链滴

对于 3DES 的理解

作者：manyue
原文链接：https://ld246.com/article/1503577066416
来源网站：链滴

文一：DES

概述

IBM公司于1975年研究成功并公开发表，1977年1月，美国政府颁布：采纳IBM公司设计的方案作为机密数据的正式数据加密标准（Data Encryption Standard)。

参数	长度	说明
key	8byte(64bit)	des算法的工作密钥
data	8byte(64bit)	要被加密或被解密的数据
Mode	--	des算法的工作方式[加密/解密]

JAVA中的实现

Cipher类为加密和解密提供密码功能。它构成了 Java Cryptographic Extension (JCE) 框架的核心。

为创建 Cipher 对象，应用程序调用 Cipher 的 getInstance 方法并将所请求转换 的名称传递给它。可以指定提供者的名称（可选）。

转换 是一个字符串，它描述为产生某种输出而在给定的输入上执行的操作（或一组操作）。转换始终括加密算法的名称（例如，DES），后面可能跟有一个反馈模式和填充方案。

转换具有以下形式：

“算法/模式/填充”或“算法”（后一种情况下，使用模式和填充方案特定于提供者的默认值）。例，以下是有效的转换：

```
Cipher c = Cipher.getInstance("DES/CBC/PKCS5Padding");
```

文二：3DES/Triple DES/DESede

概述

3DES（或称为Triple DES）是三重数据加密算法（TDEA，Triple Data Encryption Algorithm）块码的通称。它相当于是对每个数据块应用三次DES加密算法。由于计算机运算能力的增强，原版DES码的密钥长度变得容易被暴力破解；3DES即是设计用来提供一种相对简单的方法，即通过增加DES的钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。

算法原理

使用3条56位的密钥对 数据进行三次加密。3DES（即Triple DES）是DES向AES过渡的加密算法（199年，NIST将3-DES指定为过渡的加密标准）。

其具体实现如下：设Ek()和Dk()代表DES算法的加密和解密过程，K代表DES算法使用的密钥，P代表文，C代表密文，这样：

3DES加密过程为：C=Ek3(Dk2(Ek1(P)))

3DES解密过程为：P=Dk1(EK2(Dk3(C)))

原文链接：对于 3DES 的理解

猜测Java中给3DES取名为DESede的原因或许是因为算法原理是e d e

JAVA中的实现

```
Cipher c = Cipher.getInstance("DES/CBC/PKCS5Padding");
Cipher cipher = Cipher.getInstance(DESede);
```