接下来我们分析 DH 加密算法，一种适基于密钥一致协议的加密算法。

DH

Diffie-Hellman 算法(D-H 算法)，密钥一致协议。是由公开密钥密码体制的奠基人 Diffie 和 Hellman 所提出的一种思想。简单的说就是允许两名用户在公开媒体上交换信息以生成"一致"的、可以共享的密钥。换句话说，就是由甲方产出一对密钥（公钥、私钥），乙方依照甲方公钥产生乙方密钥对（公钥、私钥）。以此为基线，作为数据传输保密基础，同时双方使用同一种对称加密算法构建本地密钥（SecretKey）对数据加密。这样，在互通了本地密钥（SecretKey）算法后，甲乙双方公开自己的公钥，使用对方的公钥和刚才产生的私钥加密数据，同时可以使用对方的公钥和自己的私钥对数据解密。不单单是甲乙双方两方，可以扩展为多方共享数据通讯，这样就完成了网络交互数据的安全通讯！该算法源于中国的同余定理——中国馀数定理。

流程分析：

1.甲方构建密钥对儿，将公钥公布给乙方，将私钥保留；双方约定数据加密算法；乙方通过甲方公钥构建密钥对儿，将公钥公布给甲方，将私钥保留。
2.甲方使用私钥、乙方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥加密数据，发送给乙方加密后的数据；乙方使用私钥、甲方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥对数据解密。
3.乙方使用私钥、甲方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥加密数据，发送给甲方加密后的数据；甲方使用私钥、乙方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥对数据解密。

通过 a a 代码实现如下：

Java 代码

```
1  import java.security.Key;
2  import java.security.KeyFactory;
3  import java.security.KeyPair;
4  import java.security.KeyPairGenerator;
5  import java.security.PublicKey;
6  import java.security.spec.PKCS8EncodedKeySpec;
7  import java.security.spec.X509EncodedKeySpec;
8  import java.util.HashMap;
```

```
9  import java.util.Map;
10
11 import javax.crypto.Cipher;
12 import javax.crypto.KeyAgreement;
13 import javax.crypto.SecretKey;
14 import javax.crypto.interfaces.DHPrivateKey;
15 import javax.crypto.interfaces.DHPublicKey;
16 import javax.crypto.spec.DHParameterSpec;
17
18 /**
19  * DH 安全编码组件
20  *
21  * @author 梁栋
22  * @version 1.0
23  * @since 1.0
24  */
25 public abstract class DHCoder extends Coder {
26     public static final String ALGORITHM = "DH";
27
28     /**
29      * 默认密钥字节数
30      *
```

```
31          *     lt;pre    gt;
32          * DH
33          * Default Keysize 1024
34          * Keysize must be a multiple of 64, ranging from 512 to 1024 (inclusive).
35          *     lt;/pre    gt;
36          */
37         private static final int KEY_SIZE = 1024;
38
39          /**
40           * DH 加密下需要一种对称加密算法对数据加密，这里我们使用 DES，也可以使用其他对称加密算法。
41           */
42         public static final String SECRET_ALGORITHM = "DES";
43         private static final String PUBLIC_KEY = "DHPublicKey";
44         private static final String PRIVATE_KEY = "DHPrivateKey";
45
46         /**
47          * 初始化甲方密钥
48          *
49          * @return
50          * @throws Exception
51          */
52         public static Map    lt;String, Object    gt; initKey() throws Exception {
```

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/728133034140006063