密码技术竞赛常考点

基本知识

ZUC序列密码

内容	数据
单次输出密钥长度	32比特
密钥长度	128比特
初始向量长度	128比特
初始化迭代轮数	32轮
密钥装载LFSR时所需装入常数个数	16个

SM2加密算法

内容	数据
2048比特密文对应明文长度	1280比特
基域选择Fp-256时私钥长度	256比特
基域选择Fp-256时数字签名长度	512比特
推荐密钥长度	256比特
基域选择Fp-256时数字签名私钥长度	256比特
基域选择Fp-256时数字签名公钥长度	512比特

SM3加密算法

内容	数据
输入448比特消息生成杂凑值所需调用压缩函数次数	2次
链接变量长度	256比特
消息分组长度	512比特
压缩函数输入	768比特
压缩函数	64轮
压缩函数不同的布尔函数总数	2种
可以的压缩长度比特数	2^32; 2^48
输入的最大消息长度不超过	2^64比特
轮函数每次更新字数（若为布尔函数输出字数则不正确）	2个

SM4加密算法（分组密码）

内容	数据
分组属性值（IPSec VPN 协议）	129
密钥长度	128比特
明文长度	128比特
明文分组长度	128比特
S盒输入	8位
S盒输出	8位
轮密钥长度	32位
迭代轮数	32轮
分组长度为128比特时密钥长度	128比特
采用SM4的CBC-MAC输出标签不支持	256比特

DES加密算法

内容	数据
密钥长度（有效位数）	56位
迭代次数	16次
标准分组长度	64位
S盒数量	8个
子密钥长度	48位

AES加密算法

内容	数据
加密轮数（密钥长度256位，分组长度128位）	14
轮密钥长度	128位
允许的分组密钥长度	128，192，256比特

MD5算法

内容	数据
输出杂凑值长度	128比特
HASH算法MD5摘要长度	128位

内容	数据
处理过程轮数	4轮

Rijndael算法

内容	数据
分组长度	128位/192位/256位
密钥长度	128位/192位/256位

SHA-1算法

内容	数据
输出（报文）杂凑值长度	160比特

IDEA算法

内容	数据
加密轮次（迭代轮数）	8轮
加密所需子密钥	52个
分组长度	64比特
密钥长度	128比特

Skipjack算法

内容	数据
密钥长度	80位
迭代次数	32次

Camellia算法

内容	数据
密钥长度可为	128比特/192比特/256比特
加解密轮数可为	18轮/24轮

SM3 vs SHA-256

内容	是否相同
结构	√

内容	是否相同
压缩函数结构	√
消息填充方式	√
消息扩展方式	×
压缩函数使用的布尔函数	×
消息字介入方式	×

分组密码

题库

1.以下哪种分组密码的工作模式类似于流密码（ ）。

```
A.CFB
B.CBC
C.CTR
D.OFB
```

CD

2.下列分组密码工作模式中，加密串行解密可并行的是（ ）。

```
A.CBC
B.OFB
C.CFB
D.CTR
```

AC

3.以下分组密码算法的工作模式IV要求每个消息必须唯一，不能重用，且不可预测的是（ ）。

```
A.OFB
B.CFB
C.CBC
D.GCM
```

BC

4.下列属于分组密码的主要模式是（ ）。

```
A.ECB
B.CBC
C.CFB
D.OFB
```

ABCD

4.对称密码算法中的加密模式有（ ）。

```
A.ECB
B.CBC
C.CFB
D.OFB
```

ABCD

5.下列分组密码加密模式中，加密过程具备错误扩散的有（ ）。

```
A.CBC
B.ECB
C.CTR
D.OFB
```

AD

6.DES分组模式有( )?

```
A.ECB
B.CBC
C.CFB
D.OFB
```

ABCD

7.以下分组密码算法工作模式不需要填充的是（ ）。

```
A.CTR
B.CFB
C.CBC
D.OFB
```

ABD

8.GM/T 0006《密码应用标识规范》定义的标识中，不包括以下哪种分组密码工作模式？（ ）

```
A.ECB
B.CBC
C.CFB
D.CTR
```

D

附：分组密码模式比较表

来源：《图解密码技术》（日）结城浩 人民邮电出版社 2014 P93-94

模式	名称	优点	缺点	备注
ECB模式	Electronic Code Book 电子密码本模式	○简单 ○快速 ○支持并行计算	○明文中的重复排列会反映在密文中 ○通过删除、替换密文分组可以对明文进行操作 ○对包含某些比特错误的密文进行解密时，对应的分组会出错 ○不能抵御重放攻击	不应使用
CBC模式	Cipher Block Chaining 密文分组模式	○明文的重复排列不会反映在密文中 ○支持并行计算（仅解密） ○能够解密任意密文分组	○对包含某些错误比特的密文进行解密时，第一个分组的全部比特以及后一个分组的相应比特会出错 ○加密不支持并行计算	推荐使用
CFB模式	Cipher-FeedBack 密文反馈模式	○不需要填充（padding） ○支持并行计算（仅解密） ○能够解密任意密文分组	○加密不支持并行计算 ○对包含某些错误比特的密文进行解密时，第一个分组的全部比特以及后一个分组的相应比特会出错 ○不能抵御重放攻击	○现在已不使用 ○推荐用CTR模式代替
OFB模式	Output-FeedBack 输出反馈模式	○不需要填充（padding） ○可事先进行加密、解密的准备 ○加密、解密使用相同结构 ○对包含某些错误比特的密文进行解密时，只有明文中相对应的比特会出错	○不支持并行计算 ○主动攻击者反转密文分组中的某些比特时，明文分组中相对应的比特也会被反转	推荐用CTR模式代替
CTR模式	CounTeR 计数器模式	○不需要填充（padding） ○可实现进行加密、解密的准备 ○加密、解密使用相同结构 ○对包含某些错误比特的密文进行解密时，只有明文中相对应的比特会出错 ○支持并行计算（加密、解密）	主动攻击者反转密文分组中的某些比特时，明文分组中相对应的比特也会被反转	推荐使用

SM9

1.SM9公钥加密算法消息封装机制包括基于KDF的序列密码及结合KDF的分组密码算法两种类型。

正确　　错误

2.SM9公钥加密算法是密钥封装机制和消息封装机制的结合。

正确　　错误

3.SM9密码算法的主公钥由KGC通过随机数发生器产生。

正确　　**错误**

4.SM9密码算法的用户私钥由KGC通过随机数发生器产生。

正确　　**错误**

5.SM9密钥封装机制封装的秘密密钥由解封装用户使用主私钥进行解密。

正确　　**错误**

其他

基于口令的密钥派生函数 PBKDF ,盐值为不小于 64 比特的随机比特串，迭代次数不小于**1024**次。
RSA算法**可以**用于数字签名哦。
GM/T 0009《SM2密码算法使用规范》中，长度为32字节的数据包括 A.SM2签名结果中的R B.Z值
D.SM2签名的输入数据。
GM/T 0006《密码应用标识规范》中的标识符采用**32**位无符号整数类型。
GM/T 0015《基于SM2密码算法的数字证书格式规范》中，颁发者Issuer中AttributeValue部分首选的编码类型是**UTF8String**
GM/T 0009《SM2密码算法使用规范》中，用户身份标识ID的默认值的长度为**16**个字节。
SEAL算法本身通过**4**次迭代来改变**8**个内部寄存器的值，每个迭代包括**32**轮。
GM/T 0035《射频识别系统密码应用技术要求》第5部分，分散因子长度不小于**4字节**。
SEAL算法本身通过**4**次迭代来改变**8**个内部寄存器的值，每个迭代包括**64**轮。