AES

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4比特。令移位密码的秘钥k为3，需要加密的明文P 为 IAMFINE。

   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）。示例：当秘钥$k = 3$时，$E_k(P) = C$。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

答：

首先查表将明文 P 代换成 4-比特二进制串：

$$P = IAMFINE = 1000\ 0000\ 1100\ 0101\ 1000\ 1101\ 0100$$

由于秘钥$k = 3$，那么加密一个字母X的结果（即$E_k(X)$），便是将X在字母表中右移3位所得的字母。

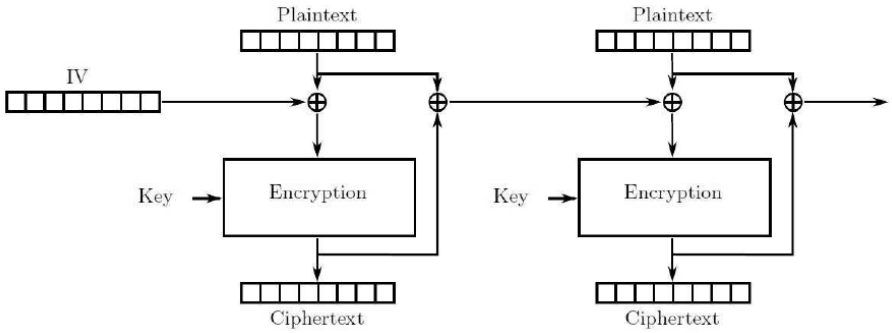
接下来用 CBC 模式对明文P加密：

$$C_0 = E_k(IV \oplus P_0) = E_k(0101 \oplus 1000) = E_k(1101) = E_k(N) = A$$
$$C_1 = E_k(C_0 \oplus P_1) = E_k(0000 \oplus 0000) = E_k(0000) = E_k(A) = D$$
$$C_2 = E_k(C_1 \oplus P_2) = E_k(0011 \oplus 1100) = E_k(1111) = E_k(P) = C$$
$$C_3 = E_k(C_2 \oplus P_3) = E_k(0010 \oplus 0101) = E_k(0111) = E_k(H) = K$$
$$C_4 = E_k(C_3 \oplus P_4) = E_k(1010 \oplus 1000) = E_k(0010) = E_k(C) = F$$
$$C_5 = E_k(C_4 \oplus P_5) = E_k(0101 \oplus 1101) = E_k(1000) = E_k(I) = L$$
$$C_6 = E_k(C_5 \oplus P_6) = E_k(1011 \oplus 0100) = E_k(1111) = E_k(P) = C$$

因此加密 P 得到的密文为ADCKFLC。

分组密码操作模式

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：C_N，P_N，C_{N-1}，P_{N-1}，$E_K(\cdot)$（秘钥K下的分组加密操作）和$D_K(\cdot)$（秘钥K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：

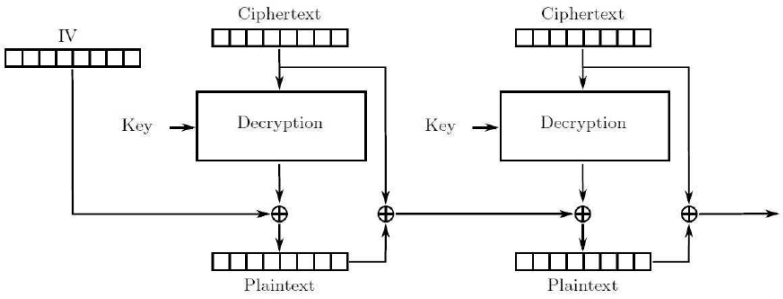
$$C_N = E_K(C_{N-1} \oplus P_N) \qquad C_0 = IV$$
$$P_N = C_{N-1} \oplus D_K(C_N) \qquad C_0 = IV$$

请按照同样的格式给出上述加密与解密的对应公式。

（3） 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？

答：

（1） 解密过程图示如下：



（2） 对应的加密解密公式如下：

$$C_N = E_K\left(P_N \oplus (C_{N-1} \oplus P_{N-1})\right) \qquad C_0 \oplus P_0 = IV$$

$$P_N = D_K(C_N) \oplus (C_{N-1} \oplus P_{N-1}) \qquad C_0 \oplus P_0 = IV$$

（3） 一个损坏的密文分组将破坏所有后续分组的解密，即错误将无限传播，导致后续所有明文分组无法正确解密。这与 CBC 不同，CBC 解密过程中，一个错误的密文分组只会影响两个明文分组。

随机数和流密码

1. 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 $0x1234$ 来加密明文数据 $0xABCD$ （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 $0xA5CD$ ，请问他如何做到？

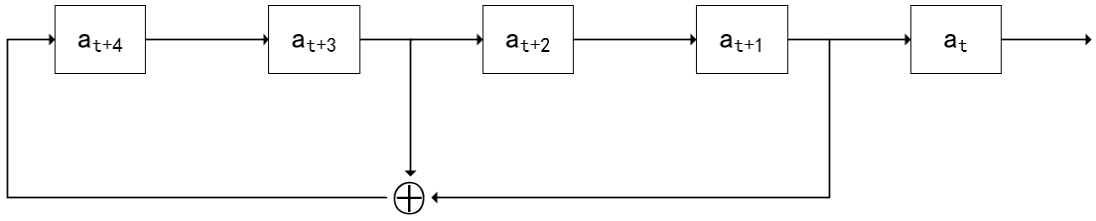
答：（1）加密过程如下：

$$\begin{array}{cccc} 1010 & 1011 & 1100 & 1101 \\ \oplus\ 0001 & 0010 & 0011 & 0100 \\ \hline 1011 & 1001 & 1111 & 1001 \end{array}$$

因此密文为 $0xB9F9$ 。
（2）敌手可以将密文的第二位与 E(1110) 异或，新的密文是$1001 \oplus 1110 = 0111$，解密之后是$0111 \oplus 0010 = 0101 = 5$。

2. 设一个 5 级线性反馈移位寄存器(LFSR)的特征多项式为$f(x) = 1 + x^2 + x^4$。
   （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$(a_1, a_2, a_3, a_4, a_5) = (1,0,0,1,1)$，写出输出序列。

答：（1）该 LFSR 的框图为：



(2) $a_{n+t} = a_{t+3} \oplus a_{t+1}, t \geq 1$
(3) 10011110011……