第二章作业

16337341 朱志儒

思考题

2.1 对称密码的本质成分：明文、加密算法、密钥、密文、解密算法。

2.2 密码算法中两个基本函数：排列和替换。

2.4 流密码：一次加密数据流的一位或一字节的密码；

分组密码：将一个明文分组作为整体加密并且通常得到的是与明文等长的密文密码。

2.5 密码分析和穷举攻击。

2.6 唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择文本攻击。

2.7 无条件安全：无论有多少可使用的密文，都不足以唯一的确定密文所对应的明文。

计算上安全：破译密码的代价超出密文信息的价值，或破译密码的时间超出密文信息的有效生命期。

2.8 Caesar 密码：对字母表中的每个字母用它之后的第 K 个字母来代替，其中 K 的范围是 1 到 25。

2.9 单表代替密码：将明文字母表映射到密文字母表，是的明文字母表中的每个字母映射到密文字母表的单个唯一字母。

2.10 Playfair 密码：基于一个由密钥词构成的 5x5 字母矩阵，使用该矩阵一次加密明文的两个字母。

2.11 多表代替密码：根据密钥对每个连续的明文字母使用单独的单表替代密码。

2.12 问题：（1）生产大规模随机密钥有实际困难，（2）对每条发送的信息，需要提供给发送方和接收方等长度的密钥，存在庞大的密钥分配问题。

2.13 置换密码：明文字母的不同排列。

2.14 隐写术：由一段文本字词重新排列组成。

习题

2.1（a）没有限制，b 值的改变会使明文字母与密文字母的关系左移或是右移，如果映射是一对一的话，b 值改变后映射还会是一对一的。

（b）与 26 不互素的值。

（c）a 的取值需与 26 互素且 a<26。因为若 a 与 26 不互斥，对任意的 p，q，有$ap(\mathrm{mod}\ 26) = aq(\mathrm{mod}\ 26)$成立，即$E(a, p) = E(a, q)$成立，则该加密算法不是单射，不满足条件。

2.2 a 的取值有 $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$，b 的取值为 0 到 25，故共有 12x26=312 种放射 Caesar 密码。

2.3 明文中最高频字母为 E，第二高频字母为 T，又 E=4，B=2，T=19，U=20，则有$1 = (4a + b) \bmod 26 \quad 20 = (19a + b) \bmod 26$，可解得 a=3，b=15，故密码：$C = E([3, 15], p) = (ap + b) \bmod 26$。

2.4 破译的明文：

A good glass in the Bishop's hostel in the Devil's seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death's head— a bee line from the tree through the shot fifty feet out.

2.5 （a）第一个字母 t 对应 a，h 对应 b，e 对应 c，s 对应 d，n 对应 e，以此类推，忽略第二次出现的字母。

密文：SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

明文：basilisk to leviathan blake is contact

（b）它是单表代替密码，很容易被破解。

（c）最后一句话可能不包含字母表中的所有字母，使用第一句话可以使用后续的句子，直到遇到字母表中 26 个字母。

2.8 密钥词为 SPUTNIK。

2.9 明文为 PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION。

2.10 （a）

L	A	R	G	E
S	T	B	C	D
F	H	I/J	K	M
N	O	P	Q	U
V	W	X	Y	Z

（b）

O	C	U	R	E
N	A	B	D	F
G	H	I/J	K	L
M	P	Q	S	T
V	W	X	Y	Z

2.11 （a）密文：UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

（b）密文：UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

2.12 （a）$25! \approx 2^{84}$

2.13 移位量由关键字确定，关键字决定了矩阵中字母的位置。

2.14 （a）消息中字母个数为奇数，所以在最后加入“q”使得个数为偶。

密文：GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRKR

（b）加密矩阵的行列式$\det A = 43$, 又$43^{-1} \bmod 26 = 23$, 则解密矩阵为$\begin{bmatrix} 25 & 14 \\ 11 & 5 \end{bmatrix}$, 其他步骤与加密步骤相同。

2.16 （a）7×13^4 （b）7×13^4 （c）13^4 （d）10×13^4 （e）$2^4 \times 13^2$

（f）$2^4 \times (13^2 - 1) \times 13$ （g）37648 （h）23530 （i）157248

2.19 明文：explanation

密钥：legleglegleg

密文：pbvwetlxozr

2.20（a）密文：BECKJDMSXZPMH

（b）密钥：25 4 22 3 22 15 19 5 19 21 12 8 4