|  | No.             |        |         |
|--|-----------------|--------|---------|
|  | Date.           | /      | 1       |
| E-6-1  | - , , , , , , , |        |         |
| ① 有先由 yi=dk (mod p),根据a计算 yia=(dk)a=   | Lak (mod p)     |        |         |
| 又因B=da(modp), FAUL y, a=Bk(modp)   | •               |        |         |
| 初り2=火+BK(modp), 用以火=y2-BK(modp)  | ,接Bk=y,a(me     | dp) 74 | 入得      |
| X= y2- y1 (modp)   | - 1 0           |        |         |
| ② I、解答→解决CDH.  |                 |        |         |
| 区东·(y,,y,),且能解密出众,已知少=X+Bk   | (mod p), 那以 B   | k= 4z- | x(modp) |
| 这里y=dk(modp), B=~a(modp)   |                 |        |         |
| · bk = dak (mod p), 即CDH问题的解   |                 |        |         |
| 亚、爱文为(y,yz),其中y,=dk(modp), B=da(m  | nod b) =        |        |         |
| 女有解 ODH的算法,则可根据 y,和 B 计算   |                 | b)     |         |
| 2.可通过 X= Y2-Bk (modp)得到火   |                 | 17     |         |
| J  |                 |        |         |
| E6.2   |                 |        |         |
| 若泄露了F酒机数k,则岩攻插飞知道察议及公东   | a, 3, p         |        |         |
| RI BB=da, L. The Bk=dak= K   | • •             |        |         |
| 170 可由 y== x·K 分級得到 x- yz·KT   |                 |        |         |
| 图比次 ElGama / 加密液酸酶   |                 |        |         |
|  | 1               |        |         |
|  |                 |        |         |
| d  |                 |        |         |
|  |                 |        |         |
| ,  |                 |        |         |
|  |                 |        |         |
| , and the second |                 |        |         |
|  |                 |        |         |
| ,  |                 |        |         |
|  |                 |        |         |
|  |                 |        |         |