链滴

AES 加密 / 解密 - 工具类

作者：hanzanr123
原文链接：https://ld246.com/article/1553851834466
来源网站：链滴

```java
import java.security.NoSuchAlgorithmException;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.spec.SecretKeySpec;

/**
 * AES工具类
 *
 * @author think
 *
 */
public class AESUtil {
public static final String KEY_ALGORITHM = "AES";

/**
 * 自动生成AES密钥
 *
 * @param digit
 *          :二进制位数 128,256等
 */
public static String getKey(int digit) {
    try {
        KeyGenerator kg = KeyGenerator.getInstance(KEY_ALGORITHM);
        kg.init(digit);// 要生成多少位，只需要修改这里即可128, 192或256
        SecretKey sk = kg.generateKey();
        byte[] b = sk.getEncoded();
        return byteToHexString(b);
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
        System.out.println("没有此算法。");
    }
    return null;
}

/**
 * 二进制byte[]转十六进制string
 */
public static String byteToHexString(byte[] bytes) {
    StringBuffer sb = new StringBuffer();
    for (int i = 0; i < bytes.length; i++) {
        String strHex = Integer.toHexString(bytes[i]);
        if (strHex.length() > 3) {
            sb.append(strHex.substring(6));
        } else {
            if (strHex.length() < 2) {
                sb.append("0" + strHex);
            } else {
                sb.append(strHex);
            }
        }
    }
    return sb.toString();
```

```
}

/**
 * 十六进制string转二进制byte[]
 */
public static byte[] hexStringToByte(String s) {
    byte[] baKeyword = new byte[s.length() / 2];
    for (int i = 0; i < baKeyword.length; i++) {
        try {
            baKeyword[i] = (byte) (0xff & Integer.parseInt(s.substring(i * 2, i * 2 + 2), 16));
        } catch (Exception e) {
            System.out.println("十六进制转byte发生错误！！！");
            e.printStackTrace();
        }
    }
    return baKeyword;
}

/**
 * 使用对称密钥进行加密
 *
 * @param data
 * @param keys
 * @return
 * @throws Exception
 */
public static String encryption(String data, String keys) throws Exception {
    byte[] keyb = hexStringToByte(keys);
    SecretKeySpec sKeySpec = new SecretKeySpec(keyb, KEY_ALGORITHM);
    Cipher cipher = Cipher.getInstance(KEY_ALGORITHM);
    cipher.init(Cipher.ENCRYPT_MODE, sKeySpec);
    byte[] bjiamihou = cipher.doFinal(data.getBytes());
    return byteToHexString(bjiamihou);
}

/**
 * 使用对称密钥进行解密
 *
 * @param encryptedStr
 * @param keys
 * @return
 * @throws Exception
 */
public static String decrypt(String encryptedStr, String keys) throws Exception {
    byte[] keyb = hexStringToByte(keys);
    byte[] miwen = hexStringToByte(encryptedStr);
    SecretKeySpec sKeySpec = new SecretKeySpec(keyb, KEY_ALGORITHM);
    Cipher cipher = Cipher.getInstance(KEY_ALGORITHM);
    cipher.init(Cipher.DECRYPT_MODE, sKeySpec);
    byte[] bjiemihou = cipher.doFinal(miwen);
    return new String(bjiemihou);
}

public static void main(String[] args) throws Exception {
```

```
    System.out.println(getKey(256));
}

}
```

原文链接：AES 加密 / 解密 - 工具类