《密码学》课程习题

执笔 张焕国

第二章习题

1、 解释密码体制的概念。
2、 说明密码体制框图（图 2-1）中攻击者的作用。
3、 说明密码体制的分类，它们各有什么特点?
4、 说明什么是演化密码？它有什么优点?
5、 什么是密码分析？密码分析的方法有哪些类型？它们各有什么特点?
6、 说明什么是“计算上不可破译”？它对我们有什么意义?
7、 为什么说，理论上任何实用的密码都是可破的?
8、 计算机的程序文件和数据库文件加密容易受到什么攻击？为什么?
9、 已知置换如下：

$$P=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 5 & 1 & 6 & 4 & 2\end{pmatrix}$$

①设明文 = 642135，求出密文 = ?
②设密文 = 214365，求出明文 = ?

10、 证明，在置换密码中，置换 p 是对合的，当且仅当对任意的 i 和 j(i, j=1,2,3,…,n)，若 p(i)=j，则必有 p(j)=i 。
11、以英文为例，用加法密码，取密钥常数 k= 7，对明文 INFORMATION SECURITY，进行加密，求出密文。
12、 已知一个加法密码的密文如下：**CSYEVIXIVQMREXIH** 用穷举法求出明文。
13、 编程实现 Vigenre 密码。
14、 分析 Vernam 密码的优缺点。
15、 什么是“一次一密” 密码？为什么它是不实用的?
16、 什么是对合运算？举出 3 种对合运算。
17、 使加法密码算法成为对合运算的密钥 k 称为对合密钥，以英文为例求出其对合密钥。
18、 分析加法、乘法和仿射密码的安全性。
19、 设明文数据块包含 1024 位，设计一个方案将 64 位的密钥扩展为 1024 位，将明文与扩展密钥进行异或运算，类似一次一密。试问这个密码是否与“一次一密”一样安全？为什么?
20、 从 SuperBase 密码被破译，能给我们什么启示?