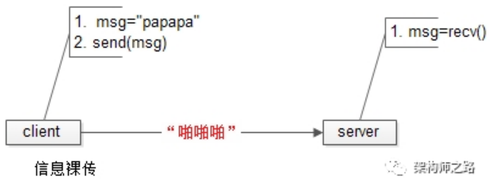
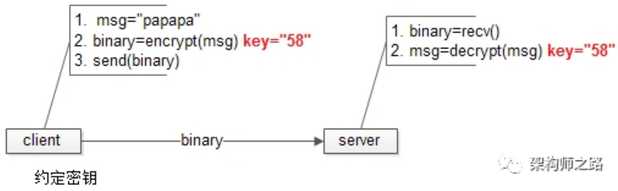
消息安全传输发展的几个阶段

一. 初级阶段: 信息裸传



1. 特点：在网络上传递明文
   黑客定理一：网络上传递的数据是不安全的，属网络于黑客公共场所，能被截取
2. 结果：传递明文无异于不穿衣服裸奔
   改进方案：先加密，然后在网络上传输

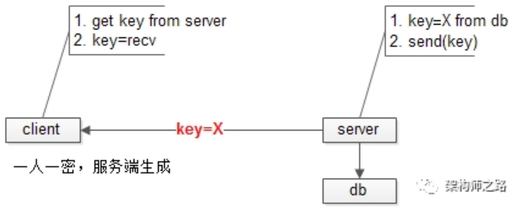
二. 进阶阶段: 传输密文



1. 特点：
   - 服务端和客户端先约定好加密算法，加密密钥
   - 客户端，传输前用约定好的密钥加密
   - 传输密文
   - 服务端，收到消息后用约定好的密钥解密

   黑客定理二：客户端的代码是不安全的，属于黑客本地范畴，能被逆向工程，任何客户端与服务端提前约定好的算法与密钥都是不安全的
2. 结果：任何客户端的代码混淆，二进制化都只能提高黑客的破解门槛，本质是不安全的
   改进方案：不能固定密钥

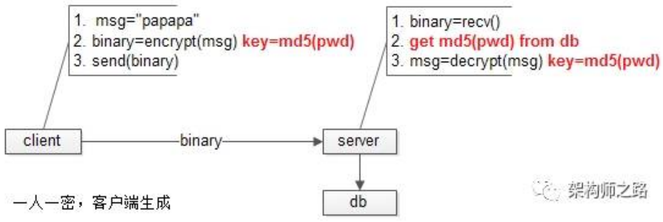
三. 中级阶段: 服务端为每个用户生成密钥



1. 特点：
   - 客户端和服务端提前约定好加密算法，在传递消息前，先协商密钥
   - 客户端，请求密钥
   - 服务端，返回密钥
   - 然后用协商密钥加密消息，传输密文
2. 结果：
   - 如黑客定理一，网上传输的内容是不安全的，于是乎，黑客能得到加密key=X
   - 如黑客定理二，客户端和服务端提前约定的加密算法是不安全的，于是乎，黑客能得到加密算法
   - 于是乎，黑客截取后续传递的密文，可以用对应的算法和密钥解密

   改进方案：协商的密钥不能在网络上传递

四. 再进阶阶段: 客户端确定密钥，密钥不再传输



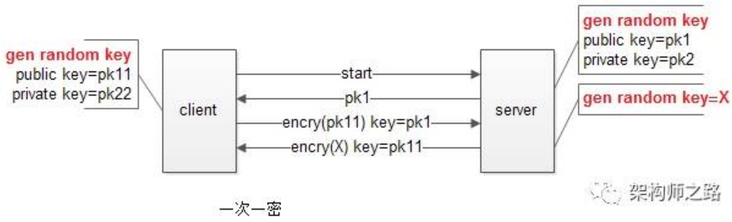
1. 特点：
   - 协商的密钥无需在网络传输
   - 使用“具备用户特性的东西”作为加密密钥，例如：用户密码的散列值
   - 一人一密，每个人的密钥不同
   - 然后密钥加密消息，传输密文
   - 服务端从db里获取这个“具备用户特性的东西”，解密

   黑客定理三：用户客户端内存是安全的，属于黑客远端范畴，不能被破解

五. 高级阶段: 一次一密，密钥协商

特点：每次通信前，进行密钥协商，一次一密

密钥协商过程，如下图所述，需要随机生成三次密钥，两次非对称加密密钥（公钥，私钥），一次对称加密密钥，简称安全信道建立的“三次握手”，在客户端发起安全信道建立请求后：



1. 服务端随机生成公私钥对(公钥pk1，私钥pk2)，并将公钥pk1传给客户端(注意：此时黑客能截获pk1)
2. 客户端随机生成公私钥对(公钥pk11，私钥pk22)，并将公钥pk11，通过pk1加密，传给服务端(注意：此时黑客能截获密文，也知道是通过pk1加密的，但由于黑客不知道私钥pk2，是无法解密的)服务端收到密文，用私钥pk2解密，得到pk11
3. 服务端随机生成对称加密密钥key=X，用pk11加密，传给客户端(注意：同理，黑客由密文无法解密出key)客户端收到密文，用私钥pk22解密，可到key=X

至此，安全信道建立完毕，后续通讯用key=X加密，以保证信息的安全性