.08 %
9	С 91_Вавровський_магістр [redacted] 11/26/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ІС33І, Спецjальна кафедра №1)	7 0.08 %
10	Дослідження та застосування методів криптографічного захисту інформації в цифрових комунікаційних системах [redacted] 3/15/2025 National Academy of the State Border Guard Service (Кафедра зв'язку та інформаційних систем)	7 0.08 %

з бази даних RefBooks (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

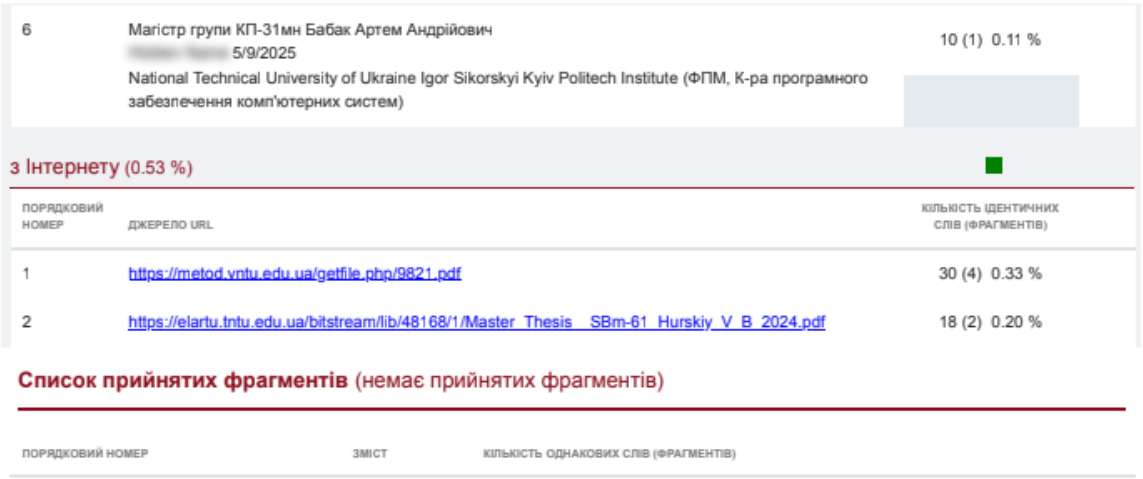
з домашньої бази даних (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з програми обміну базами даних (1.07 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Дослідження та застосування методів криптографічного захисту інформації в цифрових комунікаційних системах [redacted] 3/15/2025 National Academy of the State Border Guard Service (Кафедра зв'язку та інформаційних систем)	23 (4) 0.26 %
2	Розробка застосунку для криптографічного захисту текстових та графічних даних [redacted] 5/15/2025 Odessa National Polytechnic University (ІІБРТ, Каф. кібербезпеки та програмного забезпечення)	18 (2) 0.20 %
3	Парфьонов_Ярослав_КНТ4курс_Дипломб [redacted] 6/9/2024 Interregional Academy of Personnel Management (Інститут комп'ютерно-інформаційних технологій та дизайну)	16 (1) 0.18 %
4	ФКНТ_2024_122_ТроцькийЯВ [redacted] 11/20/2024 Ukrainian national aviation university (ФКНТ Кафедра комп'ютерних інформаційних технологій)	15 (2) 0.17 %
5	С 91_Вавровський_магістр [redacted] 11/26/2024 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ІС33І, Спецjальна кафедра №1)	14 (2) 0.16 %

Рисунок А.2 – Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ



6	Магістр групи КП-31мн Бабак Артем Андрійович [redacted] 5/9/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФПМ, К-ра програмного забезпечення комп'ютерних систем)	10 (1) 0.11 %

з Інтернету (0.53 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://metod.vntu.edu.ua/getfile.php/9821.pdf	30 (4) 0.33 %
2	https://elartu.tntu.edu.ua/bitstream/lib/48168/1/Master_Thesis__SBm-61_Hurskiy_V_B_2024.pdf	18 (2) 0.20 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

Рисунок А.3 – Звіт результатів перевірки на унікальність тексту в базі ХНУРЕ

ДОДАТОК Б
ВИХІДНИЙ КОД ДОДАТКУ

form.py

```
import tkinter as tk
from scrypt import calculate_encryption

TEXT_SIZE = 12
TEXT_FONT = "Arial"


def on_encrypt_click():
    data = input_text.get("1.0", tk.END).strip()
    result = calculate_encryption(data)
    show_labels()
    fill_results(result)


def show_labels():
    aes_label.grid(row=0, column=0, padx=50, pady=5, sticky="w")
    rsa_label.grid(row=0, column=1, padx=0, pady=5, sticky="w")
    present_label.grid(row=1, column=0, padx=50, pady=5, sticky="w")
    kyber_label.grid(row=1, column=1, padx=0, pady=5, sticky="w")
    aes_result_label.grid(row=0, column=0, padx=185, pady=5, sticky="w")
    rsa_result_label.grid(row=0, column=1, padx=100, pady=5, sticky="w")
    present_result_label.grid(row=1, column=0, padx=185, pady=5, sticky="w")
    kyber_result_label.grid(row=1, column=1, padx=100, pady=5, sticky="w")


def fill_results(result):
    aes_result_label.config(text=result.get("AES"))
    rsa_result_label.config(text=result.get("RSA"))
    present_result_label.config(text=result.get("PRESENT"))
    kyber_result_label.config(text=result.get("KYBER"))


root = tk.Tk()
root.title("Encryption Algorithm Benchmark")
root.geometry("700x300")

title_label = tk.Label(root, text="Encryption Algorithm Performance Test",
font=(TEXT_FONT, TEXT_SIZE))
title_label.pack(pady=10)

label = tk.Label(root, text="Enter the text you want to encrypt:", font=(TEXT_FONT,
TEXT_SIZE))
label.pack(anchor="w", padx=10, pady=5)

input_text = tk.Text(root, height=1, width=60, font=(TEXT_FONT, TEXT_SIZE))
input_text.pack(padx=10, pady=10)

encrypt_button = tk.Button(root, text="Encrypt", command=on_encrypt_click)
encrypt_button.pack(pady=10)

results_frame = tk.Frame(root)
results_frame.pack(padx=10, pady=10, fill="x")

aes_label = tk.Label(results_frame, text="AES result:", font=(TEXT_FONT, TEXT_SIZE))
```

```
rsa_label = tk.Label(results_frame, text="RSA result:", font=(TEXT_FONT, TEXT_SIZE))
present_label = tk.Label(results_frame, text="PRESENT result:", font=(TEXT_FONT,
TEXT_SIZE))
kyber_label = tk.Label(results_frame, text="Kyber result:", font=(TEXT_FONT,
TEXT_SIZE))
aes_result_label = tk.Label(results_frame, text="", font=(TEXT_FONT, TEXT_SIZE))
rsa_result_label = tk.Label(results_frame, text="", font=(TEXT_FONT, TEXT_SIZE))
present_result_label = tk.Label(results_frame, text="", font=(TEXT_FONT, TEXT_SIZE))
kyber_result_label = tk.Label(results_frame, text="", font=(TEXT_FONT, TEXT_SIZE))

root.mainloop()
```

scrypt.py

```
import time
import os
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding


def __format_time(seconds):
    if seconds >= 1:
        return f"{seconds:.3f} s"
    else:
        return f"{seconds * 1000:.3f} ms"


# AES (Symmetric Encryption)
def __aes_test(data):
    key = get_random_bytes(32)
    iv = get_random_bytes(AES.block_size)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    padded_plaintext = pad(data.encode(), AES.block_size)
    start = time.perf_counter()
    cipher.encrypt(padded_plaintext)
    end = time.perf_counter()
    return __format_time(end - start)


# RSA (Asymmetric Encryption)
def __rsa_test(data):
    private_key = rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048
    )
    public_key = private_key.public_key()
    start = time.perf_counter()
    public_key.encrypt(
        data.encode('utf-8'),
        padding.OAEP(
            mgf=padding.MGF1(algorithm=hashes.SHA256()),
            algorithm=hashes.SHA256(),
            label=None
        )
    )
    end = time.perf_counter()
    return __format_time(end - start)
```

```
# PRESENT (Lightweight Encryption)
def __present_test(data):
    key = os.urandom(10)
    cipher = Present(key)
    block_size = 8
    blocks = [data[i:i + block_size] for i in range(0, len(data), block_size)]
    start = time.perf_counter()
    for block in blocks:
        padded_block = block.ljust(block_size, b'\x00')
        cipher.encrypt(padded_block)
    end = time.perf_counter()
    return __format_time(end - start)


# CRYSTALS-Kyber (Post-Quantum Encryption)
def __kyber_test():
    public_key, _secret_key = generate_keypair()
    start = time.perf_counter()
    encrypt(public_key)
    end = time.perf_counter()
    return __format_time(end - start)


def calculate_encryption(data):
    return {
        "AES": __aes_test(data),
        "RSA": __rsa_test(data),
        "PRESENT": __present_test(data),
        "KYBER": __kyber_test()
    }


def main():
    data = "test data"
    results = {
        "AES (Symmetric)": __aes_test(data),
        "RSA (Asymmetric)": __rsa_test(data),
        "PRESENT (Lightweight)": __present_test(data),
        "CRYSTALS-Kyber (Post-Quantum)": __kyber_test()
    }

    print("\nEncryption Algorithm Performance:")
    for algo, timing in results.items():
        print(f"{algo}: {timing:.6f} seconds")
```

ДОДАТОК В

СЛАЙДИ ПРЕЗЕНТАЦІЇ

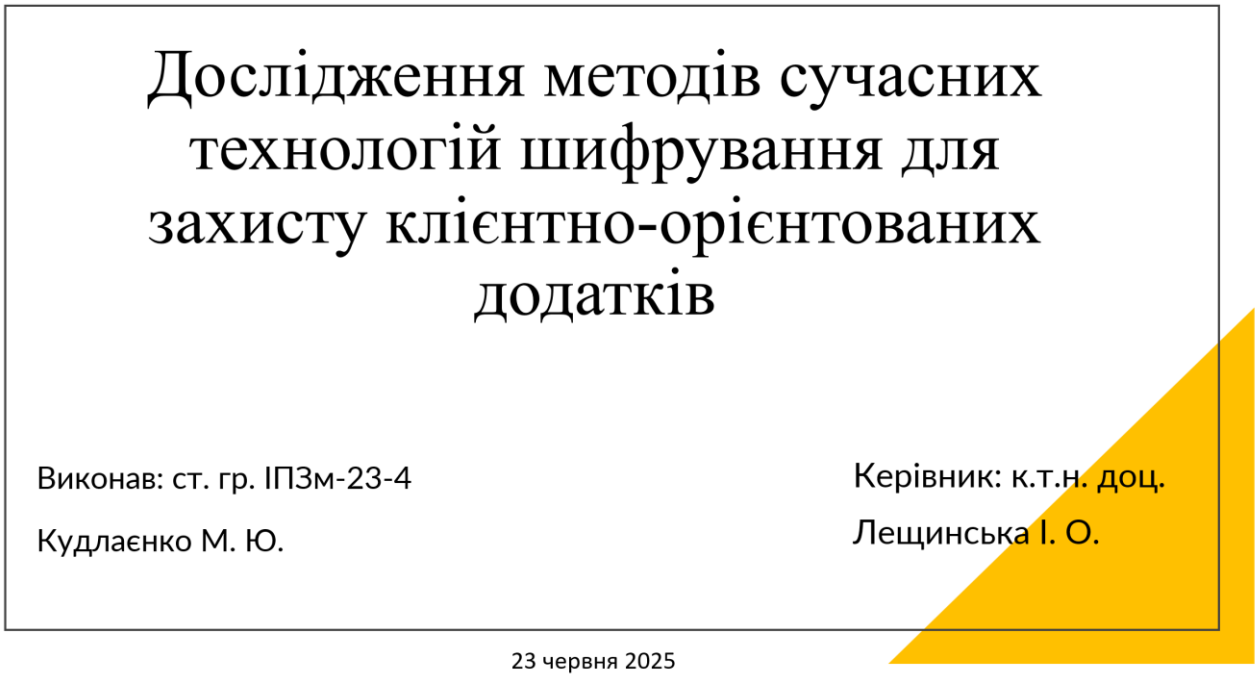


Рисунок В.1 – Перший слайд презентації

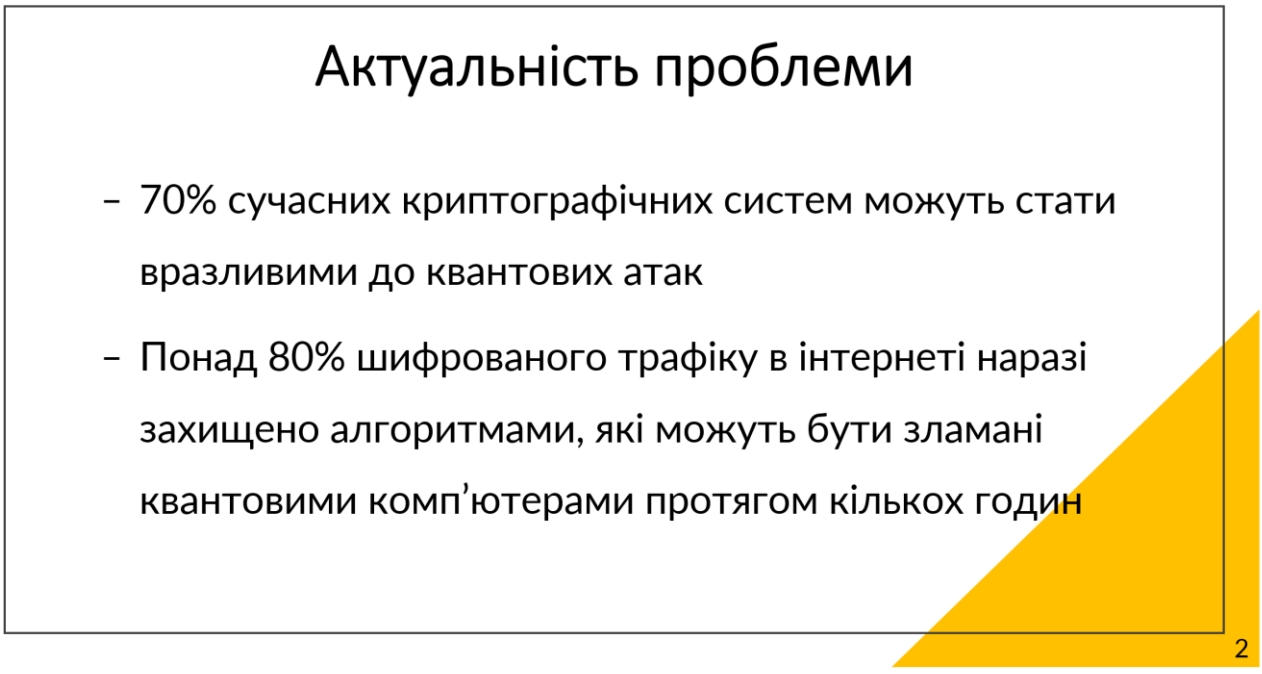


Рисунок В.2 – Другий слайд презентації

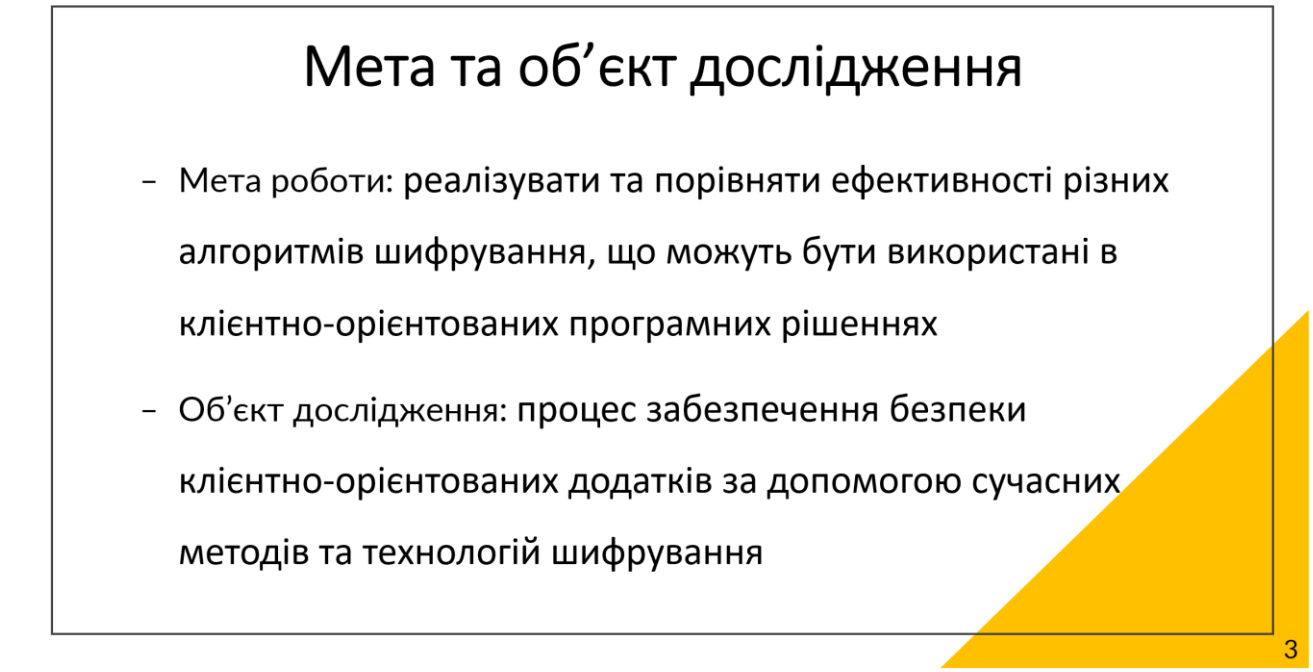


Рисунок В.3 – Третій слайд презентації

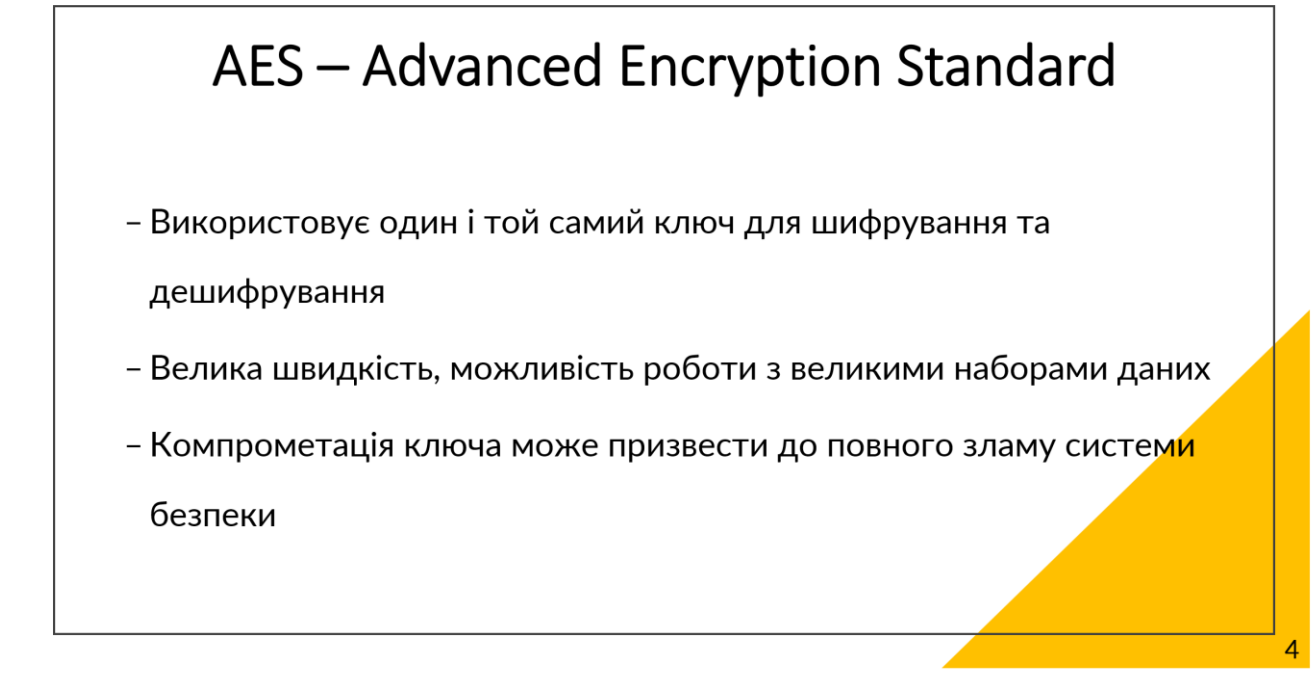


Рисунок В.4 – Четвертий слайд презентації

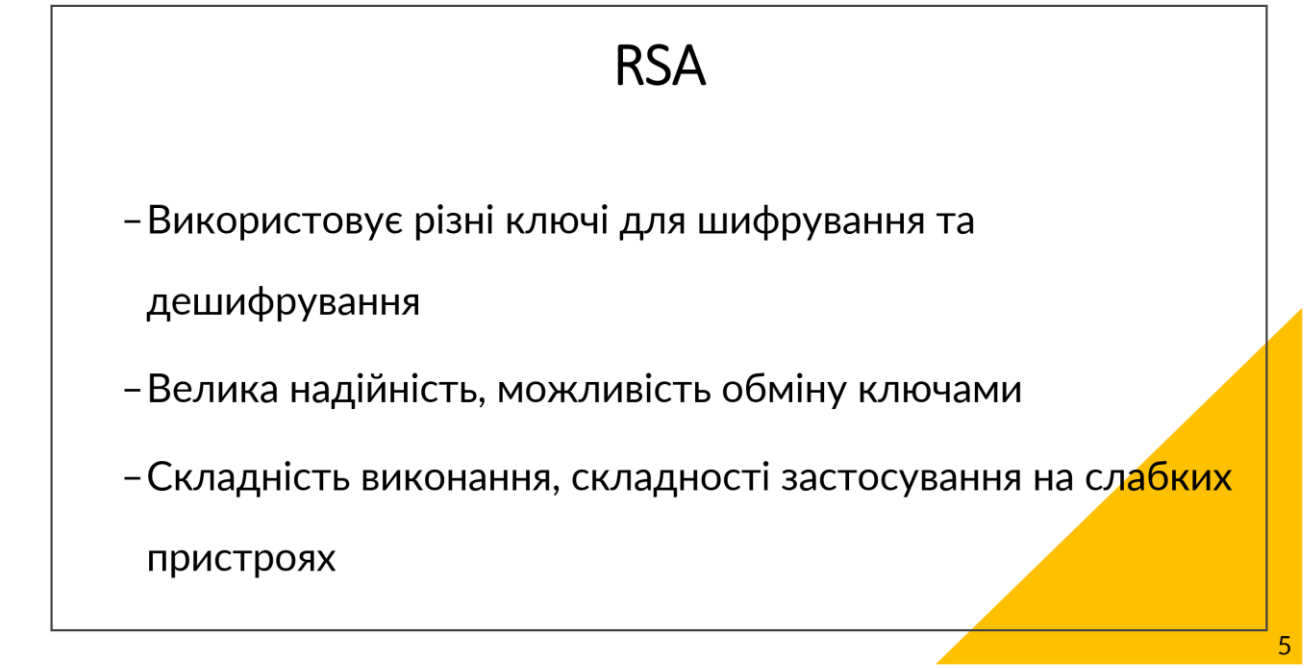


Рисунок В.5 – П’ятий слайд презентації

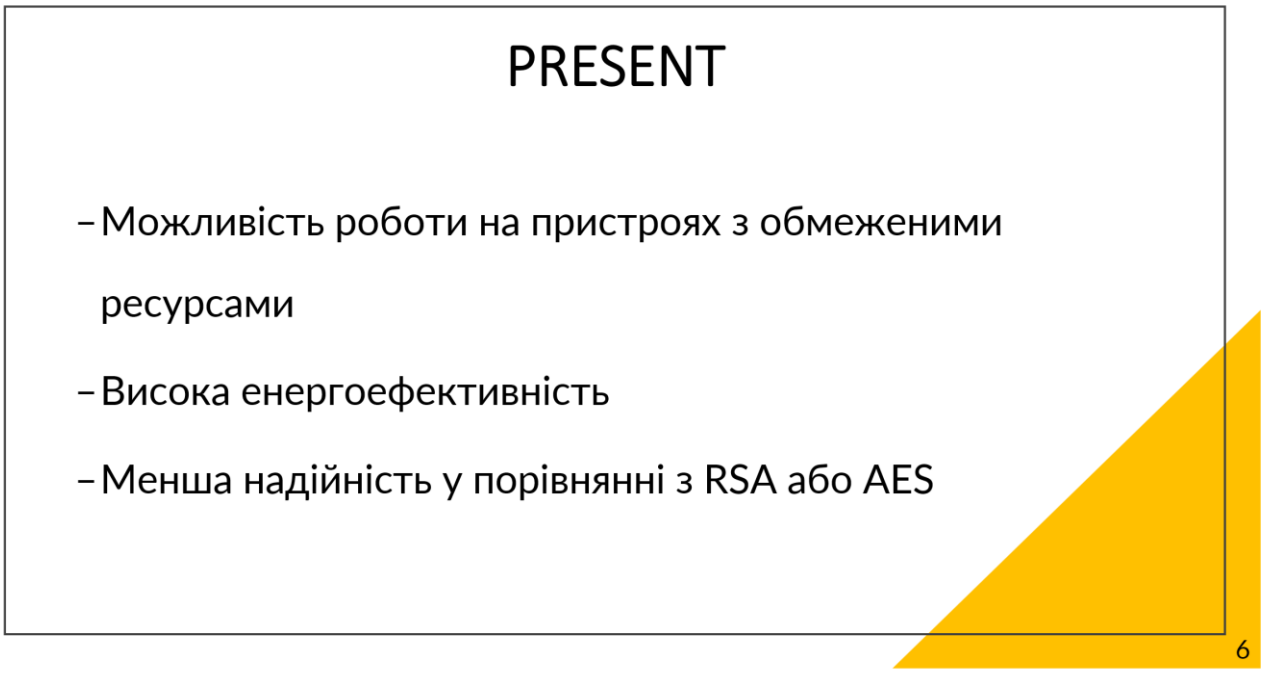


Рисунок В.6 – Шостий слайд презентації

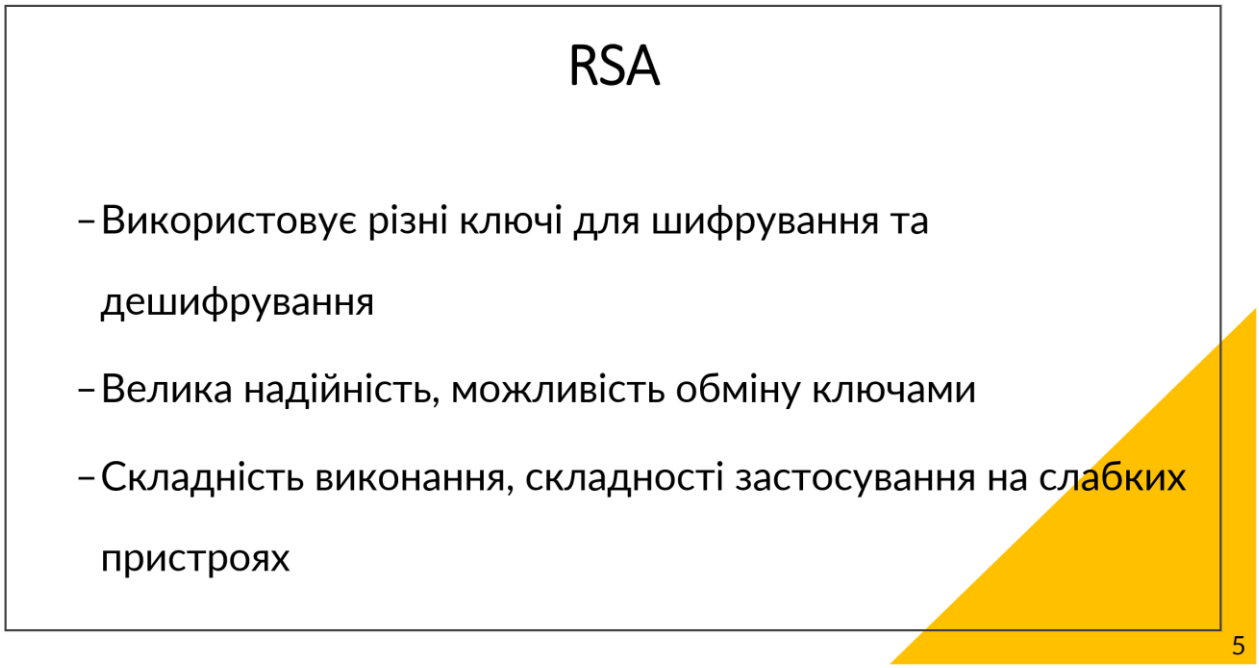


Рисунок В.7 – Сьомий слайд презентації

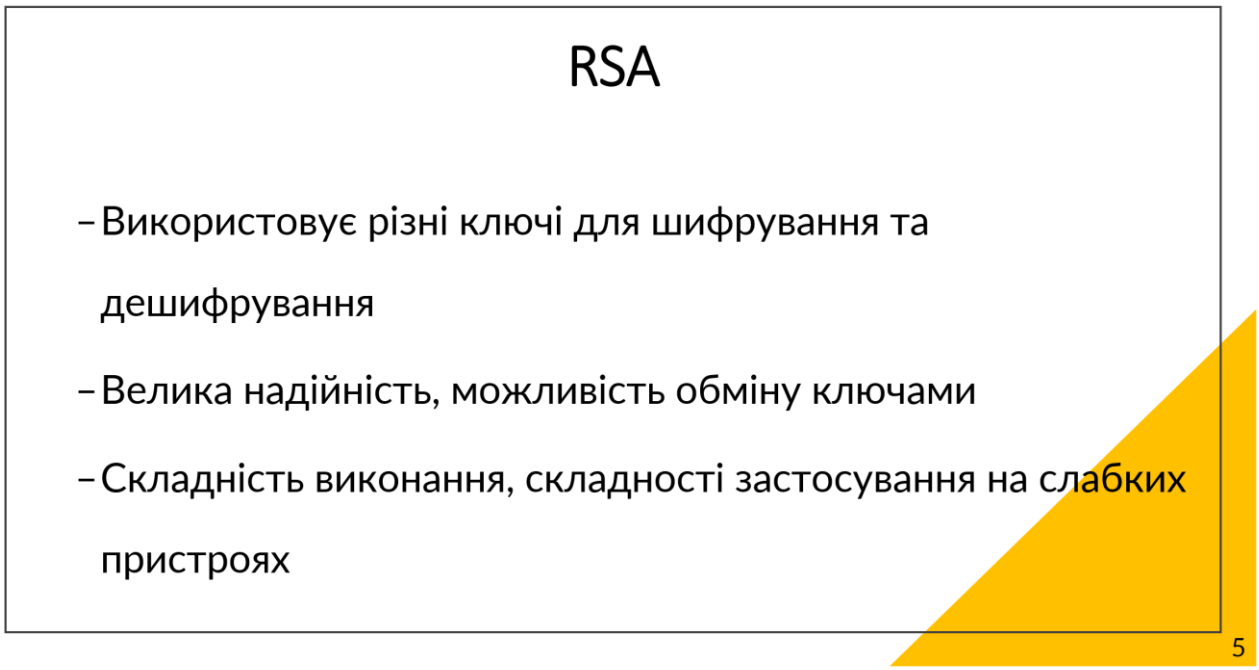


Рисунок В.8 – Восьмий слайд презентації

Порівняння алгоритмів шифрування

Критерій	AES (симетричний)	RSA (асиметричний)	PRESENT (легковагови й)	CRYSTALS-Kyber (квантостійкий)
Продуктивність	Висока	Низька	Висока	Середня
Енергоефективність	Висока	Низька	Висока	Середня
Стійкість до атак	Висока (традиційні атаки)	Висока (традиційні атаки)	Середня	Висока (включно з квантовими)
Сфера застосування	Великі обсяги даних	Автентифікація, передача ключів	IoT, мобільні пристрої	Квантова безпека, довгострокові дані

9

Рисунок В.9 – Дев’ятий слайд презентації

Експеримент з архівом

- Набори даних: архіви з текстовими файлами
- Суть експерименту: порівняння ефективності алгоритмів шифрування на різних розмірах архівів

10

Рисунок В.10 – Десятий слайд презентації

Результати експерименту

№	Розмір архіва	AES	RSA	PRESENT	CRYSTALS-Kyber
1	10 KB	0,012 мс	13 мс	0,7 мс	0,51 мс
2	100 KB	0,13 мс	0,13 с	7 мс	5,12 мс
3	1 MB	1,28 мс	1,31 с	1,01 мс	49 мс
4	10 MB	14 мс	18 с	0,7 с	0,526 с
5	100 MB	0,14 с	2 хв 23 с	6 с	4,0 с
6	1 GB	1,22 с	36 хв	54,5 с	54 с

11

Рисунок В.11 – Одинадцятий слайд презентації

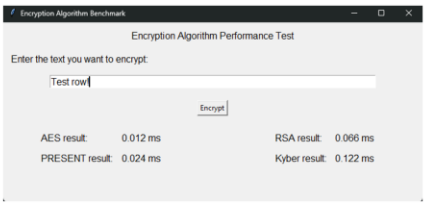
Експеримент зі строками

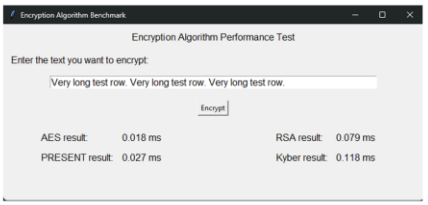
- Набори даних: дві строки довільного розміру
- Суть експерименту: порівняння часу виконання шифрування для строк різного розміру

12

Рисунок В.12 – Дванадцятий слайд презентації

Результати експерименту





13

Рисунок В.13 – Тринадцятий слайд презентації

Рекомендації використання алгоритмів

Сценарій використання	Рекомендований алгоритм	Обґрунтування
Шифрування великих обсягів даних у реальному часі	AES	Висока продуктивність та енергоефективність
Мобільні пристрої та IoT-системи	PRESENT	Низьке споживання ресурсів, висока швидкодія
Довгострокове зберігання конфіденційних даних	CRYSTALS-Kyber	Стійкість до квантових атак, довготривалий рівень безпеки
Автентифікація та обмін ключами	RSA/ECC	Надійність для забезпечення автентичності та безпечного обміну ключами

14

Рисунок В.14 – Чотирнадцятий слайд презентації

Рисунок В.15 – П’ятнадцятий слайд презентації

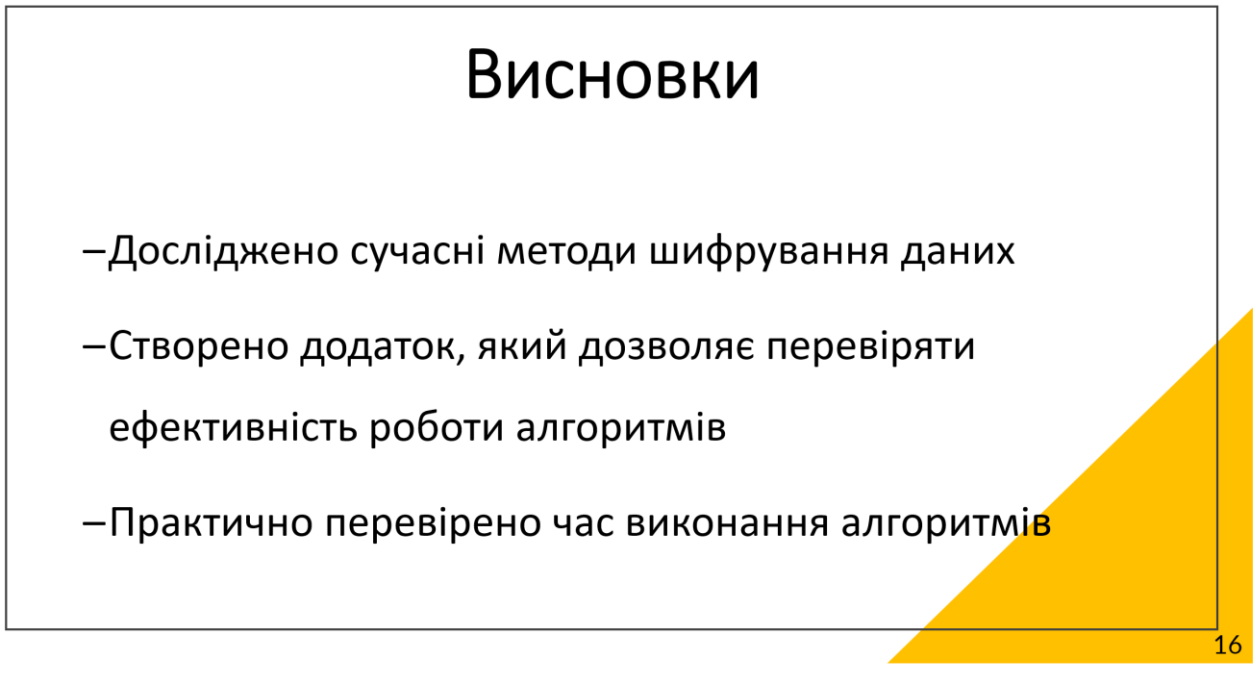


Рисунок В.16 – Шістнадцятий слайд презентації

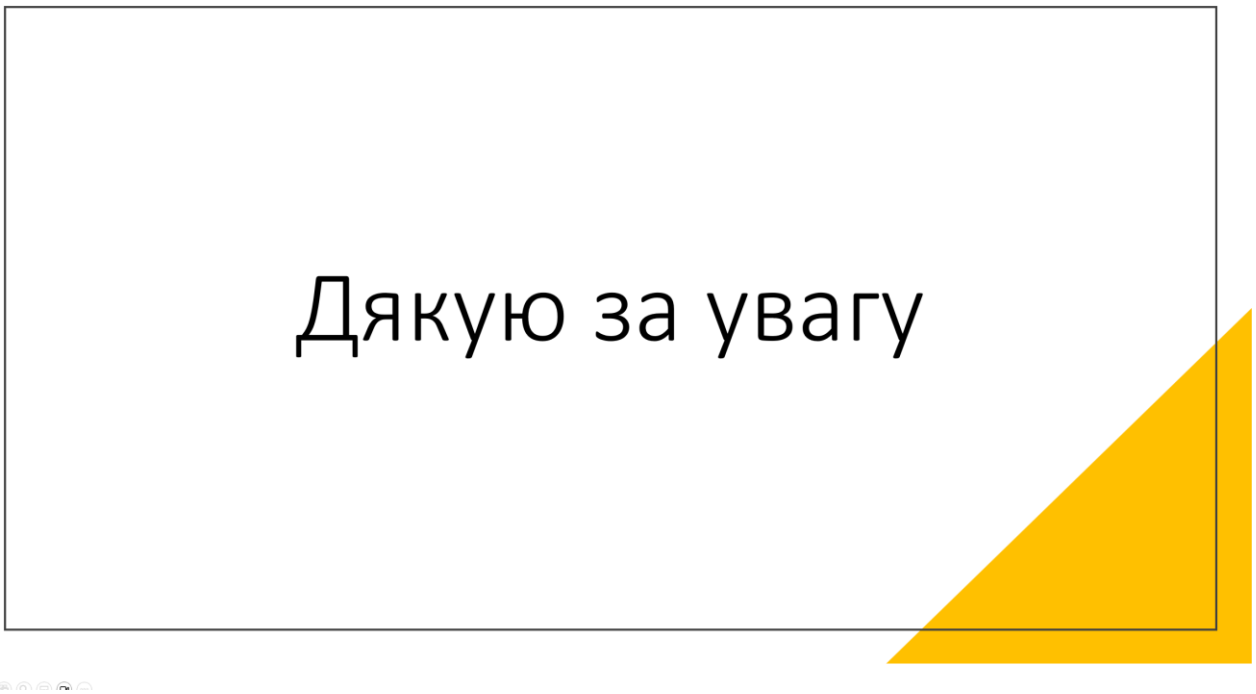
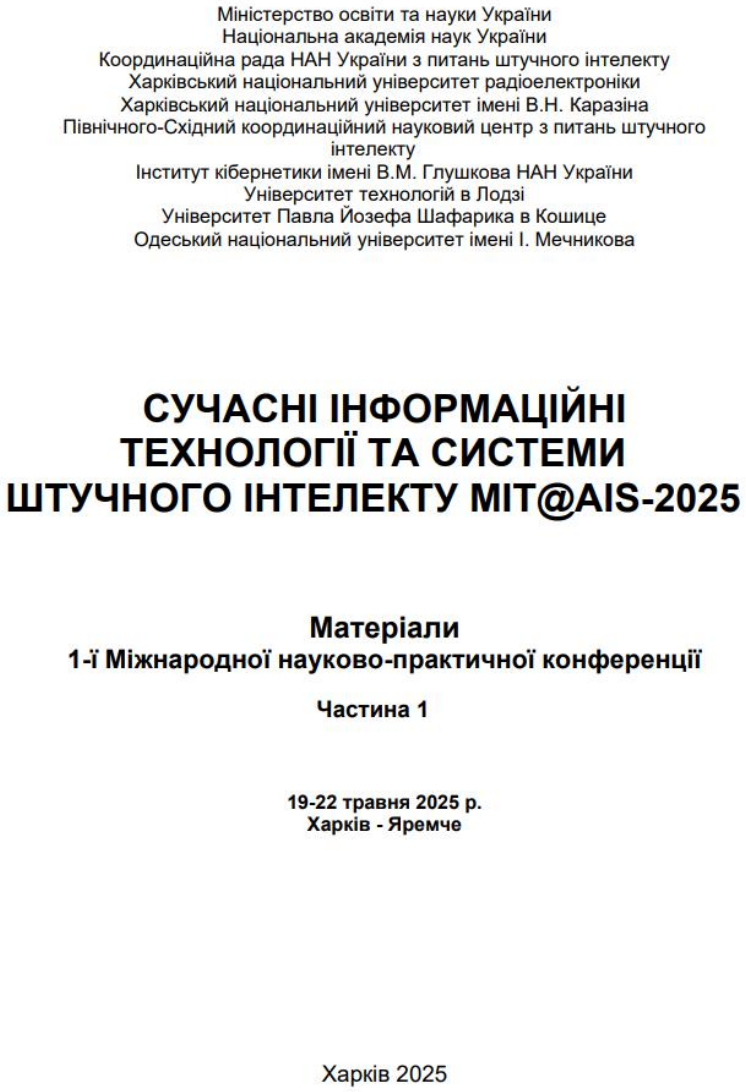


Рисунок В.17 – Сімнадцятий слайд презентації

ДОДАТОК Г
АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ



Міністерство освіти та науки України
Національна академія наук України
Координаційна рада НАН України з питань штучного інтелекту
Харківський національний університет радіоелектроніки
Харківський національний університет імені В.Н. Каразіна
Північного-Східний координаційний науковий центр з питань штучного інтелекту
Інститут кібернетики імені В.М. Глушкова НАН України
Університет технологій в Лодзі
Університет Павла Йозефа Шафарика в Кошице
Одеський національний університет імені І. Мечникова

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ MIT@AIS-2025

Матеріали
1-ї Міжнародної науково-практичної конференції

Частина 1

19-22 травня 2025 р.
Харків - Яремче

Харків 2025

Рисунок Г.1 – Перша сторінка збірника матеріалів до конференції «Сучасні інформаційні технології та системи штучного інтелекту»

Ministry of Education and Science of Ukraine
National Academy of Sciences of Ukraine
Coordination Council of NASU on Artificial Intelligence
Kharkiv National University of Radio Electronics
V.N. Karazin Kharkiv National University
North-Eastern Scientific Center on Artificial Intelligence
V.M. Glushkov Institute of Cybernetics, NAS of Ukraine
Lodz University of Technology
Pavol Jozef Šafárik University in Košice
I.I. Mechnikov Odesa National University

Modern Information Technologies and Artificial Intelligence Systems MIT@AIS-2025

Proceedings
of the 1st International Scientific and Practical Conference

Part 1

May 19-22, 2025
Kharkiv - Yaremche, Ukraine

Kharkiv 2025

Рисунок Г.2 – Друга сторінка збірника матеріалів до конференції «Сучасні інформаційні технології та системи штучного інтелекту»

Research on Modern Encryption Technologies for Protecting Client-Oriented Applications

Maksym Kudlaienko[a] and Iryna Leshchynska[a]

[a] *Kharkiv National University of Radio Electronics, Nauky Avenue 14, Kharkiv, 61166, Ukraine*

Abstract

In today's world, where information is a key resource, ensuring its confidentiality and security is of particular importance. The growth of data volumes, the expansion of cloud technologies, and the development of the internet create new challenges for protecting information from unauthorized access. Encryption technologies are among the most important tools in addressing these challenges, providing data protection by transforming it into a form unreadable without a special key. The relevance of this topic is driven by the rapid development of modern technologies, the emergence of new types of threats such as quantum computer attacks, and the need to strengthen the resilience of encryption algorithms. In this context, it is important to study modern approaches to data encryption, their strengths and weaknesses, as well as the possibilities for adapting them to new challenges. Additionally, there is an increasing need to develop effective encryption methods for specific fields, such as client-oriented applications.

Keywords

Encryption, Encryption methods, cybersecurity, AES, RSA, PRESENT, CRYSTALS-Kyber

1. Introduction

In the context of the rapid growth of data volumes, the widespread adoption of cloud computing, and the mass implementation of the Internet of Things, efficient encryption algorithms have become indispensable for protecting against malicious actors. For client-oriented applications, such as mobile apps or web services, the threat of data loss or compromise can have catastrophic consequences for end users and development companies. From banking transactions to the protection of personal data, encryption serves as a fundamental technology across all sectors.

Despite the effectiveness of modern encryption algorithms, they have several limitations. One of the main challenges is finding the optimal balance between security, performance, and energy efficiency. For example, algorithms that offer a high level of protection may be less suitable for devices with limited resources, such as mobile phones.

Additionally, the development of quantum computing poses a significant threat to traditional cryptographic methods. Quantum computers are expected to solve mathematical problems that underpin modern algorithms much faster, potentially rendering some classical algorithms vulnerable.

Modern cryptography is actively developing in several directions. First and foremost, this includes the development of quantum-resistant algorithms as a response to the threats posed by quantum computing. For example, the CRYSTALS-Kyber algorithm [1] is emerging as one of the most promising solutions in this field. At the same time, lightweight encryption algorithms are being developed for devices with limited resources, combining high efficiency with low energy consumption.

Another important trend is the integration of cryptography with client-oriented services, such as mobile applications or websites. This provides an additional level of security for processing and storing large volumes of data.

MIT@AIS'2025s: 1st International Scientific and Practical Conference "Modern Information Technologies and Artificial Intelligence Systems", May 19–22, 2025, Kharkiv-Yaremche, Ukraine
EMAIL: maksym.kudlaienko@nure.ua (A. 1); iryna.leshchynska@nure.ua (A. 2)
ORCID: 0009-0004-0492-6633 (A. 1); 0000-0002-8737-4595 (A. 2)

Рисунок Г.3 – Перша сторінка публікації

One of the key challenges is the need to adapt algorithms to different application scenarios. For client-oriented applications, energy efficiency is crucial, whereas for banking systems, security remains the top priority. Furthermore, the continuous updating of standards and regulatory requirements complicates the implementation of new solutions.

2. Existing Encryption Approaches

Modern encryption technologies can be divided into two main categories [2]: symmetric and asymmetric encryption.

Symmetric algorithms are characterized using the same key for both encryption and decryption of data. These algorithms offer high data processing speeds and efficiency, making them ideal for real-time tasks such as streaming data transmission or storing large volumes of information.

The primary challenge for symmetrical algorithms is ensuring the secure exchange of keys between parties. The loss or compromise of a key can lead to the breach of the entire system's security.

Asymmetric algorithms, on the other hand, use a pair of keys – a public key and a private key. They provide a high level of security due to complex mathematical operations that make unauthorized decryption significantly more difficult.

Asymmetric methods are ideally suited for encrypting digital signatures, authentication, and secure key exchanges. However, these algorithms are computationally intensive and require significant resources, which can be a limitation in certain scenarios, such as on low-power devices.

Thus, the choice between symmetric and asymmetric algorithms depends on the specifics of the task. For client-oriented applications, symmetric algorithms are suitable for fast real-time encryption of large amounts of data, while asymmetric algorithms provide reliable key exchange and a high level of security for critical applications such as e-commerce and the protection of confidential communications.

Hybrid encryption approaches [3] combine the strengths of both symmetric and asymmetric algorithms, providing both efficiency and a high level of security.

The main idea is that asymmetric encryption is used for secure key exchange, while symmetric encryption is employed for the actual data encryption.

For example, in SSL / TLS protocols, asymmetric algorithms are responsible for establishing the connection, after which a symmetric key is transmitted to encrypt the session data.

Hybrid methods are a standard in many modern systems, including cloud services and client-oriented applications, as they allow for an optimal balance between performance and security.

3. Encryption Integration Into The Client-Oriented Applications Architecture

In modern client-oriented applications, encryption is a crucial element of architecture. For example, mobile banking apps actively use symmetric AES algorithms to encrypt stored data and asymmetric RSA algorithms for secure key exchange between the client and server. Web applications, such as e-commerce platforms, use SSL/TLS protocols to protect data during transmission.

The use of encryption in modern systems significantly reduces the risks of data breaches, protects communications, and allows users to trust their data to apps and services. Integrating these solutions is an important step in enhancing the reliability and security of client-oriented applications.

Modern cryptographic methods, including lightweight and quantum-resistant algorithms, are increasingly being integrated into client-oriented apps to provide a balance between security, performance, and energy efficiency. Lightweight algorithms such as PRESENT are ideal for mobile devices and web apps, where resources are limited. They offer an adequate level of security with minimal energy consumption, which is critical for sensor networks and portable devices.

Quantum-resistant algorithms, such as CRYSTALS-Kyber and Dilithium, are applied in secure communications and cloud computing, as their design accounts for threats from quantum computers. The use of such methods ensures data confidentiality even in environments with high security requirements.

The integration of these methods into client-oriented applications allows for the adaptation of cryptographic solutions to specific use cases, ensuring a high level of data protection even in the most challenging conditions.

Рисунок Г.4 – Друга сторінка публікації

4. Analysis of Encryption Algorithms

To analyze encryption algorithms, it is necessary to consider their performance, energy efficiency, and resistance to attacks.

Criterion	AES (Symmetric)	RSA (Asymmetric)	PRESENT (Lightweight)	CRYSTALS-Kyber (Quantum-Resistant)
Performance	High	Low	High	Medium
Energy Efficiency	High	Low	High	Medium
Resistance to Attacks	High (traditional attacks)	High (traditional attacks)	Medium	High (including quantum attacks)
Application Area	Large volumes of data	Authentication, key exchange	IoT, mobile devices	Quantum security, long-term data

Figure 1: Comparison of encryption algorithms

From the figure it can be seen that AES is an ideal choice for encrypting large amounts of data due to its high performance and energy efficiency. In cases where authentication or secure key exchange is required, RSA provides a high level of protection, although it demands more resources. PRESENT is optimally suited for resource-constrained devices, such as the Internet of Things, due to its lightweight structure. Finally, CRYSTALS-Kyber is a promising choice for long-term data protection against quantum attacks, despite its relatively average performance.

A Python code was written to compare encryption algorithms, allowing the performance of different cryptographic algorithms to be evaluated. The implementation used popular libraries such as Crypto [4] for symmetric and asymmetric algorithms, pypresent for working with lightweight algorithms like PRESENT [5], and pqcrypto [6] for post-quantum algorithms, particularly CRYSTALS-Kyber. The choice of these libraries was driven by their convenience, wide support, and compliance with modern cryptographic standards.

```
Encryption Algorithm Performance:
AES (Symmetric): 0.000256 seconds
RSA (Asymmetric): 0.012438 seconds
PRESENT (Lightweight): 0.001798 seconds
CRYSTALS-Kyber (Post-Quantum): 0.004325 seconds

Process finished with exit code 0
```

Figure 2: Comparison results of encryption algorithms

5. Conclusion

Thus, the choice of algorithm depends on the specifics of its use. For real-time applications and large data, AES is the best option, while PRESENT is ideal for the web sector. For long-term protection,

Рисунок Г.5 – Третя сторінка публікації

CRYSTALS-Kyber is suitable, and for authentication and key exchange, RSA is the most appropriate. Each of these algorithms has its strengths and weaknesses, and their selection depends on the requirements of the specific task.

A well-informed choice of encryption algorithm not only enhances the efficiency and security of the system but also ensures its compliance with modern and future challenges in the field of information security.

6. References

[1] Udara P. CRYSTALS Kyber: The Key to Post-Quantum Encryption. URL: https://medium.com/@hwupathum/crystals-kyber-the-key-to-post-quantum-encryption-3154b305e7bd.

[2] Honcharnko D. Encryption: Types and Algorithms. What It Is, How It Differs, and Where It Is Used? URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

[3] EXBASE Comparison of Symmetric and Asymmetric Encryption. URL: https://exbase.io/uk/wiki/simetrichne-i-asimetrichne-shifruvannya.

[4] Python Cryptography Toolkit (pycrypto). URL: https://pypi.org/project/pycrypto/.

[5] Imdad M., Najwa S., Mahdin H. An Enhanced Key Schedule Algorithm of PRESENT-128 Block Cipher for Random and Non-Random Secret Keys. URL: https://www.mdpi.com/2073-8994/14/3/604.

[6] Post-Quantum Cryptography (PQCrypto). URL: https://pypi.org/project/pqcrypto/.

Рисунок Г.6 – Четверта сторінка публікації

Зміст Content

Рисунок Г.7 – Зміст збірника матеріалів до конференції «Сучасні інформаційні технології та системи штучного інтелекту»

ДОДАТОК Д

Експертний висновок результатів перевірки кваліфікаційної роботи на відповідність оформлення вимогам ДСТУ 3008: 2015

1

Експертний висновок результатів перевірки кваліфікаційної роботи

студент (посада) | програмної інженерії (кафедра) | ІПЗм-23-4 (група)

Кудлаєнко Максим Юрійович

(прізвище, ім'я, по батькові)

Зауваження

Пункт ДСТУ 3008-2015	Зміст пункту	Сторінка кваліфікаційної роботи
1	2	3
	7.1 Загальні положення	
	7.3 Нумерація сторінок звіту	
	7.4 Нумерація розділів, підрозділів, пунктів, підпунктів	
	7.5 Рисунки	
	7.6 Таблиці	
	7.7 Переліки	
	7.8 Примітки	
	7.9 Виноски	
	7.10 Формули та рівняння	
	7.11 Посилання	
	7.13 Список авторів	
	7.14 Скорочення та умовні позначки	
	7.15 Додатки	

зауважень немає

Експерт _____ (підпис) Олена ОЛІЙНИК (прізвище, ініціали)

18.06.2025