数据加密

明文：未加密的消息

密文：被加密的消息（未授权者看不懂）

加密：伪装消息以隐藏信息的过程，即明文转变为密文的过程

解密：密文转变为明文的过程

密钥：加密解密需要特定的参数，需要保密

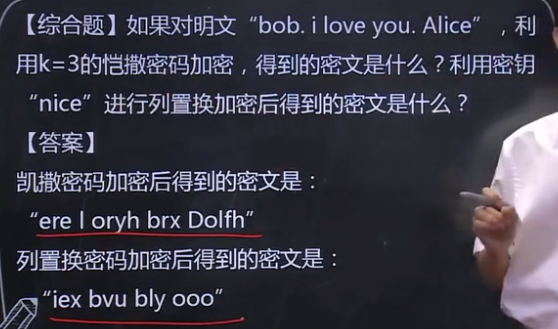
一、传统加密方式（加密强度不够）

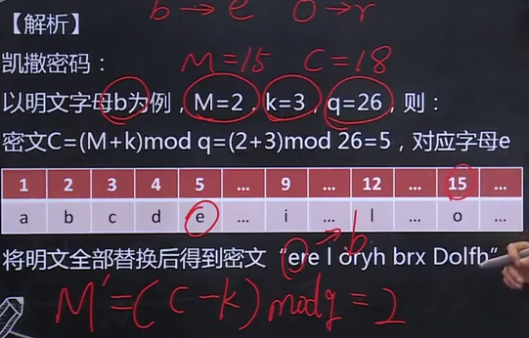
1. 代替密码：用密文字母替代明文字母

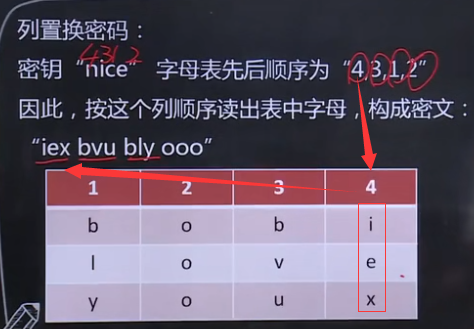
移位密码加密函数（E：加密，M：明文信息，k：密钥，运算时将其转换为数字）

解密函数（D：解密，C：密文，K：密文信息）

1. 换位密码：根据一定的规则重新排列明文







1. 对称密钥加密

现在密码分类：

对称密钥密码：加密密钥和解密密钥相同（密钥保密）

对称密钥密码分类：（注意可别被穷举攻击）

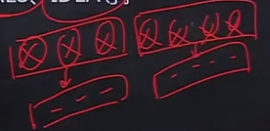
分组密码：若干位信息一组生成一组密文

DES：56位密钥，64位分组（现已经不安全<-穷举）

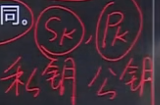
三重DES：使用两个密钥（共112位），执行三次DES算法

AES：分组128位，密钥128/192/256位（高级加密）

IDEA：分组64位，密钥128位（一般加密128已经足够）



流密码（一个一个信息进行加密）

非对称密钥密码：加密密钥和解密密钥不同（公钥密钥发送给私钥持有者）

1. 非对称/公开密钥加密

密钥成对使用，其中一个用于加密，另一个用于解密，且加密密钥可以公开，也称公开密钥加密

典型的公钥算法：Diffie-Hellman算法，RSA算法

