**Лабораторна робота №1**

**Програмна реалізація шифрів DES, AES та ДСТУ 7624:2014**

*Мета роботи:* створити криптографічну систему шифрування даних, яка базується на алгоритмах шифрування DES,AES та ДСТУ 7624:2014.

**Завдання до роботи**

Програмна реалізація криптографічної системи, ґрунтованої на алгоритмах шифрування DES,AES та ДСТУ 7624:2014, має бути оформлена як деяка програмна оболонка. У програмній реалізації має бути розроблений інтерфейс, зручний для експлуатації програми, в інтерфейсі слід передбачити:

* два режими формування ключа - ключ заданий, ключ формується за умовчанням;
* введення початкової інформації з сформованого заздалегідь файлу і з файлу, який створюється в оболонці програми;
* режими шифрування, які передбачені в DES,AES та ДСТУ 7624:2014 (ECB, CBC, PCBC, CFB, OFB);

• режими шифрування і дешифрування інформації.

Підготувати звіт по роботі. У звіті описати алгоритми DES,AES та ДСТУ 7624:2014 та режими їх роботи, описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій. У звіт включити опис алгоритму генерації ключа, деталі програмної реалізації, які представляють інтерес з точки зору розробника.

Контрольні запитання

1. По якому принципу побудовані шифри *DES,*AES та *ДСТУ 7624:2014*?
2. Який шифри передували шифрам *DES,*AES та *ДСТУ 7624:2014*?
3. Вказати довжину початкового ключа в алгоритмах *DES,**AES* та *ДСТУ 7624:2014*. Вказати основні етапи формування ключів в алгоритмах *DES,*AES та *ДСТУ 7624:2014*.
4. Скільки раундів в алгоритмах *DES,*AES та *ДСТУ 7624:2014*?
5. Скільки ключів формується в алгоритмах *DES,*AES та *ДСТУ 7624:2014* для шифрування тексту?
6. Вказати довжину ключа при шифруванні тексту в алгоритмах *DES,*AES та *ДСТУ 7624:2014*.
7. Які арифметичні операції використовуються при перетвореннях в алгоритмах *DES,*AES та *ДСТУ 7624:2014?*.
8. Вкажіть довжину шифрованого блоку в алгоритмах *DES,*AES та *ДСТУ 7624:2014*.
9. Порівняйте криптостійкість алгоритмів і вкажіть їх основні переваги і недоліки.