谈谈 RSA 加密算法

答：

RSA 公开密钥密码体制；

公开密钥密码体制就是使用不同的加密密钥与解密密钥；

是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

RSA 算法基于以下事实：将两个大素数相乘十分容易，但是想要对其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。

在公开密钥密码体制中，公钥是公开信息，而解私钥是需要保密的。加密算法和解密算法也是公开的。

RSA 加密的原则：公钥加密，私钥解密 或 私钥加密，公钥解密，如：

1、甲方在本地构建密钥对（公钥+私钥），并将公钥公布给乙方；

2、甲方用私钥对数据加密，发送给乙方；

3、乙方用公钥对数据进行解密。

如果乙方向传送数据给甲方：

1、乙方用公钥对数据进行加密，然后传送给甲方；

2、甲方用私钥对数据进行解密。

RSA 在以下领域得到广泛应用：保密通信、数字签名、认证功能、密钥管理。

由传统的政府、军事等应用领域走向商用、民用的基础，同时互联网、电子商务的发展为密码学的发展开辟了更为广阔的前景。

实际开发中，往往需要将用户注册的密码加密，防止被人盗取，即使是数据库管理员都不能查看到用户注册的密码。

加密步骤：

1、 产生私钥-公钥对，将私钥和公钥保存在服务端的数据库。

2、 在客户端中用公钥将密码加密，然后上传服务端并保存在服务端的数据库中。

3、 客户端在登陆时，将密码用公钥加密，然后上传，服务端将数据库中的密码与客户端的上传的密码比较。