

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. І. Сікорського»

Кафедра інженерії програмного забезпечення в енергетиці

Практична робота № 4
з курсу: «*Безпека програмного забезпечення*»

Виконав:
студент 4-го курсу,
групи ТВ-21
Цвігун Богдан

Київ 2025

Практична робота № 4

Завдання:

1. Розробіть інтерфейс криптографічної системи для шифрування за допомогою DES з використанням всіх можливих режимів.
2. Ознайомтесь з описом класів CryptographicServiceProvider і CryptoStream бібліотеки .NET Framework.
3. Реалізуйте шифрування DES, використовуючи класи .NET Framework.
4. Виконайте тестування роботи системи.

Хід виконання:

Для розробки веб-додатку було використано фреймворк Flask, який забезпечує ефективну взаємодію між серверною частиною та інтерфейсом користувача. Інтерфейс реалізований з використанням сучасних веб-технологій, зокрема CSS-фреймворку Bulma, що надає адаптивний і естетичний дизайн, а також шаблонізатора Jinja2, який відповідає за динамічне формування вмісту HTML-сторінок.

The screenshot shows the 'DES Cipher' web application. At the top, there is a navigation bar with links for 'Головна', 'Про розробника', and 'Вихід'. On the right side of the header, there are language selection buttons for 'Підтримка EN / UA'. The main content area has a title 'DES Cipher' and a subtitle 'Шифрування/розшифрування з використанням DES (ECB/CBC/CFB/OFB)'. Below this, there is a 'Текст' input field with placeholder text 'Введіть або вставте текст...'. A note below it says: 'При шифруванні приймається звичайний текст. При розшифруванні — base64 рядок.' There are two input fields: 'Ключ (8 символів)' containing '8 символів (ASCII)' and 'IV (для CBC/CFB/OFB, 8 символів)' containing 'IV (8 символів)'. A note next to them says: 'Ключ і IV мають бути точно 8 байт (символів ASCII). Потрібно лише для режимів, відмінних від ECB.' Below these fields are buttons for 'Режим' (with 'ECB' selected), 'Шифрувати', and 'Розшифрувати'. To the right of the input fields is a 'Порядки та попередження' sidebar with a note about the security of DES and its recommendation to use AES instead. At the bottom of the sidebar, it says 'Розробник: ТВ-21 Цвітун Богдан' and 'DES — демонстраційний приклад симетричного шифрування'. The bottom of the page has a footer note: 'Шифрування повертає base64 рядок (щоб безпечно передавати дайкові дані). При розшифруванні подавайте base64 рядок.'

Шифр DES (Data Encryption Standard) є класичним алгоритмом симетричного блочного шифрування, розробленим у 1970-х роках компанією IBM та затвердженим Національним інститутом стандартів і технологій США (NIST) у 1977 році як федеральний стандарт. DES працює з блоками даних розміром 64 біти та використовує ключ довжиною 56 біт, за допомогою якого виконується послідовність із 16 раундів перестановок і підстановок.

Основний принцип DES полягає у поєднанні операцій заміни (S-box) та перестановки (P-box), що забезпечує як дифузію, так і плутанину — ключові властивості надійного шифрування.

Попри історичну важливість і довготривале використання у фінансових та урядових системах, DES нині вважається криптографічно застарілим, оскільки його ключ можна зламати за допомогою сучасних обчислювальних засобів методом повного перебору.

Для підвищення безпеки було створено модифікацію Triple DES (3DES), у якій алгоритм виконується тричі з різними ключами. Проте сьогодні для практичного використання рекомендується застосовувати сучасні стандарти, зокрема AES (Advanced Encryption Standard), який забезпечує значно вищий рівень криптостійкості.

```

116
117     @app.route("/des/", methods=["GET", "POST"])
118     def des_cipher():
119         result = None
120         error = None
121         formdata = {}
122
123         if request.method == "POST":
124             formdata = request.form.to_dict()
125             text = request.form.get("text", "")
126             key = request.form.get("key", "")
127             iv = request.form.get("iv", "")
128             mode = request.form.get("mode", "ECB")
129             action = request.form.get("action", "encrypt")
130
131             try:
132                 # перевірка ключа (рівно 8 байт)
133                 if len(key.encode()) != 8:
134                     raise ValueError("Ключ має бути рівно 8 символів (8 байт).")
135
136                 # Вибір режиму DES
137                 mode_map = {
138                     "ECB": DES.MODE_ECB,
139                     "CBC": DES.MODE_CBC,
140                     "CFB": DES.MODE_CFB,
141                     "OFB": DES.MODE_OFB
142                 }
143
144                 if mode not in mode_map:
145                     raise ValueError("Невідомий режим DES.")
146
147                 # Ініціалізація шифра
148                 if mode == "ECB":
149                     cipher = DES.new(key.encode(), mode_map[mode])
150                 else:
151                     if len(iv.encode()) != 8:

```

Повний вихідний код проєкту доступний у репозиторії, що буде додано до завдання.

DES Cipher

Шифрування/розшифрування з використанням DES (ECB/CBC/CFB/OFB)

Текст

Лорем Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,

При шифруванні приховатися звичайний текст. При розшифруванні — баз64 рядок.

Ключ (8 символів): AABBSSDD

ІВ (для CBC/CFB/OFB, 8 символів): IV (8 символов)

Ключ повинен бути рівно 8 байт.

Потрібно лише для режимів, відмінних від ECB.

Режим: ECB

Шифрувати | **Розшифрувати**

Результат

KD0125yAp/GKz18ZbaN8Jw0z1+0UYin08w0i2d7JQOrp7IT8s8HFgn8qyG2Wq2FPbY+p986rh/8ThB5JLInhpB2Pela25hYc+21

Додатково

Шифрування повертає base64 рядок (щоб безпечно передавати дайкові дані). При розшифруванні подавайте base64 рядок.

Ендпоінт /des/ реалізує веб-інтерфейс для симетричного блочного шифру DES (Data Encryption Standard) у межах Flask-застосунку. Його основне призначення полягає у забезпеченні взаємодії між користувачем і серверною частиною для виконання процесів шифрування та розшифрування тексту. Під час обробки запиту методом POST ендпоінт отримує з форми дані — вхідний

текст, ключ, ініціалізаційний вектор, режим роботи та обрану дію. Перед початком обчислень виконується перевірка коректності введених параметрів: ключ повинен містити рівно вісім байт, а ініціалізаційний вектор (IV), якщо він використовується, також має відповідати цій довжині.

Далі відбувається створення об'єкта шифра відповідно до вибраного режиму, серед яких підтримуються ECB, CBC, CFB та OFB. У режимі шифрування текст доповнюється до довжини, кратної розміру блоку, після чого шифрується і кодується у формат Base64 для коректного відображення в інтерфейсі. У режимі розшифрування виконується зворотна процедура — вхідні дані декодуються, розшифровуються та очищаються від заповнення.

Результат операції або повідомлення про можливі помилки передаються у шаблон DES.html, який відображає відповідну інформацію користувачеві. Така реалізація забезпечує зручну демонстрацію принципів роботи блочного симетричного шифру DES та дозволяє на практиці спостерігати відмінності між різними режимами його роботи.

The screenshot shows the DES Cipher web application. At the top, there is a navigation bar with links for 'DES Cipher', 'Головна', 'Про розробника', and 'Вихід'. On the right side of the header, there is a language switcher 'Підтримка EN / UA'. The main content area is titled 'DES Cipher' and describes it as 'Шифрування/розшифрування з використанням DES (ECB/CBC/CFB/OFB)'. The interface includes several input fields: 'Текст' (Text) containing placeholder text 'Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,'; 'Ключ (8 символів)' (Key) with value 'AAB855DD'; 'IV (для CBC/CFB/OFB, 8 символів)' (Initialization Vector) with value 'DDSS88AA'; and dropdown menus for 'Режим' (Mode) set to 'CFB', 'Шифрувати' (Encrypt), and 'Розшифрувати' (Decrypt). Below these are sections for 'Результат' (Result) showing the encrypted output in Base64 format: 'io9V4yaIzOwKFCuCd15QB96MxrlnpX0ck/bzka9sMHVMeST/E16JNew9Tm5/g8gQD9nGXZDhRaruvTR32vmC7n7bQOZv9ug#FF' and 'Додатково' (Additional) with the note 'Шифрування повертає base64 рядок (щоб безпечно передавати дійсні дані). При розшифруванні подавайте base64 рядок.' A sidebar on the right contains a section titled 'Поради та попередження' (Advice and Warnings) with text about the security of DES and recommendations for AES. At the bottom right, there is a credit 'Розробив: ТВ-21 Цигун Богдан' and a note 'DES — демонстраційний приклад симетричного шифрування'.

The screenshot shows the DES Cipher web application. At the top, there are navigation links: DES Cipher, Головна, Про розробника, Вихід, and Підтримка EN / UA. The main area contains several input fields and buttons:

- Текст:** A text input field containing a long string of characters: "i0%V4yslUCKFCuCdISQQB96MirImpXoov/bka9WWh/Me5T/E6iWew9Tm5/g8gQD9tGXEDhRwu/7R32mC7n7bQOzv9gfPf07/d7ZBlaUsdQX8i+vnWbgJF3kLElAGauD3hs6kfVAQAzIyB0wBT1WfIgztypvvgf5f/MKs0J/wcNa3/hofAVtb/HUjN/3z4Yig94cfPSW9Cd8g==".
- Ключ (8 символів):** An input field containing "AAB8SSDD".
- IV (для CBC/CFB/OFB, 8 символів):** An input field containing "DSSSBAA".
- Режим:** A dropdown menu set to "CFB".
- Шифрувати** and **Розшифрувати** buttons.
- Результат:** A text area showing the decrypted text: "Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,".
- Додатково:** A note stating: "Шифрування повертає base64 рядок (щоб безпечно передавати дані). При розшифруванні подавайте base64 рядок."
- Поради та попередження:** A box containing information about DES: "DES застарілий і небезпечний для реального використання — використовуйте AES для продуктивних рішень. Ключ і IV мають бути точно 8 байт (символів ASCII). Переконайтесь, що немає зліких проблем. Для CBC/CFB/OFB IV треба генерувати випадково й передавати/зберігати разом із шифротекстом."
- Розробка:** TB-21 Цілун Богдан.
- DES:** "DES — демонстраційний приклад симетричного шифрування"

Висновок:

У результаті виконання практичної роботи було створено веб-інтерфейс для симетричного блочного шифрування за допомогою алгоритму DES з підтримкою всіх основних режимів роботи (ECB, CBC, CFB, OFB). Розроблена система забезпечує коректну обробку ключів та ініціалізаційних векторів, виконує шифрування і розшифрування тексту та відображає результат користувачеві у зручному форматі. Реалізація на базі Flask і використання сучасних веб-технологій дозволяє продемонструвати принципи роботи DES у навчальних цілях, а також надає можливість тестування різних режимів шифрування та їхнього впливу на результат, забезпечуючи практичне розуміння роботи симетричних криптографічних алгоритмів.