# 密码学基础-作业2

提交截止时间：2022年10月14日01：00； 提交方式：通过HITsz Grade平台提交

提交格式：pdf文件 文件命名规则：【学号\_姓名\_作业2.pdf】

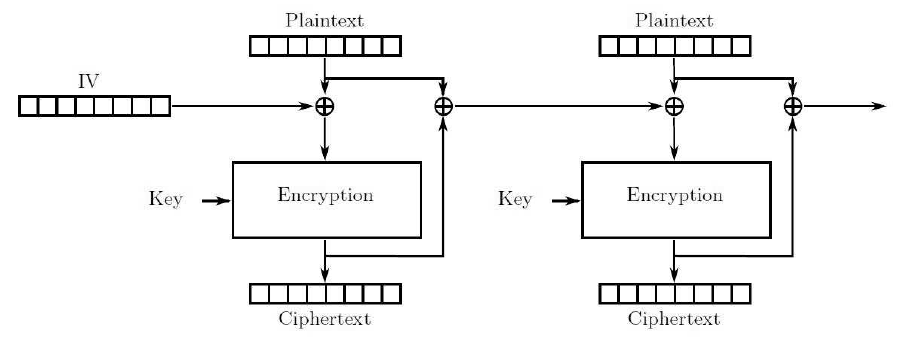
注：如包含照片或插图，请旋转至适合阅读的方向

1. 考虑如下的分组密码：使用移位密码（shift cipher）作为分组密码，其输入输出都为比特。令移位密码的秘钥为，需要加密的明文。下表给出了字母和对应4-比特二进制串的转换方法（注意本题字母表只有16个字母，而非26个。因此，示例：当秘钥时，）。请使用分组密码的CBC模式对明文P进行加密，设初始向量IV=0101，给出具体加密步骤以及最终加密结果。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H |
| 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| I | J | K | L | M | N | O | P |
| 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |

1. 考虑如下分组加密操作模式，并回答以下问题：



1. 请画图说明密文的解密过程。（所画图中应至少包含两个分组）
2. 请利用如下符号：，，，，（秘钥下的分组加密操作）和（秘钥下的分组解密操作），根据图示写出加密与解密的公式。例如，在课件中CBC的对应公式如下：

请按照同样的格式给出上述加密与解密的对应公式。

1. 假设一个密文分组被更改/损坏（由于噪声或恶意破坏）。 这将如何影响解密？ 解密后会影响多少个明文分组？
2. 现有一个系统采用流密码加密其传输的数据。
   1. 假设使用密钥流 来加密明文数据 （所有数字都是十六进制数）。请写出加密后的密文，用十六进制表示。
   2. 假设有一个敌手能够窃听传输的消息，但他不知道明文和密钥流。现在他想通过篡改密文的方式改变消息，使得接收者解密之后的明文为 ，请问他如何做到？
3. 设一个5级线性反馈移位寄存器（LFSR）的特征多项式为。
   1. 画出该LFSR的框图；
   2. 给出输出序列的递推关系；
   3. 设初始状态，写出输出序列。