HomeWork1

120L020614-刘昕烨

Problem 1：

1. 对于移位密码来说，我认为只需要知道**一个**任意的字母与其对应的密文即可得到对应的密钥。因此选取的明文串长度为 1。假设选取的字母为 m 对应的密文为 c 选取的密钥为 k。

由于$c = Enc_k(m) = (m + k) mod 26$ 因此我们可以很容易得到$k = (c - m) mod 26$ 。从而得到密钥 k。

2. 对于单字母替换密码来说其将字母表中的 26 个英文字母映射到密文中的 26 个英文字母，我们要想知道全部的 26 个字母的映射关系那么密文-明文对中明文串至少应该含有 25 个不同的英文字母（剩下的那个明文字母与剩下的密文字母相对应）。这样才能确定对应的映射关系，而这样的话我们的明文串可以是从 25 开始的任意长度的字符串（但是必须含有 25 个不同的英文字母）。

解密的话我们只要中找到明文串中的每个字母对应的密文串的字母即可得到密钥 K。

3. Vigenère 密码通过重复密码字得到长度与明文串长度相同的字符串，让每个明文字符“加”对应字符串的字符得到对应的密文。因此对于 Vigenère 密码来说解密可以分为两种情况：

如果我们事先知道其密码字长度 x 的话，我们只需要知道长为 x 的明文-密文对即可破解。例如我们假设明文串为 M 对应的密码字为 K 加密后的密文串为 C，它们对应的第 n 个元素用下标 n 表示（n<=x）。那么有：

$$(M_n + K_n) mod 26 = C_n \quad \Rightarrow \quad (C_n - M_n) mod 26 = K_n$$

则利用与移位密码相同的方法可以解出密码字的内容即可得到密钥 K。

如果我们事先并未知道其密码字长度 x 的话，我们所需要的明文长度是不确定的。例如我们想要得到密钥，先假设从明文长度为 1 开始不断尝试利用上面的方法通过明文密文对来获得密码字。我们会发现即使我们得到了形式如 XX 的密码字（X 为某一字符串），我们也没法确定字符串 X 就是最终的密钥，还需要再次进行实验。因为我们没法保证密钥的形式不为 XXY（Y 为与 X 不同的字符串）。

因此我认为我们进行实验时只能用足够长的明文进行测试后得到某个字符串 X 多次重

复组成的密码字，接着假设字符串 X 就是最终的密钥（因为此时再加入与 X 不同的字符串其加密效率较低而且密钥较长难以传输）。而这个较长的明文长度我们无法确定。

Problem 2：

这个问题与问题 1 类似。除了在这个问题中我们可以选择明文串的内容与长度来得到加密后的密文因此比较简便。

1. 对于移位密码来说其需要的长度与问题 1 相同即 1 个字母，只不过我们可以使明文为字母 Z 来简化计算。与问题 1 类似，其结果为$k=(c-m)mod26$，只不过这里 m=Z。

2. 对于字母替换密码来说根据我们问题 1 中的论述可以构造一个最简单的含有 25 个英文字母的字符串$ABCDEFGHIJKLMNOPQRSTUVWXY$来进行推断，根据得到的密文以及问题 1 第 2 问的方法我们就可以得到密钥 K 了。

3. 对于 Vigenère 密码来说我们只能通过选定明文内容来简化计算，但是需要的明文长度无法改变。

如果我们已知其密钥长度 x 那么与第 1 问类似我们可以构造一个字符串长度为 x 其内容全为字母 Z，用问题 1 中的以下公式，我们可以很容易的得到密钥 K。

$$(M_n+K_n)mod26=C_n \quad \Rightarrow \quad (C_n-M_n)mod26=K_n$$

如果我们未知其密钥长度，我们仍然无法知道需要多长的明文。但就像问题 1 中的表达一样我们可以利用全为字母 Z 的明文串来简化计算。我们需要构造足够长的明文，例如我们如果构造以下明文得到密文：

$$ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ$$
$$ABCABCDABCABCDABCABCDABCABCDABCABCDAB$$

那么我们可以相信 ABCABCD 就是其密钥，因为如果不是的话加密效率会过低且密钥太难传送。（当然这种假设是可能出错的，只有不断地实验才能检验其正确性）

Problem 3：

这一论述是错误的，证明如下：

证：假设这一论断是正确的，由于加密方法是完美保密的，我们根据完美保密的定义 1 可以得出：

$$Pr[M=m|C=c]=Pr[M=m]$$

又因为给出了条件：

$$\forall m,m' \in M, \forall c \in C\ , Pr[M=m|C=c]=Pr[M=m'|C=c]$$

我们可以推断出：

$$\forall m,m' \in M, Pr[M=m]=Pr[M=m']$$

因此我们可以得到随机变量 M 的分布函数是确定的，假设|M|=X，则有：

$$\forall m \in M, Pr[M=m]=\frac{1}{|X|}$$

但是题目中给的是 M 的分布函数是任意的，因此有矛盾所以这一论述是错误的。

Problem 4:

(a) 证明：

首先证明移位密码的密钥空间大小为 26，由于移位密码中的密文字母 c 与明文字母 m 以及密钥 k 满足：

$$c=Enc_k(m)=(m+k)mod26$$

因此我们可以知道当$k \notin [0,25]$时我们可以通过求余运算的性质将其变为$k' \in [0,25]$。因此我们可以认为 K 的密钥空间大小为 26

而且变换后的密文 C 与变换前的明文 M 其空间大小也为 26。并且移位密码的密钥是在其密钥空间上等概率选取的，因此$\forall k \in K, Pr[K=k]=\frac{1}{|K|}$。

并且$\forall m \in M, \forall c \in C\ \ k=(m-c)mod26$ 由于 m 与 c 是确定的，并且由于 k 的取值范围限定在了 0 到 25 之间，因此 k 也是确定且唯一的。

所以由香农定理可知在该条件下移位密码是完美保密的。

(b)我认为其为$26!$

首先由于要使单字母替换为完美保密我们由定理 5 及完美保密的局限性知道|M|<=|K|所以明文空间 M 的大小最大为 K 的密钥空间大小及 $26!$。下证当 M 取到 $26!$ 时单字母替换为完美保密。

首先由于其映射函数的一对一特性密文空间与明文空间大小一定相同所以|M|=|C|=|K|，此外其密钥选取满足$\forall k \in K, Pr[K=k]=\frac{1}{|K|}$，并且由于其映射的唯一性给定任意明文与密文其对应的密钥是唯一的。所以由香农定理当|M|=$26!$ 单字母替换是完美保密的。

由上面的论述要想单字母替换为完美保密其明文空间 M 的大小最大为 $26!$。

(c)密钥长度应该和明文长度相同为 t 并且满足$\forall k \in K, Pr[K=k]=\frac{1}{|K|}$。

下证其满足完美保密的要求。

证明:

首先我们很容易知道密文长度为 t，密文空间大小与明文空间与密钥空间相同，并且由于对于明文 M 与密文 C 的位置为 n 的字母均满足以下公式:

$$(M_n+K_n)mod26=C_n \quad \Rightarrow \quad (C_n-M_n)mod26=K_n$$

因此我们很容易由取余运算的性质知道密钥 K 在明文与密文确定的情况下是唯一的。因此由香农定理我们可以知道此时的 Vigenère 密码满足完美保密。

Problem 5：

（a）我认为首先从完美保密来说这种改动是不应该的，经过改变后其已经不是完美保密的加密方式了，因为密钥空间的大小小于明文空间的大小。这同时也意味着会暴露关于原文的信息，例如攻击者可以知道密文里绝对不会出现明文的任何信息，那么如果在密文中出现了某个地址，那么明文中肯定不是对应的地址，这就给了攻击者明文中的信息的提示。

其次由于密钥为全零的概率与别的任何一个密钥的概率一样是很小的，我们没有理由删除它。我们举一个例子，我们对 one 进行加密，我们知道其加密为 one 与加密为 two 的可能性是相同的因为其对应的密钥都是一个可能性均为$\frac{1}{|K|}$。所以即使对方收到了对应的明文也没法假设它就是明文。反而如果删除了它受到 two 后可以肯定原文不是 two 会对保密性造成影响。

（b）首先从公式上 OTP 是符合完美保密的定义的，因此我们可以知道在知道密文的情况下攻击者无法获得关于明文的任何信息，即使他获得了明文他也会认为其原文很可能不是这样，因为 ASCII 码长度与密文相同的任何明文加密为该明文的概率都是一样的。

我们现在的问题是为什么即使明文可能传给对方的情况下 OTP 仍然是完美保密的。举个例子，我发送了一句话 I like apple，其可能会被发给对方，但是如果对方收到了这句话他是否能相信这句话呢?

我们假设这个攻击者是完全理性的，从他的角度来看，我的原句子可能是 I like apple，也可能是 I hate apple，也可能是 I hate fruit。这三者由明文加密为密文的概率是相同的，此外还有很多种可能性，只要密文对应的 ASCII 码长度与明文一样长则均可能加密出来且可能性与 I like apple 完全相同均为$\frac{1}{|K|}$，所以一个理智的攻击者会把这句话直接当作明文的可能性基

本不存在。