**(by zzw4257)**

# 浙江大学
# 《数据安全与密码学基础》课程期中考试卷

课程代码：21192050　　授课课时：48　　考试用时：90 分钟
课程名称：**数据安全与密码学基础**　　适用对象：一群可怜人
试卷命题人：张聪　　试卷审核人：Unknown

---

## 一、选择题（各 5 分）

1. Kerckhoffs 准则强调，一个密码系统的安全性主要取决于以下哪个因素？

   - A. 算法的复杂性
   - B. 算法的保密性
   - C. 密钥的保密性
   - D. 加密设备的安全性

2. 香农安全和完美安全的关系？

   - A. 香农安全强于完美安全
   - B. 香农安全弱于完美安全
   - C. 二者等价
   - D. 不可比较

3. （多选）可忽略函数的定义为：对于任意多项式 $p(n)$ 以及所有足够大的 $n$ 值，满足 $f(n) \leq \frac{1}{p(n)}$。下列函数是可忽略函数的有？

   - A. $2^{-n}$
   - B. $2^{-\sqrt{n}}$
   - C. $n^{-\log n}$
   - D. $n^{-5}$

4. （多选）$\varepsilon = (E, D)$ 是定义在 $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^2$ 上的 One-timePad 加密方案。现对加密算法 $E$ 进行如下 4 种修改，选出修改后仍然安全的加密方案。

   - A. $E_1(k, m) = 0 \parallel E(k, m)$
   - B. $E_2(k, m) = E(k, m) \parallel \text{parity}(m)$
   - C. $E_3(k, m) = \text{reverse}(E(k, m))$
   - D. $E_4(k, m) = E(k, \text{reverse}(m))$

## 二、填空题（各 5 分）

5. 在密码学中,凯撒密码是一种最简单且最广为人知的加密技术。已知加密算法 $Enc_k(m_1 \cdots m_l) = c_1 \cdots c_l$，$c_i = (m_i + 3) \mod 26$，对于消息 $m =$ "lovezju"，计算 $c = Enc_k(m) =$ _____

6. $Func_n$ 表示将 $n$ 位字符串映射到 $n$ 位字符串的所有函数的集合，计算该集合大小 $|Func_n| =$ _____

7. 根据移位密码的定义，我们有 $\mathcal{K} = \{0, \cdots, 25\}$，对于每个 $k \in \mathcal{K}$，$Pr[K = k] = \frac{1}{26}$。假设 $\mathcal{M}$ 的分布如下：$Pr[M = a] = 0.7$，$Pr[M = z] = 0.3$，则 $Pr[C = b] =$ _____

8. 加密方案 $(KG, Enc, Dec)$ 是完美安全的，其明文空间 $M$ 和密钥空间 $\mathcal{K}$ 必须满足什么大小关系：$|\mathcal{K}|$_____$|\mathcal{M}|$

## 三、计算题 (10 分)

依照某标准，一安全的登录系统其登录口令应具有 16 bit 熵。请判断下述口令生成策略是否满足该标准

**策略**：生成 8 字节的字符串口令 str，每个字符由不同信源产生。其中第 1 个字符从集合 $\{x, y\}$ 中均匀选取，第 2-4 个字符从集合 $\{a, b, c, d, e\}$ 中均匀独立选取，第 5 8 个字符从集合 $\{@, \#, \&, \%\}$ 中均匀独立选取。

**提示**：若字符 U 有 n 种取值：$U_1 \cdots U_n$，对应概率为：$p_1 \cdots p_n$，则 $U$ 的熵 $H(U) = -\sum_{i=1}^{n} p_i \log_2 p_i$。

## 四、主观题（20 分）

1. 形式化描述密码学中 EAV Security（indistinguishable encryptions in the presence of an eavesdropper）的定义。(10 分)

2. 定义一个消息长度为 $\ell$ 的加密方案 $(KG, Enc, Dec)$ 如下，其中明文空间 $M = \{0,1\}^\ell$，密文空间 $\mathcal{C} = \{0,1\}^\ell$，密钥空间 $\mathcal{K} = \{0,1\}^n$，$G : \{0,1\}^n \to \{0,1\}^p$ 为一函数，

- 密钥生成算法 $KG(1^n) \to k$
- 加密算法 $Enc(k, m) = G(k) \oplus m$
- 解密算法 $Dec(k, c) = G(k) \oplus c$

请用归约的方法证明以下定理：若 $G$ 是一个带扩展因子 $\alpha$ 的伪随机数生成器，则加密方案 $(KG, Enc, Dec)$ 是 EAV Security。只需画出归约的图即可：(10 分)

## 五、主观题 (15 分)

请证明以下加密方案 $(KG, Enc, Dec)$ 是完美安全的，已知 $p$ 是 $n$ bit 长的素数，明文空间 $M = \{0,1\}^n$，密文空间 $C = \{0,1\}^n$，密钥空间 $\mathcal{K} = \{1, \cdots, p-1\}$

- 密钥生成算法 $KG(1^n) \to k$

- 加密算法 $Enc(k,m) = k \cdot m \mod p$
- 解密算法 $Dec(k,c) = k^{-1} \cdot c \bmod p$，其中 $k \cdot k^{-1} = 1 \mod p$

提示：加密方案 $(KG, Enc, Dec)$ 是完美安全当且仅当：

$$Pr[k \leftarrow KG(1^n); Enc_k(m_1) = c] = Pr[k \leftarrow KG(1^n); Enc_k(m_2) = c]$$

## 六、主观题 (15 分)

F 是一个定义在 $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$ 上安全的伪随机函数，$\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$，对伪随机函数 $F$ 进行如下修改，得到的还是安全的伪随机函数吗？简单描述理由即可

- $F_1(k,x) = F(k,x)||0$
- $F_2(k,x) = F(k,x)||x$
- $F_3(k,x) = F(k,x) \oplus x$