1．是非判断题

(1) 序列密码（又称流密码）是属于对称密码体制。(V)

(2) 序列密码的加密/解密运算只是简单的模二加运算，所以序列密码只应用于安全保密要求不高的场合。(X)

(3) 在计算机的应用环境中，真正的随机数是不存在的。(V) 注：计算机是有限状态机

(4) 序列密码的加解密钥是由种子密钥生成的，而种子密钥的长度是由需加密的明文长度决定。(X)

(5) 在密钥序列产生器中，同样要求具备类似分组密码的设计思想，即具有混淆性和扩散性。(V)

(6) 线性反馈移位寄存器所产生的序列中，有些类如 m 序列具有良好的伪随机性，所以它可直接作为密钥序列。(X)

(7) 利用反馈移位寄存器来生成序列密码的密钥的过程中，反馈移位寄存器的初始值是由种子密钥决定的。(V)

(8) 密钥序列生成器使用非线性组合函数的目的是实现更长周期的密钥序列。(X)

注：增加前序密钥流与后续密钥流之间的复杂非线性关系，使得已知前序密钥流不能推出后续密钥流。

2．选择题

(1) m-序列本身是适宜的伪随机序列产生器，但只有在（ A ）下，破译者才不能破解这个伪随机序列。

A. 惟密文攻击　B. 已知明文攻击　C. 选择明文攻击　D. 选择密文攻击

(2) A5 算法的主要组成部分是三个长度不同的线性移位寄存器，即 A, B, C。其中 A 有（ B ）位， B 有 22 位， C 有 23 位。

A. 18　B. 19　C. 20　D. 21

(3) 按目前的计算能力，RC4 算法的种子密钥长度至少应为（ B ）才能保证安全强度。

A. 64 位　B. 128 位　C. 256 位　D. 1024 位

(4) 下面哪个序列密码是主要用于加密手机终端与基站之间传输的语音和数据。（ B ）

A. RC4　B. A5　C. SEAL　D. PKZIP

(5) n 级线性反馈移位寄存器的输出序列周期与其状态周期相等，只要选择合适的反馈函数便可使序列的周期达到最大，其最大值是（ C ）。注：不能出现全零的状态

A. n　B. 2n　C. 2^n-1　D. 不确定

(6) RC4 算法是世界上使用最广泛的序列密码之一，其可看成一个有限状态自动机，其状态决定了输出的内容，当选择 8 位-RC4 算法时，请指出生成密钥序列的最大周期是（ C ）字节。

A. 256!　B. 256^{256}　C. $256!*256^2$　D. 256^{258}

注：256 位寄存器有 256! 中状态，变量 i 和 j 各有 256 个取值范围。

(7) 国家商用密码管理办公室制定了一系列密码标准，其中（ D ）是序列密码算法。

A. SM4　B. SM7　C. SM9　D. ZCU

3．填空题

(1) 序列密码的起源可以追溯到__维尔姆密码__ 。

(2) 序列密码通常可以划分为__同步序列密码__（譬如分组密码的 OFB 模式）和__自同步序列密码__（譬如分组密码的 CFB 模式）两大类。

注：区别在于输出结果有没有反馈影响之后的输出。

(3) 序列密码的关键是在于密钥序列产生器，而密钥序列产生器一般是由__驱动器__和__非线性组合器__两个部分组成的，譬如 A5 算法。

(4) 反馈移位寄存器输出序列生成过程中，__抽头位__ 对输出周期长度的影响起着决定性的作用，而__初态__ 对输出的序列起着决定性的作用。

(5) 选择合适的 n 级线形反馈函数可使序列的周期达到最大值__2^n-1__ ，并具有 m-序列特性，但敌手知道一段长为__2n__的明密文对时即能破译这 n 级线形反馈函数。

4. 思考题

(1) 已知序列密码的密文串 101，011，0110 和相应的明文串 010，001，0001，而且还已知密钥流是使用 3 级线性反馈移位寄存器产生的，试破译该密码系统。

解：由明密文串可得密钥序列为：111，010，011，1

可得：$(0\ 1\ 0)=(c_3\ c_2\ c_1)\begin{pmatrix}1&1&1\\1&1&0\\1&0&1\end{pmatrix}$

$(c_3\ c_2\ c_1)=(0\ 1\ 0)\begin{pmatrix}1&1&1\\1&0&1\\1&1&0\end{pmatrix}=(1\ 0\ 1)$

即 $c_{i+4}=c_{i+1}+c_{i+3}$

(2) ZUC 算法，即祖冲之算法，是我国自主设计的序列密码算法，第一个成为国际密码标准的密码算法，请了解 ZUC 算法的基本思想，并简要回答以下问题：

（ⅰ）ZUC 算法的种子密钥长度是多少？

（ⅱ）ZUC 算法的密钥输出阶段，每运行一个节拍输出的密钥长度是多少比特？

（ⅲ）ZUC 算法在逻辑上采用几层结构设计，每层的主要作用是什么？

答：（ⅰ）128 比特。

（ⅱ）32

（ⅲ）3 层

上层为定义在素域 GF(2^{31} − 1) 上的线性反馈移位寄存器(LFSR)，具有 m 序列周期长、统计特性好，且在特征为 2 的有限域上是非线性的，又具有线性结构弱等特点。

中间层为比特重组，采用取半合并技术，实现 LFSR 数据单元到非线性函数 F 和密钥输出的数据转换，其主要目的是破坏 LFSR 在素域上 GF(2^{31} − 1) 上的线性结构。

下层为非线性函数 F，充分借鉴了分组密码的设计技巧，采用 S 盒和高扩散特性的线性变换 L ，非线性函数 F 具有高的抵抗区分分析、快速相关攻击和猜测确定攻击等方法的能力。