

《密码学》课程习题

执笔 张焕国

第三章习题

- 1、说明在 DES 中 S 盒的安全作用。
- 2、说明在 DES 中 P 置换的安全作用。
- 3、证明 DES 的可逆性和对合性。
- 4、分析 DES 的弱密钥和半弱密钥。
- 5、分析 DES 的互补对称性。
- 6、画出 2DES 的框图，试分析其安全性（提示：考虑中间相遇攻击）。
- 7、画出 3 密钥 3DES 的框图。
- 8、大作业：以 3DES 作为加密算法开发出文件加密软件系统，软件要求如下：
 - ①具有文件加密和解密功能；
 - ②具有加解密速度统计功能；
 - ③采用密文反馈链接和密文挪用短块处理技术；
 - ④具有较好的人机界面。
- 9、分析 SKIPJACK 的弱密钥。
- 10、证明：在 SKIPJACK 密码算法中
 - 1 解密轮函数 1 是加密论函数 1 的逆。
 - 2 解密轮函数 2 是加密论函数 2 的逆。
- 11、证明 SKIPJACK 的加解密算法是互逆的。

- 12、 证明 SKIPJACK 密码算法种加密函数 F 与逆加密函数 F^{-1} 是互逆的。
- 13、 编程实现 SKIPJACK 的加解密算法。
- 14、 分析 IDEA 的弱密钥。
- 15、 实现 IDEA 密码 $r = a \odot b$ 运算的伪代码如下（ c 为 32 位无符号数，返

回结果为 $(r \text{ AND } 0xFFFF)$) :

```

if (a=0)  $r \leftarrow (0x10001 - b)$ 
    else if (b=0)  $r \leftarrow (0x10001 - a)$ 
        else {  $c \leftarrow a \cdot b$ ;

                 $r \leftarrow ((c \text{ AND } 0xFFFF) - (c \gg 16))$ ;
                if ( $r < 0$ )  $r \leftarrow (0x10001 + r)$ 
            }
endif

```

分析说明其数学原理。

- 16、 编程实现 IDEA 密码算法。
- 17、 比较 AES 和 DES，说明它们各有什么特点？
- 18、 AES 的解密算法与加密算法有什么不同？
- 19、 在 $GF(2^8)$ 中，01 的逆元素是什么？
- 20、 在 AES 中，对于字节 “00”和 “01”计算 S 盒的输出。
- 21、 证明：模 x^4+1 ， $c(x)$ 与 $d(x)$ 互逆。
- 22、 证明： $x^i \bmod (x^4+1) = x^{i \bmod 4}$ 。
- 23、 利用 AES 的对数表或反对数表计算 ByteSub(25)。
- 24、 求出 AES 的 S 盒的逆矩阵。
- 25、 设 S 是状态， W 是圈密钥：

①证明： $\text{InvShiftRow}(\text{InvByteSub}(S)) = \text{InvByteSub}(\text{InvShiftRow}(S))$ 。

② 证 明 : $\text{InvMixColumn}(S \oplus W) = \text{InvMixColumn}(S) \oplus \text{InvMixColumn}(W)$ 。

③说明上述结论对 AES 解密算法的设计有何作用。

26、 大作业：以 AES 作为加密算法开发出文件加密软件系统，软件要求如下：

- ①具有文件加密和解密功能；
- ②具有加解密速度统计功能；
- ③采用密文反馈链接和密文挪用短块处理技术；
- ④具有较好的人机界面。

27、 编程实现 KASUMI 密码算法。

28、 KASUMI 密码算法是对合运算吗？试证明。

29、 大作业：以 SMS4 作为加密算法开发出文件加密软件系统，软件要求如下：

- ①具有文件加密和解密功能；
- ②具有加解密速度统计功能；
- ③采用密文反馈链接和密文挪用短块处理技术；
- ④具有较好的人机界面。

30、 比较 SMS4 和 AES，说明它们各有什么特点？

31、 计算机数据加密有些什么特殊问题？它对加密的安全性有什么影响？

32、 分析 ECB、CBC、CFB、OFB、X CBC、CTR 工作模式的加解密错误传播情况。

- 33、 画出 CFB 模式的加解密框图。
- 34、 为什么说填充法不适合计算机文件和数据库加密应用？
- 35、 密文挪用方法有什么优缺点？