Ch7

1.(a) $p(x)$是关于 s、f 的二元一次函数，已知任意两个人的信息，相当于解有两个线性无关等式的二元一次方程组，具有唯一解，因此可以恢复 s。

(b) 10 位相关人员收到的信息是 $p(i)$等式的值，它有 s 和 f 两个未知量。又知 f 是 101 个比特的素数 q 的剩余域中的元素，它约有 2^{101} 种选择，命中的概率是 $1/2^{101}$。因此仅凭自己的信息解得 s，需要尝试大约 2^{101} 次。以超级计算机“太湖之光”的算力为例，它每秒能计算约 2^{56} 次浮点运算，使用它解得 s 仍然需要 2^{45} 秒，约 111,569 年。

2.(1) 该算法属于舍伍德算法，因为它一定能求得正确解。

(2) 证:引入随机变量 X(i)，当随机选择的元素是第 i 小时，X(i)=1，k 的左边有 i-1 个元素，右边有 n-i 个元素，因此集合大小的期望可以表示为 E[$\sum_1^n$X(i)max(i-1, n-i))]=E[X(i)]max(i-1, n-i)。其中，E[X(i)]恒为 1/n。当 $i\in$[1, n/2]时，max(i-1, n-i)=n-i，否则 max(i-1, n-i)=i-1。得到 E⩽1/n*$\sum_1^{n/2}(k-1)$+1/n*$\sum_{n/2}^{n}(n-k)$=$\frac{n-1}{2}$,命题得证。

(3) 当选定元素 k 后，划分过程的时间复杂度是 O(n)，因此 E(T(n))=E[$\sum_1^n$X(i)T(max(i-1, n-i))]+O(n)=$\sum_1^n$E[X(i)T(max(i-1, n-i))]+O(n)，缩放过程同(2)，得 E(T(n))⩽cn/4-c/2-O(n)。设 O(n)=an，a 是一个常数，则 E(T(n))⩽cn/4-c/2-an=O(n)，命题得证。

3. 算法 **RandomPolyEqual**($p(x)$, $q(x)$, $r(x)$, m, n, l)

输入 :多项式 $p(x)$, $q(x)$, $r(x)$,阶 m, n, l

输出 : $p(x)$、$q(x)$之积是否等于 $r(x)$

```
k = max{m+n, l}
For c=1 to k Do
    X[c]=random()
Endfor
For c=1 to k Do
    If p(X[c])*q(X[c])!=r(X[c]) then return false
Endfor
return true
```

算法的时间复杂度取决于 k，因此为 O(max{m+n, l})。设实数集大小为 S，获得正确解的概率为 1-max{m+n, l}/S。由于返回的解不一定正确，因此该算法是蒙特卡洛算法。

4. 算法 **RandomMatrixEqual**(A, B, C)

输入 :矩阵 A, B, C

输出 : 是否满足 AB=C

```
Random generate a r*1 vector r //随机产生 r*1 的向量，其中的值仅取 0 或 1
    If A(Br)==Cr then return true
return false
```

$m\cdot n$ 的时间复杂度为 O(pqr)。当 AB=C 时，算法返回的结果一定正确；当 AB!=C 时，出错的概率≤1/2，下进行证明。证：令 D=AB-C，由于矩阵乘法不满足消去律，算法出错的情况是 D!=0，而 Dr=0。下证当 D!=0 时，p(Dr!=0)≥1/2，即当 AB!=C 时，正确的概率≥1/2，与原命题等价。假设 R 是所有满足 Dv=0 的 r 的向量集合。令 v 为除了 v_i=1，其余元素均为 0 的向量，如下所示。

$$D \times \vec{v} = \begin{pmatrix} d_{11} & \cdots & d_{1j} & \cdots & d_{1n} \\ d_{21} & \cdots & d_{2j} & \cdots & d_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_{i1} & \cdots & d_{ij} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & d_{n2} & d_{1n} & d_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} d_{1j} \\ d_{2j} \\ \vdots \\ d_{ij} \\ \vdots \\ d_{nj} \end{pmatrix}$$

则当对应的 d_{ij}!=0 时，Dv!=0。对于任意 r_k∈R，均满足 Dr_k =0。根据 r_k 的第 i 行数值是 0 还是 1，构造 $r'=r_k+v$ 或 $r'=r_k-v$。对 $r'=r_k+v$ 作说明，则 $Dr'=D(r_k+v)=Dv$!=0，减法同理。显然，是 r_k 随机生产的使算法出错的向量，而 r' 是使算法正确的向量，并且二者仅在第 i 行不同。那么，每当有一个算法出错的向量，总能找到与之对应的是算法正确的向量，因此当 AB!=C 时，正确的概率≥1/2，命题得证。已知算法错误的概率≤1/2，当我们重复 k 次，该算法得到正确解的概率≥$1\text{-}2^k$。由于算法返回错误时 AB 不一定等于 C，而返回正确时 AB 也不一定等于 C，因此该算法是蒙特卡洛算法。

5.证:由于权值随机分配，每次选择 T 中权值最大的边删除和课件中 9.6 问题等价。所以由定理 2，得到正确解的概率大于 $2/n^2=\Omega(1/n^2)$，命题得证。

6.(1)证:因为第 6 步删去了和 u 相邻的顶点，所以 I 中顶点两两不相邻，它是一个独立集。

(2)证:对第 6 步来说，S 每次要删除 d_u+1 个顶点。若 $u\in I$，则第 4 步每次选择标签最小的顶点为 u 的概率为 $1/(d_u+1)$，命题得证。

7.引入随机变量 X(i)，当 a_i 和 a_{i-1} 需要交换时，X(i)=1。交换元素个数的期望表示为 $E=E[\sum_2^n X(i)]=\sum_2^n E[X(i)]=\sum_1^2(2-i)/2+\cdots+\sum_1^n(n-i)/n=n^2-n(n-1)/4=O(n^2)$

8. 算法 **RandomOutputFz**(F, Z)

输入 :数组 F, 数值 Z

输出 : 经过映射后的 F(Z)值

1:	Random select $X_z\in\{0, 1, \ldots, n-1\}$
2:	$Y_z=(Z-X_z) \bmod n$
3:	**return** $(F[X_z]+F[Y_z]) \bmod m$

将 Z 拆分为 X_z 和 Y_z，则映射等价于将$(X_z+Y_z) \bmod n$ 通过 F 函数投影到 F(Z)，满足 $F(Z)=F(X_z)+F(Y_z) \bmod m$。有 3 种情况: X_z 和 Y_z 均未被篡改，正确的概率为 4/5*4/5=16/25；X_z 和 Y_z 有一个被篡改，正确的概率为 2*1/5*4/5=8/25；X_z 和 Y_z 均被篡改，正确的概率为 $1/5*1/5*1/m=1/25m$。算法总的正确率为 $p=16/25+1/25m>1/2$。运行 3 次，若 3 次相同，则返回相同值，正确概率为 $1-(1-p)^3>0.95$，3 次错误且相同的概率忽略不计；若 2 次相同，则返回 2 次的相同值，正确概率为 $1-(1-p)^2>0.87$；若仅有 1 次相同，随机返回一个值，正确概率为 $16/25+1/25m>0.64$。