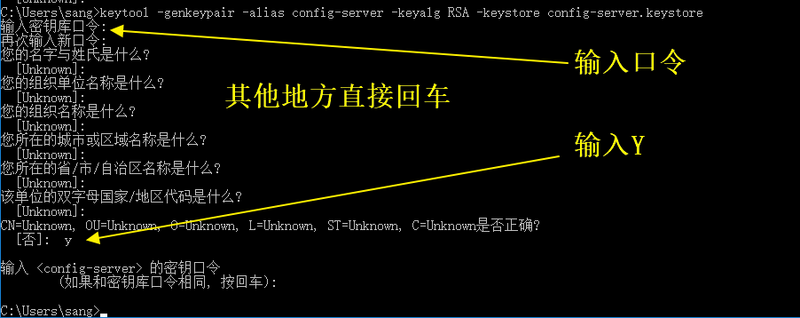
# 非对称加解密

使用非对称加解密的方式，我们的安全性将会得到进一步的提高。使用非对称加密的话需要我们先生成密钥对，生成密钥对可以直接使用jdk中自带的keytool工具，方式如下：

keytool -genkeypair -**alias** **config**-server -keyalg RSA -keystore **config**-server.keystore

执行效果如图：



执行成功之后，会在命令执行目录下生成一个名为config-server.keystore的文件

修改config-server的application.yml文件 添加如下配置：

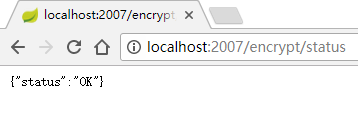
**encrypt:  
 key-store:**

**//**config-server.keystore文件的位置 **location:** file:C:/Users/ASUS/Desktop/UnlimitedJCEPolicyJDK8/config-server.keystore //  
 **alias:** config-server

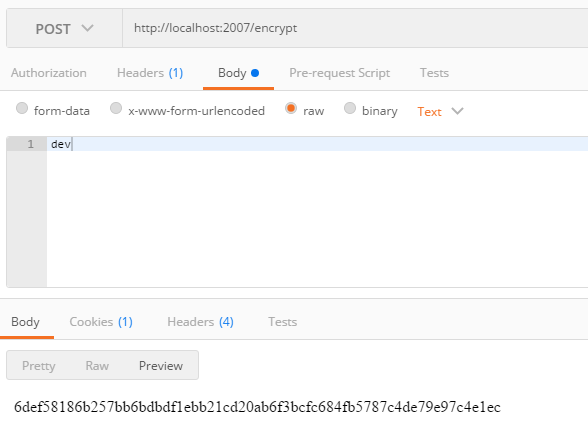
//生成config-server.keystore文件时指定的密码  
 **password:** 123456

//生成config-server.keystore文件时指定的密码  
 **secret:** 123456

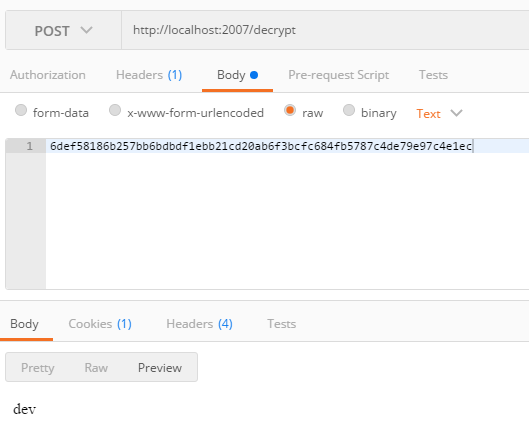
配置完成之后，启动我们的config-server工程，然后访问如下地址[http://localhost](http://localhost/" \t "_blank):8055/encrypt/status，如果看到如下访问结果，表示环境搭建成功了：



此时我们就可以通过第三方工具如POSTMAN、RestClient等来访问/encrypt和/decrypt接口，比如说我要给dev这个字符加密，方式如下(我这里以POSTMAN为例，注意是POST请求)：



解密方式如下：



git上的配置文件的值如果是以{cipher}开头，表示该值是一个加密字符，配置中心config-server在获取到这个值之后会先对值进行解密，解密之后才会返回给客户端使用。

所以我们可以git上的需要加密的字段如下所示标注即可

