https://www.cnblogs.com/zhangshitong/p/6478721.html

HTTP权威指南

a. Alice生成一个密钥对：pk与sk，然后向Bob发布她的公钥pk
b. Bob接到pk后生成一个随机密钥k，然后用pk对k进行加密，得到密文E
c. Bob将E发送给Alice
d. Alice用私钥sk对E解密，即可得到k
e. Alice与Bob可以用k进行安全通信了