|  |  |  |
| --- | --- | --- |
| 参数符号 | 参数含义 | 备注 |
|  | 一个素数 | 公开 |
|  | 有限域的一个生成元 | 公开 |
|  | 加密密钥 | 公开 |
|  | 脱密密钥 | 保密 |
|  | 明文空间 |  |
|  | 密文空间 |  |
|  | 加密算法 |  |
|  | 脱密算法 |  |

（1）选取大素数，使离散对数问题在有限域上难解；

选取作为生成元。

（2）随机选取,计算.其中为脱密密钥，为加密密钥。

加密：

对任意明文，秘密随机选取一个整数，;

计算,得到密文.