注：自学教材第 2 章 2.1 节内容，再结合第三讲课件，回答如下问题：

1．是非判断题

(1) 现在使用大多数密码系统的安全性都是从理论上证明它是不可攻破的。(X)

(2) 从理论上讲，穷举攻击可以破解任何密码系统，包括“一次一密”密码系统。(X)

(3) 设计密码系统的目标就是使其达到无条件保密。(X) 注：计算上安全

(4) 任何一个密码体制都可以通过迭代来提高其安全强度。(X) 注：要求包含非线性部分

(5) 按照现代密码体制的原则，密码分析者如果能够找到秘密密钥，那么，他就能够利用密文恢复出其明文。(V)

(6) 现代密码系统的安全性不应取决于不易改变的算法，而应取决于可随时改变的密钥。(V)

(7) 能经受住已知明文攻击的密码体制就能经受住选择明文攻击。(X)

2．选择题

(1) 一个密码系统至少由明文、密文、加密算法和解密算法、密钥五部分组成，而其安全性是由（ D ）决定的。

A. 加密算法　　B. 解密算法　　C. 加密算法和解密算法　　D. 密钥

(2) 密码分析者通过各种手段掌握了相当数量的明-密文对可供利用，这种密码分析方法是（ B ）。 注：C 是所要求的明密文对

A. 只有密文攻击　　B. 已知明文的攻击　　C. 选择明文攻击　　D. 选择密文攻击

(3) 一般来说，按照密码分析的方法，密码系统至少经得起的攻击是(A)。

A. 唯密文攻击　　B. 已知明文的攻击　　C. 选择密文攻击　　D. 选择文本攻击

(4) 计算复杂性是密码分析技术中分析计算量和研究破译密码的固有难度的基础，算法的运行时间为难解的是（ D ）。

A．$O(1)$　　B．$O(n)$　　C．$O(n^2)$　　D．$O(2^n)$

(5) 计算出或估计出破译一个密码系统的计算量下限，利用已有的最好方法破译它所需要的代价超出了破译者的破译能力（诸如时间、空间、资金等资源），那么该密码系统的安全性是（ A ）。

A. 实际安全　　B. 条件安全　　C. 可证明安全　　D. 无条件安全

3．填空题

(1) 密码学(Cryptology)是研究信息及信息系统安全的科学，密码学又分为__密码编码__学和_密码分析_学。

(2) 一个密码系统一般是__明文__、___密文__、___加密算法_、__解密算法_、___加密密钥__、__解密密钥__六部分组成的。

(3) 密码体制是指实现加密和解密功能的密码方案，从使用密钥策略上，可分为__对称密码体制__和__非对称密码体制(或公钥密码体制)____。

(4) 对称密码体制又称为_单密钥_密码体制，它包括__分组_密码和_序列_密码。

(5) 认证通信系统模型中，目前广泛使用的基于对称认证体制主要是__消息认证码__，非对称的消息认证技术代表为__数字签名__。

(6) 密码的强度是破译该密码所用的算法的计算复杂性决定的，而算法的计算复杂性由它所

需的 时间 、 空间 来度量。

(7) 在密码学中，密码设计者都希望对其密码算法的任何攻击算法具有 亚指数级 或 指数级 的复杂度。

4. 思考题

1. 请简要说明对称密码体制和公钥密码体制各自的优势和不足。

对称密码体制的优势(相对公钥密码体制)

加解密速度快、性能高；

密钥短；

没有数据扩展，即明文和密文长度一样。

对称密码体制的不足(相对对称密码体制)

密钥分发需要安全通道；

密钥量打，难以管理；

难以解决不可否认的问题。

公钥密码体制的优势(相对对称密码体制)

密钥分发简单；

需秘密保存的密钥量减少，密钥管理容易；

可以实现数字签名功能。

公钥密码体制的不足(相对对称密码体制)

加解密速度慢；

密钥长；

有数据扩展，即明文和密文长度不一样。

2. 请简要说明密码算法公开的意义。

(1) **有利于增强密码算法的安全性；**

接受大众检验，尤其专业密码分析人员的检验。

(2) **有利于密码技术的推广应用；**

使用相同密码算法的人或集体才能实现保密通信。

(3) **有利于增加用户使用的信心；**

即使密码算法设计者没有密钥也不能破译。

(4) **有利于密码技术的发展。**

公开密码设计思想，密码设计者可取长补相互，设计更好的密码算法。

3. 假设你使用的计算机具有如下能力：

(1) 每台计算机每秒可尝试 1 百万个密钥。

(2) 共有 100 万台计算机参与并行使用。

那么，遍历 64 比特和 128 比特的密钥分别**大约**需要多少年？(要求简要过程)

注： $2^{10}\approx10^3$

1 年=356*24*3600≈$3*10^7$ 秒

1 年遍历密钥个数≈$3*10^{19}$

$2^{64}\approx10^{19.2}$

$2^{128}\approx10^{38.4}$

年数≈1

年数≈10^{18}

4. 密码学的运算都是模运算，模运算与整数运算最大不同在于除法，

譬如 a/b mod p=a*b^{-1} mod p，b^{-1} 是 b mod p 的逆元，问题：

(1) 请说明 b mod p 的逆元的存在性。

对于整数 a、p，如果存在整数 b，满足 ab mod p =1，则 b 是 a 的模 p 乘法逆元。

定理： a 存在模 p 的乘法逆元的充要条件是 gcd(a，p) = 1

证明：

首先证明充分性

如果 gcd(a，p) = 1，根据欧拉定理，$a^{\phi(p)} \equiv 1 \bmod p$，因此，$a^{\phi(p)-1} \bmod p$ 是 a 的模 p 乘法逆元。

再证明必要性

假设存在 a 模 p 的乘法逆元为 b，ab ≡ 1 mod p

则 ab = kp +1 ，1 = ab − kp

因此，gcd(a，p) = 1， gcd(b，p) = 1。

(2) 请掌握一种求逆元的方法，并用这方法求 13 mod 120 的逆元。

已知整数 a、b，扩展欧几里得算法可以在求得 a、b 的最大公约数的同时，能找到整数 x、y（其中一个很可能是负数），使它们满足等式：gcd(a,b)=ax+by

如果 gcd(a,p)=1,求满足 ab≡1(mod p)的 b,即 a 的逆元。

找到满足等式：px+ay=1 中的 x 和 y，即得 a 的逆元为 y。

介绍一种求逆元的方法：

$$\begin{pmatrix} a \\ b \end{pmatrix} = \prod_{i=0}^{N} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix}.$$

其中：q_i 是商，r_{N-1} 是余数，由于 a 与 b 互素，r_{N-1} 是 1。

$$\begin{pmatrix} 120 \\ 13 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 13 & 4 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 120 & 37 \\ 13 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} -4 & 37 \\ 13 & -120 \end{pmatrix} \begin{pmatrix} 120 \\ 13 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

得：-4*120+37*13=1，即 13 mod 120 的逆元是 37。