1．是非判断题

(1) 现代密码学技术现仅用于实现信息通信保密的功能。（ X ） 注：认证

(2) 密码学是对信息安全各方面的研究，能够解决所有信息安全的问题。（ X ）

注：譬如网络 Dos 攻击等

(3) 早期密码的研究基本上是秘密地进行的，而密码学的真正蓬勃发展和广泛应用源于计算机网络的普及和发展。（ V ）

(4) 古典密码大多比较简单，一般可用于手工或机械方式实现其加密和解密过程，目前破译比较容易，已很少采用，所以，了解或研究它们的设计原理是无意义的。（ X ）

(5) 在置换密码算法中，密文所包含的字符集与明文的字符集是相同的。（ V ）

(6) 多表代换密码中，明文序列的相同字母因位置不同而生成不同的密文字母，从而能够抵抗统计密码分析。（ X ） 注：能抵抗频率分析

(7) Kasiski 测试法是由普鲁士军官 Friedrich Kasiski 在 1863 年提出的一种重码分析法，主要针对多表代换密码的分析，能够确定密钥。（ X ） 注：主要用于确定密钥长度

(8) 在单表代换情况下明文与密文的重合指数 *IC* 值相同，而在多表代换情况下密文的重合指数 *IC* 较低，利用这个信息可以判断文本是用单表代换还是用多表加密的。（ V ）

2．选择题

(1) 1949 年，（ A ）发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成了一门科学。

A. Shannon　　B. Diffie　　C. Hellman　　D. Shamir

(2) 截取的攻击形式是针对信息（ A ）的攻击。

A. 机密性　　B. 完整性　　C. 认证性　　D. 不可抵赖性

(3) 篡改的攻击形式是针对信息（ B）的攻击。

A. 机密性　　B. 完整性　　C. 认证性　　D. 不可抵赖性

(4) 伪造的攻击形式是针对信息（ C ）的攻击。

A. 机密性　　B. 完整性　　C. 认证性　　D. 不可抵赖性

(5)字母频率分析法对下面哪种密码算法最有效。（ B ）

A.置换密码　B.单表代换密码　C.多表代换密码　D.序列密码

(6)重合指数法对下面哪种密码算法的破解最有效。（ C ）

A.置换密码　B.单表代换密码　C.多表代换密码　D.希尔密码

(7)维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（ C ）。

A.置换密码　B.单表代换密码　C.多表代换密码　D.序列密码

(8)下面哪种密码其明文与密文的重合指数 *IC* 值通常是不相同的。（ D ）

A.列置换密码　B.周期置换密码　C.单表代换密码　D.多表代换密码

3．填空题

(1) 信息安全的主要目标是指__机密性__、__完整性__、__认证性__和__不可否认性__、可用性。

(2) 密码学是保障__信息安全__的核心，__信息安全__是密码学研究与发展的目的。

(3) 1949 年，香农发表题为__《保密系统的通信理论》__，为密码系统建立了理论基础，从

此密码学成了一门科学。

(4) 密码学的发展大致经历了两个阶段：__古典密码阶段__、__现代密码阶段__。

(5) 1976 年，W. Diffie 和 M. Hellman 在__《密码学的新方向》__一文中提出了公开密钥密码的思想，从而开创了现代密码学的新领域。

(6) 密码学的发展过程中，两个质的飞跃分别指__1949 年 Shannon 发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成了一门科学。__和 __1976 年，Diffe 和 Hellman 发表了《密码学的新方向》，提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元__。 还有两次具有**重要意义的标志性事件**？

(7)在 1949 年香农发表“保密系统的通信理论”之前，密码学算法主要通过字符间的__置换__和__代换__实现，一般认为这些密码体制属于古典密码学范畴。

(8)代换是古典密码体制中最基本的处理技巧，按照一个明文字母是否总是被一个固定的字母代替进行划分，代换密码主要分为两类：__单表代换__和__多表代换__。

(9)从重合指数的定义可知，一个完全随机的文本其 IC 约为__0.0385__，而一个有意义的英文文本其 IC 却是__0.065__左右，两者的差异是很明显的。

4．思考题

Enigma 密码机的出现是近代密码发展史中里程碑的事件，也引发了这场旷日持久的密码战。请上网查询有关 Enigma 密码机的资料，了解 Enigma 密码机的兴衰史，从中你得到的启示有哪些？请在密码方面进行简要总结。

这是一道灵活题，内容非常多，下面未必全面，只要意思合理，能说出 5 点即可。

Enigma 密码机是一款成功的密码设备，之所以能广泛使用，具有以下特点：安全、快速、使用方便、成本低。这也是目前一个实用密码设备应必备的特点。

从 Enigma 密码机的兴衰史中，可得到如下启示：

科学技术的发展，是密码学得以前进发展的基石；

Enigma 密码机的出现源于当时机械设备、电等技术工具

密码学的发展，促进新科学技术的出现；

破译 Enigma 密码机的“巨人”就是计算机的“雏形”

实际需求是推动密码学前进的最大动力；

“二战”时期军事信息重要性使得迫切需要密码设备

密码编码和密码分析，两者既彼此对抗，有相互促进；

矛与盾的关系

在密码对抗中，人的因素是第一位的；

打造转轮密码机鼎盛王朝的“开国功臣”**谢尔比乌斯**(德国)，首开破译机器密码记录的“平乱先锋”**雷耶夫斯基**(波兰)，奠定机械化破译基础的“科学先知”**图灵**(英国)

密码系统的保密性只应建立在密钥的保密上；

密码算法终有一天会被对手得到，比如奸细、战场失败密码设备被缴获等

复合密码体制更有利于增强算法的安全性；

Enigma 密码机既有单表代换又有多表代换

密码设备是武器装备，军队不可或缺的装备；

密码设备配发到各部队，出口受到严格限制

任何密码设备或算法不可能永不被攻破的；

号称“不可破译”的 Enigma 密码机最终以被破译收场。

在某方面应用中，密码技术能成为关键技术；

纳粹德国的海军将领邓尼茨的“群狼战术”在二战名噪一时，依赖的就是 Enigma 密码机密码设备的失败有时可能会改变时局或战局。
二战时期的“中途岛战役”说明这一点。