在RSA加密体制中，取p=7,q=11,公钥e=13,则密文41所对应的明文为

- 41
- 62
- 71
- 13

在背包公钥密码体制中，设超递增背包A=(3,13,29,61,147)，取M=383,U=311,则密文517所对应的明文为

- 19
- 20
- 21
- 22

以下几项中，不属于公钥密码体制所依据的数学难题的是

- 模幂运算问题
- 大整数因子分解问题
- 离散对数问题
- 椭圆曲线离散对数问题

2000年10月，NIST将下列哪个候选算法作为高级数据加密标准，该算法是由两位比利时密码学者提出的

- MARS
- Rijndael
- Twofish
- Bluefish

清空 保存答案

下列算法中哪个是不可逆的数学运算

- MD5算法
- Rijndael算法
- ElGamal算法
- 背包算法

清 空 保存答案

在美国数字签名算法 DSA 中，取 $p=47$，$q=23$，取 $g=25$，公钥 $y=8$，设消息的 Hash 值 $SHA(M)=19$，那么消息[$SHA(M)$，(r，s)]=[19，(12，18)]是否为正确签名？答：_____。

是

高级数据加密标准 AES 的轮函数中有一个计算部件是字节替换，在字节替换中有一步是将字节看做 $GF(2^8)$ 上的元素，映射到自己的乘法逆，而 $GF(2^8)$ 上的乘法运算的模多项式是 $m(x)=x^8+x^4+x^3+x+1$，在当前阵列中某个元素的字节值为 $(a_7a_6a_5a_4a_3a_2a_1a_0)=(00001011)$，则该字节值的乘法逆是_____；

11000000

设对某英文文件进行仿射密码的加解密算法，加密算法为c=19m+7 (mod 26)，则密文单词'ydfim'所对应的明文单词是

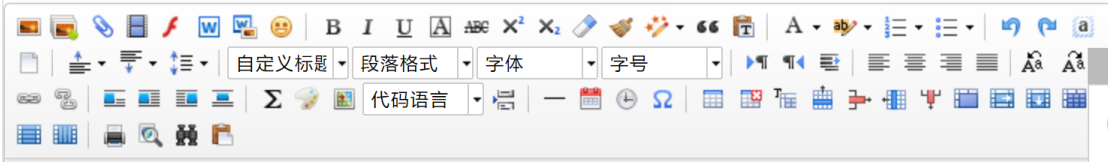
field

分组密码DES算法的钥控非线性函数F中有8个S盒，下表是第三个S盒S_3：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

若S_3的输入为110010，则输出为_____；

已知一个周期为15的2元序列为011101100101000，则该序列在一个周期内的1游程的个数为



(1) 设LFSR1是一个3级m－序列，其特征多项式为：$f_1(x)=1+x+x^3$，取初始值为$a_0=a_1=1, a_2=0$，则该序列的一个周期$\{a_k\}=1101001$；设LFSR2是另一个3级m－序列，其特征多项式为：$f_2(x)=1+x^2+x^3$，取初始值为$b_0=b_1=b_2=1$,则输出序列$\{b_k\}=1110010$,现使用钟控序列中的走停生成器来产生一个周期为49的钟控序列，试给出钟控序列的前20位。

(2) 一个周期为8的2元序列$\{s_k\}=11010011$，计算该序列的自相关函数值。

已知F_{23}上的椭圆曲线

$$E_{23}(9,17): y^2=x^3+9x+17,$$

取$P=(16,5)$作为$E_{23}(9,17)$的一个生成元，解答下列几个问题：

(1) 设用户B的私钥为$a=13$，求B的公钥$Q=13P$;

(2) 设用户A欲发消息$m=(10,16)$给B，选择随机数$k=5$，求密文c;

(3) 设用户B收到密文$c=((15,13),(14,9))$，试求明文m。

(1) 在分组密码IDEA中，设MA变换的输入为

$a=1001\ 1100\ 1010\ 0110,\ b=1111\ 1010\ 1101\ 1011,\ c=1010\ 1010\ 0011\ 0010,$

$d=1110\ 0100\ 1010\ 0101,\ z_5=0000\ 1010\ 1101\ 1011, z_6=0000\ 1101\ 0010\ 1101,$

计算此MA部件的输出。

(2) 在分组密码AES中，设列混合（又称列混淆）部件的输入状态阵列中的一列为 $\begin{pmatrix}10100011\\11100010\\01111111\\00010101\end{pmatrix}$，计算对该列进行列混合之后的结果。

现打算用密钥短语密码加密算法对某英文文件进行加解密，请计算下面两题：(1) 若所选择的密钥字是英文句子“pack my boxes with five dozen liquor jugs”，试给出某明文文件中“des algorithm”的密文；(2) 若所选择的密钥字是英文短语“heavy box perform waltzes and jigs quickly ”，试给出某密文文件中“hmotnpjxw”的明文。

秘密分割的原始模型是“海盗分割藏宝图”。设共有 n 个海盗有权参加宝物分配。为了防止独吞或联手作弊，规定：t 个人以上同时到场才能找到宝物，而 t-1 个人以下同时到场是不能找到宝物的。著名密码学家 Shamir 提出一个基于有限域上的多项式的秘密分割门限方案，方案的设计如下所述。

选择一个素数 p，假设秘密是一个系数取自有限域 Z_p 上的 $t-1$ 次多项式

$$h(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0,$$

也就是多项式 $h(x)$ 的系数 $\{a_0,a_1,\cdots,a_{t-1}\}$ 是要分割的秘密。设参与秘密分割的总人数是 n，其中第 k 个人的公开身份是 x_k，$x_k\in Z_p$，$k=1,2,\cdots,n$，而第 k 个人的秘密身份是 $h(x)$ 在 x_k 点的多项式值，即 $h(x_k)\bmod p$。也就是第 k 个人拥有 $(x_k,\ h(x_k)\bmod p)$，其中 x_k 对其他参与者公开，而 $h(x_k)\bmod p$ 对其参与人保密。任何 t 个人以上同时到场，不妨设分别是第 k_i 个人，$i=1,2,\cdots,t$，每个人交出自己的身份 $(x_{k_i},\ h(x_{k_i})\bmod p)$，将这些拼在一起列出线性方程组

$$\begin{cases}a_0+a_1x_{k_1}+a_2x_{k_1}^2+\cdots+a_{t-1}x_{k_1}^{t-1}=h(x_{k_1})\bmod p\\ a_0+a_1x_{k_2}+a_2x_{k_2}^2+\cdots+a_{t-1}x_{k_2}^{t-1}=h(x_{k_2})\bmod p\\ \cdots\quad\cdots\quad\cdots\\ a_0+a_1x_{k_t}+a_2x_{k_t}^2+\cdots+a_{t-1}x_{k_t}^{t-1}=h(x_{k_t})\bmod p\end{cases},$$