现代密码学作业——第五讲

1、

状态	输出
1000	0
1100	0
1110	0
1111	1
0111	1
1011	1
0101	1
1010	0
1101	1
0110	0
0011	1
1001	1
0100	0
0010	0
0001	1
1000	0

输出为：000111101011001

2、

状态	输出
1011	1
1101	1
1110	0
1111	1
0111	1
1011	1

输出：11011

周期：5

3、

初始化：

S: 0 1 2 3

K: 1 2 3 1

KSA：

i=0, j=0+s[0]+k[0] mod 4 = 1 , swap(s[0],s[1]) => S: 1 0 2 3

i=1, j=1+s[1]+k[1] mod 4 = 3 , swap(s[1],s[3]) => S: 1 3 2 0

i=2, j=2+s[2]+k[2] mod 4 = 3 , swap(s[2],s[3]) => S: 1 3 0 2

i=3, j=3+s[3]+k[3] mod 4 = 2 , swap(s[3],s[2]) => S: 1 3 2 0

PRGA:

i=0, j=0:

i=(i+1) mod 4=1

j=(j+s[i]) mod 4=3

swap(s[i],s[j])=swap(s[1],s[3])

=>S: 1 0 2 3

t=(s[i]+s[j])=(s[1]+s[3]) mod 4=3

k=s[t]=s[3]=3

=>key:11

重复上述过程，可得密钥 key:1100110111

明文 p=OK=14,10=01110 01010

密文 c=p⊕key=10111 11101=XE

4、

5 级本原多项式 $P(x)=x^5+x^3+1$

对应的反馈函数为 $b_{i+6}=b_{i+3}\oplus b_{i+1}$

5、

4 二元序列的检测

4.1 数据格式

待检数据以比特串的形式接受检测。

4.2 显著性水平

本标准确定的显著性水平为 $\alpha=0.01$。

4.3 样本长度

本标准中样本长度选取 10^6 比特。

4.4 检测项目

4.4.1 概述

本标准采用的随机性检测项目共有 15 项，分别为单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大“1”游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似熵检测、线性复杂度检测、Maurer 通用统计检测、离散傅立叶检测。附录 A 描述了这 15 种检测项目的原理。

4.4.2 单比特频数检测

a) 将待检序列 ε 中的 0 和 1 分别转换成 -1 和 1，$X_i=2\varepsilon_i-1(1\leqslant i\leqslant n)$。

b) 对其累加求和得 $S_n=\sum_{i=1}^{n}X_i$。

c) 计算统计值 $V=\frac{|S_n|}{\sqrt{n}}$。

d) 计算 $P\text{-value}=erfc(V/\sqrt{2})$。

e) 如果 $P\text{-value}\geqslant\alpha$，则认为待检序列通过单比特频数检测。

4.4.3 块内频数检测

a) 将待检序列 ε 分成 $N=\left\lfloor\frac{n}{m}\right\rfloor$ 个长度为 m 的非重叠子序列，将多余的比特舍弃。本规范取 $m=100$。

b) 计算每个子序列中 1 所占的比例 $\pi_i=\frac{\sum_{j=1}^{m}\varepsilon_{(i-1)m+j}}{m}, 1\leqslant i\leqslant N$。

c) 计算统计量 $V=4m\sum_{i=1}^{N}\left(\pi_i-\frac{1}{2}\right)^2$。

d) 计算 $P\text{-value}=igamc\left(\frac{N}{2},\frac{V}{2}\right)$。

e) 如果 P-value$\geqslant\alpha$，则认为待检序列通过块内频数检测。

4.4.4 扑克检测

a) 将待检序列划 ε 分成 $N=\left\lfloor\frac{n}{m}\right\rfloor$ 个长度为 m 的非重叠子序列，将多余的比特舍弃，统计第 i 种子序列模式出现的频数，用 $n_i(1\leqslant i\leqslant 2^m)$ 表示。本规范取 $m=4,8$。

b) 计算统计值 $V=\frac{2^m}{N}\sum_{i=1}^{2^m}n_i^2-N$。

c) 计算 P-value$=igamc((2^m-1)/2,V/2)$。

d) 如果 P-value$\geqslant\alpha$，则认为待检序列通过扑克检测。

4.4.5 重叠子序列检测

a) 由待检序列 ε 构造一个新的序列 ε'，构造方法如下：将序列 ε 最开始的 $m-1$ 位数据添加到序列 ε 的结尾即可得到新序列 ε'，新序列 ε' 的长度为 $n'=n+m-1$。本规范取 $m=2,5$。

b) 计算 ε' 中每一种 m 位子序列模式（共有 2^m 个）出现的频数，记 m 位子序列模式 $i_1i_2\cdots i_m$ 的出现频数为 $v_{i_1i_2\cdots i_m}$。计算每一种 $m-1$ 位子序列模式（共有 2^{m-1} 个）出现的频数，记 $m-1$ 位子序列模式 $i_1i_2\cdots i_{m-1}$ 的出现频数为 $v_{i_1i_2\cdots i_{m-1}}$。计算每一个 $m-2$ 位子序列模式（共有 2^{m-2} 个）出现的频数，记 $m-2$ 位子序列模式 $i_1i_2\cdots i_{m-2}$ 的出现频数为 $v_{i_1i_2\cdots i_{m-2}}$。

c) 计算

$$\Psi_m^2=\frac{2^m}{n}\sum_{i_1i_2\cdots i_m}\left(v_{i_1i_2\cdots i_m}-\frac{n}{2^m}\right)^2=\frac{2^m}{n}\sum_{i_1i_2\cdots i_m}v_{i_1i_2\cdots i_m}^2-n$$

$$\Psi_{m-1}^2=\frac{2^{m-1}}{n}\sum_{i_1i_2\cdots i_{m-1}}\left(v_{i_1i_2\cdots i_{m-1}}-\frac{n}{2^{m-1}}\right)^2=\frac{2^{m-1}}{n}\sum_{i_1i_2\cdots i_{m-1}}v_{i_1i_2\cdots i_{m-1}}^2-n$$

$$\Psi_{m-2}^2=\frac{2^{m-2}}{n}\sum_{i_1i_2\cdots i_{m-2}}\left(v_{i_1i_2\cdots i_{m-2}}-\frac{n}{2^{m-2}}\right)^2=\frac{2^{m-2}}{n}\sum_{i_1i_2\cdots i_{m-2}}v_{i_1i_2\cdots i_{m-2}}^2-n$$

d) 计算

$$\nabla\Psi_m^2=\Psi_m^2-\Psi_{m-1}^2$$
$$\nabla^2\Psi_m^2=\Psi_m^2-2\Psi_{m-1}^2+\Psi_{m-2}^2$$

e) 计算 P-value1$=igamc(2^{m-2},\nabla\Psi_m^2/2)$，$P$-value2$=igamc(2^{m-3},\nabla^2\Psi_m^2/2)$。

f) 如果 P-value1$\geqslant\alpha$ 且 P-value2$\geqslant\alpha$，则认为待检序列通过重叠子序列检测。

4.4.6 游程总数检测

a) 对长度为 n 的待检序列 $\varepsilon_1\varepsilon_2\cdots\varepsilon_n$，计算 $V_n(obs)=\sum_{i=1}^{n-1}r(i)+1$。其中，当 $\varepsilon_i=\varepsilon_{i+1}$ 时，$r(i)=0$；否则，$r(i)=1$。

b) 计算序列中 1 的比例 $\pi=\frac{\sum_{i=1}^{n}\varepsilon_i}{n}$。

c) 计算 P-value$=erfc\left(\frac{|V_n(obs)-2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right)$。

d) 如果 P-value$\geqslant\alpha$，则认为待检序列通过游程总数检测。

4.4.7 游程分布检测

a) 计算 $e_i=(n-i+3)/2^{i+2}$，$1\leqslant i\leqslant n$，并求出满足 $e_i\geqslant5$ 的最大整数 k。

b) 统计待检序列 ε 中每一个游程的长度。变量 b_i，g_i 分别记录一个二元序列中长度为 i 的 1 游程和 0 游程的数目。

c) 计算 $V=\sum_{i=1}^{k}\frac{(b_i-e_i)^2}{e_i}+\sum_{i=1}^{k}\frac{(g_i-e_i)^2}{e_i}$。

d) 计算 P-value$=igamc(k-1,V/2)$。

e) 如果 P-value$\geqslant\alpha$，则认为待检序列通过游程分布检测。

4.4.8 块内最大"1"游程检测

a) 将待检序列 ε 划分成 $N=\left\lfloor\frac{n}{m}\right\rfloor$ 个长度为 m 的非重叠子序列，舍弃多余的位不用。本规范取 $m=$ 10 000。

b) 计算每一个子序列中最大 1 游程的长度，并将其归入相应的集合 $\{v_0,v_1,\cdots,v_5\}$。

c) 计算统计值 $V=\sum_{i=0}^{6}\frac{(v_i-N\pi_i)^2}{N\pi_i}$。其中，$v_i$ 和 π_i 的定义见附录 A.7。

d) 计算 P-value$=igamc(3,V/2)$。

e) 如果 P-value$\geqslant\alpha$，则认为待检序列通过块内最大"1"游程检测。

4.4.9 二元推导检测

a) 对待检序列 ε，依次将初始序列中相邻两个比特作异或操作得到新序列 ε'，即 $\varepsilon'_i=\varepsilon_i\oplus\varepsilon_{i+1}$。

b) 重复 a)操作 k 次。本规范取 $k=3,7$。

c) 将新序列 ε' 中的 0 和 1 分别转换成 -1 和 1，然后对其累加求和得 $S_{n-k}=\sum_{i=1}^{n-k}(2\varepsilon'_i-1)$。

d) 计算统计值 $V=\frac{|S_{n-k}|}{\sqrt{n-k}}$。

e) 计算 P-value$=erfc(|V|/\sqrt{2})$。

f) 如果 P-value$\geqslant\alpha$，则认为待检序列通过二元推导检测。

4.4.10 自相关检测

a) 计算 $A(d)=\sum_{i=0}^{n-d-1}(\varepsilon_i\oplus\varepsilon_{i+d})$。本规范取 $d=1,2,8,16$。

b) 计算统计值 $V=\frac{2(A(d)-((n-d)/2))}{\sqrt{n-d}}$。

c) 计算 P-value$=erfc(|V|/\sqrt{2})$。

d) 如果 P-value$\geqslant\alpha$，则认为待检序列通过自相关检测。

4.4.11 矩阵秩检测

a) 将待检序列 ε 分成大小为 $M*Q$ 的子序列，共有 $N=\left\lfloor\frac{n}{MQ}\right\rfloor$ 个，舍弃多余的位不用。将每一个 $M*Q$ 的子序列组装成一个 $M\times Q$ 的矩阵，此矩阵有 M 行 Q 列，每一行则由序列 ε 中连续的 Q 位填充。本规范取 $M=Q=32$。

b) 计算每一个矩阵的秩 $R_i(i=1,2,\cdots,N)$。

c) 令 F_M 为秩为 M 的矩阵的个数，令 F_{M-1} 为秩为 $M-1$ 的矩阵的个数，则 $N-F_M-F_{M-1}$ 为秩小于 $M-1$ 的矩阵的个数。

d) 计算统计值

$$V=\frac{(F_M-0.2888N)^2}{0.2888N}+\frac{(F_{M-1}-0.5776N)^2}{0.5776N}+\frac{(N-F_M-F_{M-1}-0.1336N)^2}{0.1336N}。$$

e) 计算 P-value$=igamc(1,V/2)$。

f) 如果 P-value$\geqslant\alpha$,则认为待检序列通过矩阵秩检测。

4.4.12 累加和检测

a) 将待检序列 ε 中的 0 和 1 分别转换为 -1 和 1,$X_i=2\varepsilon_i-1(1\leqslant i\leqslant n)$。

b) 计算 $S_i=S_{i-1}+X_i$,其中 $S_1=X_1$,$(1\leqslant i\leqslant n)$。

c) 计算 $Z=\max_{1\leqslant i\leqslant n}|S_i|$。

d) 计算

$$P\text{-value}=1-\sum_{i=(-(n/z)+1)/4}^{((n/z)-1)/4}\left[\Phi\left(\frac{(4i+1)z}{\sqrt{n}}\right)-\Phi\left(\frac{(4i-1)z}{\sqrt{n}}\right)\right]$$
$$+\sum_{i=(-(n/z)-3)/4}^{((n/z)-1)/4}\left[\Phi\left(\frac{(4i+3)z}{\sqrt{n}}\right)-\Phi\left(\frac{(4i+1)z}{\sqrt{n}}\right)\right]$$

e) 如果 P-value$\geqslant\alpha$,则认为待检序列通过累加和检测。

4.4.13 近似熵检测

a) 由待检序列 ε 构造一个新的序列 ε',构造方法如下:将序列 ε 最开始的 $m-1$ 位数据添加到序列 ε 的结尾即可得到 ε',新序列 ε' 的长度为 $n'=n+m-1$。本规范取 $m=2,5$。

b) 计算 ε' 中所有的 2^m 个 m 位子序列模式的出现频数,记 m 位模式 $i_1i_2\cdots i_m$ 出现的频数为 $v_{i_1i_2\cdots i_m}$。

c) 对于所有的 $j(0\leqslant j\leqslant 2^m-1)$,计算 $C_j^m=\frac{v_{i_1i_2\cdots i_m}}{n}$。

d) 计算 $\varphi^{(m)}=\sum_{i=0}^{2^m-1}C_i^m\ln C_i^m$ 。

e) 用 $m+1$ 代替 m,重复操作 a)至 d),计算得到 $\varphi^{(m+1)}$。

f) 计算 $ApEn(m)=\varphi^{(m)}-\varphi^{(m+1)}$,计算统计值 $V=2n[\ln 2-ApEn(m)]$。

g) 计算 P-value$=igamc(2^{m-1},V/2)$。

h) 如果 P-value$\geqslant\alpha$,则认为待检序列通过近似熵检测。

4.4.14 线性复杂度检测

a) 将待检序列 ε 划分为 $N=\left\lfloor\frac{n}{m}\right\rfloor$ 个长度为 m 的非重叠子序列,将多余的比特舍弃。本规范取 $m=500$。

b) 计算每一个子序列的线性复杂度 $L_i(1\leqslant i\leqslant N)$。

c) 计算 $\mu=\frac{m}{2}+\frac{9+(-1)^{m+1}}{36}-\frac{1}{2^m}\left(\frac{m}{3}+\frac{2}{9}\right)$。

d) 对每一个子序列,计算 $T_i=(-1)^m(L_i-\mu)+2/9$。

e) 设置 7 个正整数 $v_0,v_1,\cdots,v_6$,将这 7 个正整数的初值都设为 0。对所有的 $1\leqslant i\leqslant N$ 有:

如果:$T_i\leqslant -2.5$,v_0 加 1;

$-2.5<T_i\leqslant -1.5$,v_1 加 1;

$-1.5<T_i\leqslant -0.5$,v_2 加 1;

$-0.5<T_i\leqslant 0.5$,v_3 加 1;

$0.5<T_i\leqslant 1.5$,v_4 加 1;

$1.5 < T_i \leqslant 2.5$，v_5加 1；

$T_i > 2.5$，v_6加 1。

f) 计算统计值 $V=\sum_{i=0}^{6}\frac{(v_i-N\pi_i)^2}{N\pi_i}$。其中，$\pi_i$的值见附录 A.13。

g) 计算 P-value$=igamc(3,V/2)$。

h) 如果 P-value$\geqslant\alpha$，则认为待检序列通过线性复杂度检测。

4.4.15 Maurer 通用统计检测

a) 将待检序列 ε 分成两部分：初始序列和测试序列。初始序列包括 Q 个 L 位的非重叠的子序列，测试序列包括 K 个 L 位的非重叠的子序列，将多余的位(不够组成一个完整的 L 位子序列)舍弃，$K=\lfloor n/L\rfloor-Q$。本规范取 $L=7$，$Q=1\ 280$。

b) 针对初始序列，创建一个表，它以 L 位值作为表中的索引值，$T_j(1\leqslant j\leqslant 2^L)$表示表中第 j 个元素的值，计算 $T_j=i(1\leqslant i\leqslant Q)$，其中 j 是初始序列中第 i 个 L 位子序列的十进制表示。

c) 计算 $sum=\sum_{i=Q+1}^{Q+K}\log_2(i-T_j)$，其中，遍历完第 $i(Q+1\leqslant i\leqslant Q+K)$ 个 L 位子序列后，应更新 $T_j=i$。

d) 计算 $V=\frac{\frac{sum}{K}-E(L)}{\sigma}$，$E(L)$和 σ 的计算见附录 A.14。

e) 计算 P-value$=erfc(|V|/\sqrt{2})$。

f) 如果 P-value$\geqslant\alpha$，则认为待检序列通过通用统计检测。

4.4.16 离散傅立叶检测

a) 将待检序列 ε 中的 0 和 1 分别转换成 -1 和 1，得到新序列 $X_1,X_2,\cdots,X_n(X_i=2\varepsilon_i-1)$。

b) 对新序列进行傅立叶变换，得到一系列的复数 $f_1,f_2,\cdots,f_n$。

c) 对每一个 f_i，计算其系数 $\mathrm{mod}_i=modulus(f_i)=|f_i|$，这里 $i\in[0,n/2-1]$。

d) 计算门限值 $T=\sqrt{2.995\ 732\ 274n}$。

e) 计算 $N_0=0.95*n/2$。

f) 计算系数 f_i小于门限值 T 的复数个数，记作 N_1。

g) 计算统计值 $V=(N_1-N_0)/\sqrt{0.95*0.05*n/4}$。

h) 计算 P-value$=erfc(|V|/\sqrt{2})$。

i) 如果 P-value$\geqslant\alpha$，则认为待检序列通过离散傅立叶检测。

4.5 结果分析

每一个检测项目对应的具体结果分析参见附录 C。

5 随机数发生器的检测

5.1 采样

本规范建议样本数量为 1 000。

在采样过程中，应将随机数发生器产生的样本数据转换为等价的二元序列。

5.2 存储

将采集的样本按照样本长度要求，逐一存储为二进制文件。

二进制文件宜按照日期和流水号相结合的方式命名，以表明数据采集的时间和先后顺序。全部二进制文件宜存放在统一的文件目录下，且文件目录的名称应能明示样本的来源（如随机数发生器的名称、编号、采集人等）信息。

5.3 检测

对每一个样本按第4章描述的检测方法进行检测，分别得到每一个随机性检测项目的 P-value 值，记录这些结果。

5.4 判定

对于每一个随机性检测项目，统计 P-value 值不小于显著性水平 α（表示该样本通过该项检测）的样本个数。记样本数量为 s，则通过检测的样本个数应不小于 $s\left(1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{s}}\right)$。当样本数量为 1 000个时，如果通过的样本个数不小于 981，则随机数发生器通过此项检测；否则，未通过此项检测。

如果随机数发生器通过本规范规定的所有检测项目，则随机数发生器通过本规范检测；否则，未通过本规范检测。

对于使用随机数发生器的各种装置或设备，其随机性检测可参照本规范。