1. 基本的离散对数问题
2. 离散对数问题的其他构造（变种）
3. 与大整数分解问题的不同和Diffie-Hellman问题关联。
4. 离散对数（Discrete logarithm）：

当模有原根时，设为模的一个原根，则当 (mod 时：

, 此处的为 以整数为底，模时的离散对数值

性质:

和一般的对数有着相类似的性质：

历史及由来：（可略）

默克勒(R.C.Merkle)甚至在迪菲(W.Diffie)和赫尔曼(E.Hellman)之前的1975年就提出了类似的公钥密码体制思想，他们三人只是提出了一种关于公钥密码体制与数字签名的思想，而没有真正实现。不过，他们确实是实现了一种体现公钥密码体制思想、基于**离散对数**问题的、在不安全的通道上进行密钥形成与交换的新技术。



求解离散对数问题：寻找指数

2、离散对数问题的其他构造（变种）

**（1）有限域上的离散对数问题：**

定义9.5.2(有限域上的离散对数问题)

设p，q为两个素数，G=, )为阶为的有限域上的乘法群。给定一个元素,找到一个整数, 使得的问题，称为有限域上的离散对数问题.

**（2）有限域上的离散对数问题：**

有限域扩域上的离散对数问题；

**（3）有限域椭圆曲线群上的离散对数问题：**

将生成元由上的一个数变成椭圆曲线上的一个点元素，而点的横纵坐标、椭圆曲线方程中的系数、椭圆曲线上的运算限定在有限域上

（可略，列举一下然后展开讲下面两种形式）

形式1：

g，h为两个无关原根（即以为底的离散对数未知），p为素数，a与p互素：若：

为无关原根，p为素数，a与p互素：

用于设计群签名（Group Signature）和可追踪的盲签名（Traceable Blind Signature）

形式2：**有限域椭圆曲线群上的离散对数问题**

Ep（a，b）: 是有限域上的所有点构成的群的一个循环子群, 其阶为是的生成元，给定G中任意点Q，找到一个整数xp使得Q=xP;

3、与大整数分解问题的不同和Diffie-Hellman问题关联

**（1）大整数分解问题：**

给定一个大整数N，找出其质因数p和q，使得N = p × q；

将两个大素数相乘容易，但对其乘积进行因式分解极其困难

应用：RSA加密等

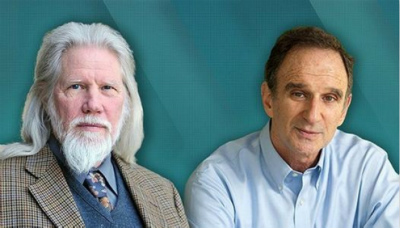
**（2）离散对数问题：**

在有限群G中，给定生成元g和元素h，找到整数x使得gx = h（mod n）

x求解在大素数阶群上时间复杂度为指数级

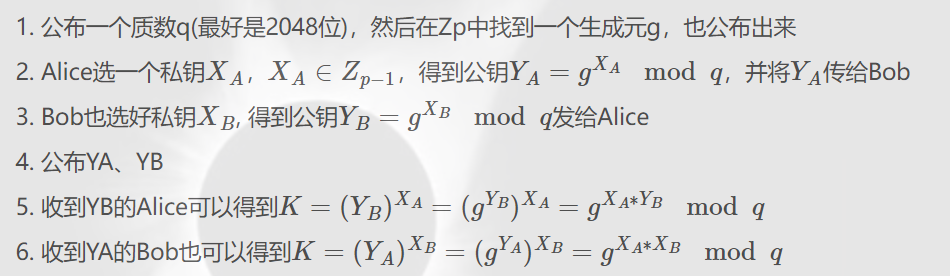
应用：Diffie-Hellman密钥交换和ElGamal加密

## **密钥交换协议 （Diffie Hellman）**



以两位发明者命名的密码方案，其思想为理解ElGamal加密奠定了基础。

密钥交换协议****不是****一种****加密明文的算法****，而是****生成****一个较为安全的****密钥的算法****



**(Diffie-Heliman 问题)**

设p为素数，g为p的原根.任意可以表示为 ,其中是未知的.

Diffie- Hellman 问题是找到一个 c 使其满足

1. H 问题和离散对数问题之间的关系如下：

若离散对数问题能够在多项式时间内被解决，则 D-H 问题也能够在多项式时间内被解决；反之则未必成立·已经证明在某些条件下，这两个问题是等价的，但即使是在这些条件下，解决离散对数问题仍是困难的，否则离散对数问题就无法应用于密码学了

Diffie-Hellman密钥交换协议的有效性依赖于计算离散对数的困难性

离散对数问题： g？≡ h （mod p）

D-H问题： ？≡ gxy （mod p）