## Plan

1. 加密算法测试
2. 对称加密密钥生成算法

———————————————————————————————————————

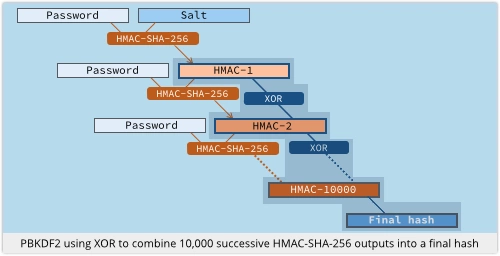
## 1、基于口令的秘钥生成算法（PBKDF2算法）

**1.1 PBKDF2（Password-Based Key Derivation Function）**

算法过程：



迭代描述：



相关链接：

算法描述：<https://segmentfault.com/a/1190000004261009>

Python库：<https://www.dlitz.net/software/python-pbkdf2/>

使用协商好的salt值，得到相同的秘钥（c=1000, dkLen=256 bit）。

**1.2 共享密钥**

（1）TGS-Cloud共享密钥：

b'\x87\xe9\x11\xfe\x82\xce\x8dS\x08;9\xd2\xbfx\x03\x95\x15\x99\xc2\x02\x9c\xcb\xaa\xd7G\x16\xd8\xae\x157U\xdb'

**seed**：kerberos\_hadoop@401

（2）AS-TGS共享密钥：

b'\xce\xea\x9c\x13yy\xcf\xe9\xe0\x19|\xe7\x99\xb4h\xdc\xc5\x1f\xd7\x99\x9b\xbc\xfe>\xc1r#\xfcP\x9a\x11~'

**seed**：AS\_TGS@401

## 2、加密算法测试

**2.1 AES加密**

细节：

1. 加密模式：CBC（也可以使用其他的模式）
2. 填充方式：PKCS7padding (16的倍数)
3. 偏移量（iv）：16byte，取key的前16byte
4. 密钥（key）：32byte
5. 输出结果：base64编码

相关链接：

官方文档：<https://pycryptodome.readthedocs.io/en/latest/src/cipher/classic.html#cbc-mode>

简单示例：<https://www.jianshu.com/p/5d27888e7c93>

* 1. **3DES加密**

细节：

1. 加密模式：CBC（也可以使用其他的模式）
2. 填充方式：PKCS7padding (8的倍数)
3. 偏移量（iv）：16byte，取key的前16byte
4. 密钥（k1,k2,k3）：k1=k3\=k2，key的长度为24byte
5. 输出结果：base64编码

相关链接：

官方文档：<https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html>