EIT-ex12-information security based on IT  
1. 解释密码安全性的内涵.

答：密码系统有两种安全性标准:

一是无条件安全性(理论安全性、完善保密性、完全保密性)，指破译者具有无限时间、截获足够多的密文、具有无限计算资源下的抗破译能力;

二是实用安全性，指在破译者仅有一定计算资源及其它实际限制下的抗破译能力。可分为计算安全性和可证明安全性。

一个安全的密码系统通常应满足以下条件:  
 (1).系统即使不是理论上不可破译,至少也应当是实用上不可破译;  
 (2).系统保密性不是依赖于加密算法与解密算法，而是依赖于密钥的保密性;  
 (3).加密运算、解密运算简单快速、易于实现;  
 (4).密钥量适中，密钥的分配、管理方便。

2. 分别用概率论和信息论解释完善保密性(perfect secrecy)的内涵.

答：

概率论：密码系统(M,B,K,,)（（message，密文空间，密钥空间，带参数的加密变换，带参数的解密变换））称为完全保密，是指对一切有.

信息论：密码系统(M,B,K,,)（（明文空间，密文空间，密钥空间，带参数的加密变换，带参数的解密变换））称为完全保密，是指对明文空间和密文空间而言，有I(M;B)=I(B;M)=0.

3. 证明:对于完善保密系统而言,密钥空间的大小不小于明文空间的大小.

证明：

且当i≠j时，（否则对于不同明文将变换成同一密文，与“编码

变换是一一对应的”相矛盾）.

从而加密变换数不会小于明文数目，即密钥空间的大小不小于明文空间的大小.

4. 证明:存在完善保密系统.

证明：完善保密的密码体制是存在的。

比如，当明文P＝（x1，x2，x3……xn）是n比特长的均匀分布随机变量，密钥K＝（k1，k2，k3……kn）也是n比特长的均匀分布随机变量，加密算法为C＝P⊕K，其中 ⊕ 为逐比特异或运算。由于 ⊕ 是群运算，故容易看出C是n比特长的均匀分布随机变量，且P和C相互独立。