六.论述题：

(1) a b c d e f g h i j k l m n o p q r s t u v w x y z
p a c k m y b o x e i s w i t h f v d z n l q u r j g

`des_algorithm` 密文为 kmzl pwbhdxnoi

(2) a b c d e f g h i j k l m n o p q r s t u v w x y z
h e a v y b o x p r f m w l t z s n d j i g q u c k

hmotnpjxw 的明文是 algorithm

七.证明题：

(1) $(a \dot{+} c, b \dot{+} d) = (e, f) = (0011011010010100, 0001111001111110)$

$((e \times z_5) \text{“}+\text{”} f) \times z_6 = u = 0110000111011010$

$u \text{“}+\text{”} (e \times z_5) = v = 1101100000100110$

$(a, b, c, d)(\dot{+}\dot{+}\dot{+}\dot{+})(u, v, u, v)$

$= (w_1, w_2, w_3, w_4) = (1111110101111100, 0010001011111101$

$1100101111101000, 0011110010000011)$

(2) $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 10100011 \\ 11100010 \\ 01111111 \\ 00101010 \end{pmatrix} \bmod (x^8 + x^4 + x^3 + x + 1)$

$= \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \begin{pmatrix} x^7 + x^5 + x + 1 \\ x^7 + x^6 + x^5 + x \\ x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ x^4 + x^2 + 1 \end{pmatrix} = \begin{pmatrix} 00001010 \\ 11101000 \\ 10000000 \\ 01001001 \end{pmatrix}$

对于合法的用户来说，

四、

$$\begin{pmatrix}1 & x_1 & x_1^2\\ 1 & x_2 & x_2^2\\ 1 & x_3 & x_3^2\\ \phi & & \\ \phi & & \end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} = h(\quad a_0 \quad a_1 \quad a_2$$

$$\begin{pmatrix}1 & 3 & 9\\ 1 & 5 & \cancel{25}\ 12\\ 1 & 7 & \cancel{49}\ 19\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} = \begin{pmatrix}2\\ 5\\ 12\end{pmatrix} \qquad \begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} = \begin{pmatrix}5\\ 4\\ 7\end{pmatrix}$$

$$\begin{pmatrix}1 & 3 & 9\\ 1 & 5 & \cancel{25}\ 12\\ 1 & 9 & \cancel{81}\ 3\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} = \begin{pmatrix}2\\ 5\\ 8\end{pmatrix} \qquad \begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} = \begin{pmatrix}7\\ 9\\ 8\end{pmatrix}$$

$\because \begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix} \neq \begin{pmatrix}a_0\\ a_1\\ a_2\end{pmatrix}$ ∴存在假储

五.计算题：

(1) $Q = 13P = (1,21)$

(2) $m = (10,16) = 18P$

$k = 5$

$C_1 = kP = 5P = (13,10)$

$C_2 = m + kY = 18P + 5\cdot 13P = 19P = (1,2)$

密文：$\{(13,10),(1,2)\}$

(3) $C_2 - xC_1 = C_2 - 13C_1 = 29P - 13\cdot 17P = \cancel{(16,5)}\ 32P = O$

计科1802 张世深 180403040l

一、选择题

1、D(13) 2、C(21) 3、A(模幂运算) 4、B(Rijndael) 5、A(MD5)

二、填空题

1、是 2、1100000 3、field 4、0001

5、4

三、名词解释

(1) a: 110100111010011101001

b: 111001011100101110010

$a_0=111$ $a_1=110$ $a_2=100$ $a_3=001$ $a_4=010$ $a_5=101$ $a_6=011$

$a_7=111$ $a_8$ $a_9$ $a_{10}$ $a_{11}$

a: 110100111010011101001

$a_0\ a_1\ a_2\ a_2\ a_3\ a_3\ a_3\ a_4\ a_5\ a_6\ a_6\ a_7\ a_7\ a_7\ a_8\ a_9\ a_{10}\ a_{10}\ a_{11}\ a_{11}\ a_{11}$

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

前20位输出 11110000100111111110000

(2) $\{S_k\}=11010011$

$R_{aa}(0)=(-1)^{1+1}+(-1)^{1+1}+(-1)^{0+0}+(-1)^{1+1}+(-1)^{0+0}+(-1)^{0+0}+(-1)^{1+1}+(-1)^{1+1}$

$=8$

$R_{(a,a)}(1)=(-1)^{1+1}+(-1)^{1+0}+(-1)^{0+1}+(-1)^{1+0}+(-1)^{0+0}+(-1)^{0+1}+(-1)^{1+1}+(-1)^{1+1}$

$=1-1-1\underline{-1}+1\underline{-1+2}=0$

$R_{(a,a)}(2)=0$, $R(a,a)_{(3)}=0$

$R_{aa}(4)=(-1)^{1+0}+(-1)^{1+0}+(-1)^{0+1}+(-1)^{1+1}+(-1)^{0+1}+(-1)^{0+1}+(-1)^{1+0}+(-1)^{1+1}$

$=-1-1\underline{-1+1}-1-1\underline{-1+1}=-4$ $R_{(a,a)}(5)=R_{aa}(6)=R_{(a,a)}(7)=0$