密码学第六次作业

1.随机数发生器

（1）： 分布均匀性、独立性　　（2）熵源

（3）：

1. 输入要求不同：PRNG通常接受一个种子（seed）作为输入，并根据该种子生成伪随机比特流。而PRF通常接受一个密钥和一个消息作为输入，并根据密钥和消息生成伪随机值。
2. 输出形式不同：PRNG的输出通常是一个比特流，可以用于生成伪随机数或密钥流等。而PRF的输出通常是一个固定长度的伪随机值，可以用于加密、认证、消息认证码等应用。
3. 安全性要求不同：PRF通常要求比PRNG更高的安全性，因为PRF的输出需要满足伪随机性、不可预测性和抗攻击性等更严格的安全性要求，以确保其在密码学应用中的安全性。

（4）：$2^n!$　　（5）：RC4　ZUC-128　雪崩效应

2.线性同余算法

（1）：

$\varphi(16)=(1-\frac{1}{2})*16=8$,根据欧拉定理知，$\forall a\in\mathbb{N}^+,(a,m)=1$,都有$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$

，我们可知，$a^8\equiv 1(\mathrm{mod}\ 16)$，而$a^4\equiv\pm 1(\mathrm{mod}\ 16)$，而验证得所有满足$\forall a\in\mathbb{N}^+,(a,m)=1$的$a$都是$a^4\equiv 1(\mathrm{mod}\ 16)$的，所以最大周期一定为4，此时a的取值可能性为：3、5、7、9、11、13、15

（2）：

$X_{n+1}=6X_n\ \mathrm{mod}\ 13$,$x=1$时产生随机序列：1,6,10,8,9,2,12,7,3,5,4,11

$X_{n+1}=7X_n\ \mathrm{mod}\ 13$,$x=1$时产生随机序列：1,7,10,5,9,11,12,6,3,8,4,2

后者有$X_{n+1}=7X_n=14(X_n/2)\ \mathrm{mod}\ 13=X_n/2\ \mathrm{mod}\ 13$，易被预测，随机性不佳

（3）：

有$a^{m-1}=1\ \mathrm{mod}\ m$，则$a^{(m-1)k}=1\ \mathrm{mod}\ m$，我们知道$\forall i<m-1,a^i\neq 1\ \mathrm{mod}\ m$

假设最大周期不是$m-1$，假设是i，那么必有$t\in\mathbb{N}^+$使得$t(m-1)=ik$，这与$gcd(k,m-1)=1$相矛盾

3.线性反馈移位寄存器

（1）：异或　高位　$c_1b_1\oplus c_2b_2\oplus\ldots c_n\oplus b_n$　$c_nx^n+c_{n-1}x^{n-1}+\ldots+c_2x^2+c_1x+1$

（2）：级数　2^n-1　000...00　始终为0

（3）：最大周期　阶　m序列

（4）：$x^5+x^3+x^2+x+1$

时刻	1级	2级	3级	4级	5级	输出
0	0	0	0	0	1	1
1	0	0	0	1	1	1
2	0	0	1	1	1	0
3	0	1	1	1	0	0
4	1	1	1	0	0	1
5	1	1	0	0	1	1
6	1	0	0	1	1	0
7	0	0	1	1	0	1
...	...	...	....	....	...	...
30	1	0	0	0	0	1
31	0	0	0	0	1	1

（5）：

$2n$位明文$m_i, i \in [1, 2n]$，密文$c_i, i \in [1, 2n]$，得到$2n$位密钥$k_i, i \in [1, 2n]$。有$n+1$种状态，$\{k_1, k_2, \ldots, k_n\}$，$\{k_2, k_3, \ldots, k_{n+1}\}$，....，$\{k_{n+1}, k_{n+2}, \ldots, k_{2n}\}$。递推关系：

$$k_{n+i} \leftarrow \{k_i, k_{i+1}, \ldots, k_{i+n-1}\}$$

线性方程组：

$$\begin{cases} k_{n+1} = k_1 c_n + k_2 c_{n-1} + \ldots + k_n c_1 \\ k_{n+2} = k_2 c_n + k_3 c_{n-1} + \ldots + k_{n+1} c_1 \\ \qquad\qquad \ldots \\ k_{2n} = k_n c_n + k_{k+1} c_{n-1} + \ldots + k_{2n-1} c_1 \end{cases}$$

这个方程组，n个方程，n个未知数（c_i），我们可以解出c_i，由$k_i = m_i \oplus c_i$可解出密钥流