最近有很多小伙伴咨询关于elgamal加密算法的问题，小编结合多年的经验整理出来一些elgamal加密算法总结对应的资料，分享给大家。

ElGamal方法分为密钥生成、加密过程和解密过程进行描述。假设Alice和Bob分别为通信的双方，则：

密钥生成

通信发起一方的Alice按以下方法生成公钥：

Alice通过生成元g和阶q定义一个乘法循环群G；

Alice在集合R={0, 1, 2, ..., q-1}中随机选择一个整数x；

Alice根据群G的生成元和阶生成群中的一个元素h：；

Alice将{G, q, g, h}作为公钥发布，x作为私钥妥善保存。

加密过程

通讯另一方的Bob在加密过程中通过公钥{G, q, g, h}对明文m进行加密(其中1-3步可以事先完成。)：

Bob在集合R={0, 1, 2, ..., q-1}中随机选择一个整数y；

Bob根据{G, q, g, h}生成群中的一个元素 ；

Bob根据 得到对称密钥；(由于Bob每次接收到消息后都会生成s，因此s也称为临时密钥)

Bob将明文m转换为群G中的一个元素 ；(如将特定信息进行编码)

Bob计算 ；

Bob将 作为密文发送。

解密过程

Alice使用私钥x对密文 进行解密，步骤为：

Alice计算 ；

Alice计算群中的元素 ，并将其还原为明文。(将编码还原为信息)

下述等式保证了Alice计算出的编码与Bob转换的编码相同：

不能。如果使用了相同的随机数，可以计算出 K 值，从而计算出私钥 a。

ElGamal加密算法可以定义在任何循环群G上。它的安全性取决于G上的离散对数难题。

ElGamal加密算法是一个基于迪菲-
赫尔曼密钥交换的非对称加密算法。它在1985年由塔希尔·盖莫尔提出。

公钥密码（Public-key cryptography） 也称非对称式密码（Asymmetric cryptography）是密码学的一种算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥； 公钥用作加密，私钥则用作解密 。使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。公钥可以公开，可任意向外发布；私钥不可以公开。

1976年以前，所有的加密方法都是同一种模式:加密和解密使用同样的规则。

1976年，由惠特菲尔德·迪菲（Bailey Whitfield Diffie）和马丁·赫尔曼（Martin Edward Hellman）在1976年首次发表 迪菲-赫尔曼密钥交换 。

1977年，Ralph Merkle和Martin Hellman
共同设计了一种具体的公钥密码算法– Knapsack 。

1978年，罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）共同发表了一种公钥密码算法– RSA 。

RSA 可以说是现在公钥密码的事实标准 。

在对称密码中，由于加密和解密的密钥是相同的，因此必须向接收者配送密钥。由于解密的密钥必须被配送给接收者，在传输中的过程中存在着被窃听的问题，这一

问题称为 密钥配送问题 。

解决密钥配送问题的方法有以下几种：

RSA 是世界第一个广泛使用的公钥算法，可以被用于公钥密码和数字签名。RSA 公开密钥密码体制的原理是：根据数论，寻求两个大素数比较简单，而将它们的乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。它的强度被认为与分解一个非常大的数字的难度上述文章内容就是。以现代数字计算机的当前和可预见的速度，在生成 RSA 密钥时选择足够长的素数应该使该算法无限期地安全。但是，这种信念尚未在数学上得到证明，并且可能有一种快速分解算法或一种完全不同的破解 RSA 加密的方法。

ab = 1

然而只根据 N 和 E（注意：不是p和q）要计算出 d 是不可能的。因此，任何人都可对明文进行加密，但只有授权用户（知道D）才可对密文解密。

RSA 是现在最为普及的一种公钥密码算法，但是除了 RSA之外还有其他的公钥密码，基于与 RSA 等效复杂度的不同数学，包括 ElGamal 加密 、 Rabin 方式 和 椭圆曲线加密 。

在密码学中， ElGamal 加密算法 是一个基于迪菲-赫尔曼密钥交换的非对称加密算法。它在1985年由塔希尔·盖莫尔（Taher ElGamal）提出。ElGamal加密算法利用了 求离散对数的困难数。

Rabin 利用了 下平方根的困难度

椭圆曲线密码 是通过将椭圆曲线上的特定点进行特殊的乘法运算实现，它利用了这种乘法运算的逆运算非常困难这一特性。它的特点是所需的密钥长度比 RSA 短。

关于elgamal加密算法和elgamal加密算法总结的介绍到此就结束了，不知道你从中找到你需要的信息了吗 ？如果你还想了解更多这方面的信息，记得收藏关注本站。