Лабораторна робота №1.

Симетричне шифрування. Алгоритм AES.

Мета.

Дослідити принципи роботи симетричного шифрування на прикладі алгоритму AES.

Завдання.

Реалізувати алгоритм симетричного шифрування AES (будь-якої версії - 128 або 256).

Довести коректність роботи реалізованого алгоритму шляхом порівняння результатів з існуючими реалізаціями (напр. сайтом-утилітою https://cryptii.com).

Виконання.

AEC це специфікація для шифрування електронних даних, створена Національним інститутом стандартів та технологій США (NIST) у 2001 році. Двигун AES вимагає простого тексту та секретного ключа для шифрування, і той же секретний ключ потрібен для його повторного розшифрування.

Вхідні дані можуть бути 128-бітними або 192-бітними або 256-бітними, і генерується відповідний біт шифрованого тексту.

Метод шифрування вихідного тексту.

```
public static String encrypt(String secretKey, String plainText){
  SecretKeySpec key = new SecretKeySpec(secretKey.getBytes("UTF-8"), "AES");
  Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
  cipher.init(Cipher.ENCRYPT_MODE, key);

  return new String(Hex.encodeHex(cipher.doFinal(plainText.getBytes("UTF-8")), false));
}
```

Метод дешифрування зашифрованого тексту.

```
public static String decrypt(String secretKey, String cipherText){
  SecretKeySpec key = new SecretKeySpec(secretKey.getBytes("UTF-8"), "AES");
  Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
  cipher.init(Cipher.DECRYPT_MODE, key);

  return new String(cipher.doFinal(Hex.decodeHex(cipherText.toCharArray())));
}
```

Процес шифрування та дешифрування.

```
public static void main(String[] args) {
  String secretKey = "secretsecretsecr";
  String plainText = "Hello, world!";
  String encryptedText;
  System.out.println("Encripted text: " + (encryptedText = AesCipher.encrypt(secretKey, plainText)));
  System.out.println("Decrypted text: " + AesCipher.decrypt(secretKey, encryptedText));
}
```

Результати роботи програми.

```
Encripted text: 066DA0EB61D3444750AF130BE9388401
Decrypted text: Hello, world!
```

Висновки.

Дослідили принципи роботи симетричного шифрування на прикладі алгоритму AES.