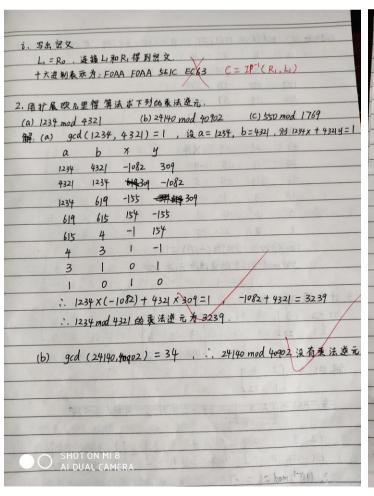
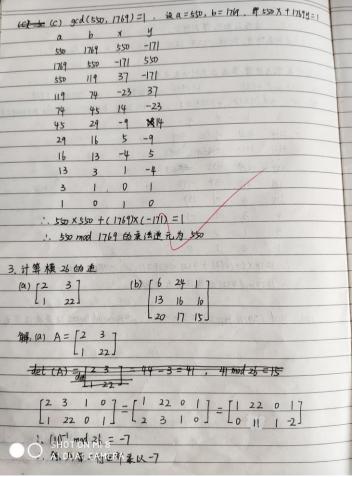
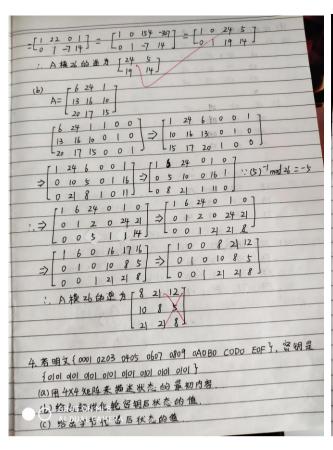
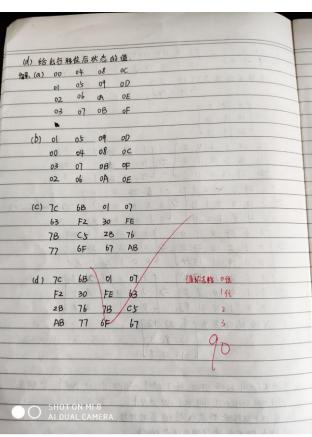


1. 这个问题给出3用一轮 DES 加密的具体数字的例子。假设明文和 密钥 K 有相同的 位模式,即 用十六进制表示:0123456789ABCDEF 用二进制表: 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 a、推导出第一轮的子密钥K, 解: 64位初始密钥经过置换选择1分为2个28位数据G和D。 Co: 1111 0000 1100 1100 1010 1010 0000 Do: 10/0 /0/0 1/00 1/10 1/11 0000 0000 循环左移/位 C': 1010 0001 1001 1001 0101 0100 0001 Di: 0101 0101 1001 1100 0000 0001 再经过置换选择2. 得到 48位密钥 K, K1:0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101 用十六进制表示:0B02679849A5 b、推导Lo、Ro. 对好色明文进行初始置换(IP),前32位为Lo,后32位为Ro. Lo: 1100 1100 0000 0000 1100 1100 1111 1111 Ro. 1111 0000 1010 1010 1111 0000 1010 1010 用十六进制表示: Lo: CC DO CCFF Ro: FO AA FOAA C. 扩展 Ro 或E(Ro) 利用扩展器换 E将 Ro 扩展成 48位 十六进制: 7A 1555 7A 1555 O ALDUAL CAMERA









```
1. 用RSA 算法对下列数据实现加密和解密
(a) p=3 q=11 e=7 M=5
(b) p=5 9=11 e=3 M=9
(c) p=7 9=11 e=17 M=8
(d) p=11 9=13 e=11 M=7
(e) P=17 9=31 e=7 M=2
 雅(1) n=pq=3×11=33 , Y(n)=9(3)9(11)=2×10=20
      ed = 1 (mad 20) , ex d= 3 , 公钥对(33,7) 私钥对(33,3)
     pa 强, 57 = c (mod 33), c= 14
    爾實: 143 = m (md 33) , m=5
    (2) n = pq = 55, \varphi(n) = \varphi(5) \varphi(11) = 4 \times 10 = 40
      ed=(mod40), d=27, 公嗣对(55,3) 拉嗣对(55,27)
      力a密: 93 = c (mod 55) , c=14
      解望: 1427 = m (mad 55) , m=9/
    (3) n = pq = 77 \varphi(n) = \varphi(7) \varphi(11) = 6 \times 10 = 60
       ed = 1 (mad 60), d= 53, 12 (17.17) 和明对(77.53)
      Dog: 817 = c (mod 17) , c=57/
      解定: 57<sup>53</sup> = m (mad 77), m=8
    (4) n=pq=143 , q(n= p(1)) p(13) = 10x12 = 120
      ed=| (mod(20) , d=) ( 安明对(193,11) 私服对(143,11)
      10 8: 7" = c (mod 143) . c= 106
      解密: 106"= m (mod 143) , m=7
   (5) n = pq = 527 . p(n) = p(1) p(31) = 16 \times 30 = 480
       ed = 1 (mod 480) , d= 343, '254xt (527, 7), 7444xt (527, 10)
      もの語: 27 = c (mad 480) C= 128
    1930 12,8343 = m (mod 480) , m= 2
```

```
2. 在使用 RSA 的公钥体 制中, 己载鉴发给某用户的密文 C=10, 该用户的
    公钢e=5, n=35, 那么明文M 是多少?
   解: M' = 10 (mod 35)
      :: n=pxq , p, q为厦数
      · P. P. 分别为5和7
      : 4(n) = 4(5)4(7) = 4x6=24
     : ed = 1 (mad 24) . . . d = 5
      : C5 = m (mod 35) PP 105 = m (mod 35)
 3. 在RSA体制中,某给定用户的公钥e=31, n=3599, 那么该用户的私
  铜 等于多少?
   解: : n=3599=59×61/
      : 4(n) = 4(59)4(61) = 58x60 = 3480
       : 31 Xd = 1 (mod 3480)
      i. d= 3031 /
      : 私钢等于3031
4. 用PA和B使用 Diffie-Hellman 密铜交换技术来交换密钥,设公用素数
  9=71,本原根 a=7,
 (a) 著用PA的科钢 XA=5,则A的公钢 YA为多少?
  (b) 若用PB的私钢XB=12,则B的公钢YB为多少?
  (1) 共身的容明为多少?
 爾: (a) 75 mod 71 = 51 , : 1 = 51
  (b) 712 mod 71 = 4, i. YB = 4.
   (c) 共享發明 K=YB*n=45=Yx*e=512 mod 71=30
   O AL DUAL CAMERA mod 71
```

