



# 现代密码学

## 第三十八讲 ElGamal公钥密码体制简介

信息与软件工程学院



## 第三十八讲 ElGamal公钥密码体制简介

---





## A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms

TAHER ELGAMAL, MEMBER, IEEE

**Abstract**—A new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.

### I. INTRODUCTION

IN 1976, Diffie and Hellman [3] introduced the concept of public key cryptography. Since then, several attempts have been made to find practical public key systems (see, for example, [6], [7], [9]) depending on the difficulty of solving some problems. For example, the Rives-Shamir-Adleman (RSA) system [9] depends on the difficulty of factoring large integers. This paper presents systems that rely on the difficulty of computing logarithms over finite fields.

Section II shows a way to implement the public key distribution scheme introduced by Diffie and Hellman [3] to encrypt and decrypt messages. The security of this system is equivalent to that of the distribution scheme. Section III introduces a new digital signature scheme that depends on the difficulty of computing discrete logarithms over finite fields. It is not yet proved that breaking the system is equivalent to computing discrete logarithms. Section IV develops some attacks on the signature scheme, none of which seems to break it. Section V gives some properties of the system. Section VI contains a conclusion and some remarks.

Hence both  $A$  and  $B$  are able to compute  $K_{AB}$ . But, for an intruder, computing  $K_{AB}$  appears to be difficult. It is not yet proved that breaking the system is equivalent to computing discrete logarithms. For more details refer to [3].

In any of the cryptographic systems based on discrete logarithms,  $p$  must be chosen such that  $p-1$  has at least one large prime factor. If  $p-1$  has only small prime factors, then computing discrete logarithms is easy (see [8]).

Now suppose that  $A$  wants to send  $B$  a message  $m$ , where  $0 \leq m \leq p-1$ . First  $A$  chooses a number  $k$  uniformly between 0 and  $p-1$ . Note that  $k$  will serve as the secret  $x_A$  in the key distribution scheme. Then  $A$  computes the "key"

$$K \equiv y_B^k \pmod{p}, \quad (1)$$

where  $y_B \equiv \alpha^{x_B} \pmod{p}$  is either in a public file or is sent by  $B$ . The encrypted message (or ciphertext) is then the pair  $(c_1, c_2)$ , where

$$c_1 = \alpha^k \pmod{p} \quad c_2 = Km \pmod{p} \quad (2)$$

and  $K$  is computed in (1).

Note that the size of the ciphertext is double the size of the message. Also note that the multiplication operation in (2) can be replaced by any other invertible operation such as addition mod  $p$ .

The decryption operation splits into two parts. The first step is recovering  $K$ , which is easy for  $B$  since  $K \equiv (\alpha^k)^{x_B} \pmod{p}$  and  $x_B$  is known to  $B$  only. The second step



## 第三十八讲 ElGamal公钥密码体制简介

---





# ElGamal公钥加密体制原理

---

密钥生成:

$p$  , 一个较大素数

$g$  ,  $Z_p^*$  中的生成元

$\alpha \in Z_{p-1}, \beta = g^\alpha \bmod p$

$p, g, \beta$  为公钥;  $\alpha$  为私钥

加密:

随机生成一个秘密数  $k, k \in Z_{p-1}$  。

$E(x, k) = (r, s)$ , 其中

$$r = g^k \bmod p$$

$$s = x\beta^k \bmod p$$

解密:  $D(r, s) = s(r^\alpha)^{-1} \bmod p = xg^{\alpha k}g^{-\alpha k} \bmod p = x$

---



## 第三十八讲 ElGamal公钥密码体制简介





# ElGamal与RSA的区别

---



□数学困难问题

□公开参数设置

---



---

感谢聆听!

xionghu.uestc@gmail.com

---