eit_ex14_AES

1. 解释对称密码体制。
2. 以 AES 为例，解释对称密码体制的设计思想。
3. 从中间状态数据与轮密钥的叠加，能否将 AES 解释为完全保密系统?
4. 字节替换是否改变熵?
5. 行移位是否改变熵?
6. 列混合是否改变熵?