实验原理

ELGamal密码体制是T.ElGamal在1985年提出的公钥密码体制。它的安全性是基于求解离散对数问题的困难性，是RSA以后比较有希望的一个公钥密码。美国的DSS(Digital Signature Standard)的DSA(Digital Signature Algorithm)算法就是经ElGamal算法演变而来。目前DSA算法应用也非常广泛。

1．公钥的生成算法

系统提供一个大素数p和GF(p)上的本原元素g。对每一个用户A可选择

$X_A \in [0, 1, 2, \cdots\cdots, p-1]$

计算$Y_A = g^{XA} \bmod p$

其中，X_A就是用户的私钥，Y_A就成为用户的公钥，将Y_A公开，X_A保密，由A自己掌握。

2．加密算法

若A欲与B保密通信，设明文是m，$m \in [0, 1, 2, \cdots\cdots, p-1]$则可按如下步骤进行：

（1）A找出B的公钥$Y_B = g^{XB} \bmod p$

（2）A任意选随机数$x \in [0, 1, 2, \cdots\cdots, p-1]$，A计算$C_1 = (g)^x \bmod p$

（3）A计算：$K = (Y_B)^x \bmod p = (g^X)^{XB} \bmod p$，求$C_2 = (K*m) \bmod p$

（4）A将（C_1，C_2）作为密文发送给B

3．解密算法

B收到密文以后解密方法如下：

（1）B用自己的密钥X_B计算：$K = (Y_B)^x \bmod p = (g^X)^{XB} \bmod p = (C_1)^{XB} \bmod p$

（2）B计算：$K^{-1} \bmod p$

（3）求$m = (K^{-1}*C_2) \bmod p$

举例说明如下：

设p = 11，g = 7，在GF（11）上有$7^0=1$，$7^1=7$，$7^2=5$，$7^3=2$，$7^4=3$，$7^5=10$，$7^6=4$，$7^7=6$，$7^8=9$，$7^9=8$，$7^{10}=1$，因此7是GF（11）上的本原元素。

设A的私钥$X_A = 3$，公钥$Y_A = 2$；B的私钥$X_B = 5$，公钥$Y_B = 10$，假定A要将信息m = 7发送给B，A取随机数x = 5，A计算$C_1 = g^5 \bmod 11 = 10$，$K = (Y_B)^5 \bmod 11 = 10$，$C_2 = K*m \bmod 11 = 70 \bmod 11 = 4$。A将（10，4）作为密文发送给B，B收到后计算$K = (C_1)^{XB} \bmod p = 10^5 \bmod 11 = 10$，$K^{-1} = 10$（根据$K* K^{-1} = 1 \bmod 11$），则$m = K^{-1}* C_2 = 40 \bmod 11 = 7$。