

```
# > REQUEST EXCHANGE
# < CONFIRMED
# > KEY
7abed4245dec0a5df17c672d799488c7b5ef5b9110c43e0c3eae586c21b7369095569fc3aa0cc2cde94a362cc6
e7902b8bb1bd6d32f358d8e7091e7e8c48b9fa2aabe1579328cfa18e55927c5e9c7d50ccba5b5f4e173b606b65
a95c6f6c27b9fa8b482c45ce9605700856869b2beb7f663bf6244902ab57bf681a31fdbe86d7107daa7cc53dcf
f6633cb7a591508da29e1016dc85211f83052efc8e987e4d5cf5bac407ee187795dbba722e8b3650c555d119c5
5676a5ff90af6a0eabbba477/010001
# < KEY
55b0a8cbbba652468362b92444a4336da542eb8641ac83fc85e4e44bc77965842aa18f783d150a03a084f04e680
9ee60e5bfe8379397a665936d91b5f3433b48339d22b8b3de2544898376c87ddc385b8e6994eda6e385996a102
a6cf5e241dbb0c78eae345c01a1bdad9d30d9bf84c02d976965654ec028d965833bd7072fbeb8c576b49cc9f66
6757300fca0877f88a0975b3b5c67555f1de17aa153d2b9b54c6a51bcb35ca840e7f5cabdb1bd4eab542cbae8a
2dd5a59f8e84785089bdd383/010001
# > MSG
2cb5e614c40eb325cdcec0410884b5e4b20cb63c39f93b720710b2b4a2d66b76588129d24172faf0ef84ca02b3
f89b718eaf2a7ba7a13e444a7772ed79b3db6c621c02a0d32ec09c510fcd39b1c76d715507de8634d217dceb33
cb4d0cb0309b58bf89e4e27e6ab0a24c32f97d820013cefc35408e12d11644928a368526d1482503995c0d392
1164fc0b301329fffb1aac13f66dcaa21a6f63e371308be12366de0e68db27751ec12f9e02976bc52b2a2888f07
608d26a637a46f03a6f1a1ab
# < MSG
3c94c8dffb44880a13acc3e40826d021e4da41aca832cb6d396e83f528eb6fdd4aed8f59ed837d072230b0d6e3
8e57d90dd409de1c2e867a5b6a3962a83aa330b12516c313b0ba4820887fc7761c673d223b51f4f97ed1a7a90a
009a880f7317b3681a8ca64b53f2416d7daf43b8da2358d19d7e38d10c22bf7c55cf8fb587d33b9ee87492149a
d959c0154b4708c5961705f08a45423d4f5cabcb3b2ec43266589ac3dbaf72a88377b9fe2afa84be2feacdb62
2f508d5d2874fa3106334bbd

a =
0x7abed4245dec0a5df17c672d799488c7b5ef5b9110c43e0c3eae586c21b7369095569fc3aa0cc2cde94a362c
c6e7902b8bb1bd6d32f358d8e7091e7e8c48b9fa2aabe1579328cfa18e55927c5e9c7d50ccba5b5f4e173b606b
65a95c6f6c27b9fa8b482c45ce9605700856869b2beb7f663bf6244902ab57bf681a31fdbe86d7107daa7cc53d
cff6633cb7a591508da29e1016dc85211f83052efc8e987e4d5cf5bac407ee187795dbba722e8b3650c555d119
c55676a5ff90af6a0eabbba477

b =
0x55b0a8cbbba652468362b92444a4336da542eb8641ac83fc85e4e44bc77965842aa18f783d150a03a084f04e6
809ee60e5bfe8379397a665936d91b5f3433b48339d22b8b3de2544898376c87ddc385b8e6994eda6e385996a1
02a6cf5e241dbb0c78eae345c01a1bdad9d30d9bf84c02d976965654ec028d965833bd7072fbeb8c576b49cc9f
666757300fca0877f88a0975b3b5c67555f1de17aa153d2b9b54c6a51bcb35ca840e7f5cabdb1bd4eab542cbae
8a2dd5a59f8e84785089bdd383

c =
0x3c94c8dffb44880a13acc3e40826d021e4da41aca832cb6d396e83f528eb6fdd4aed8f59ed837d072230b0d6
e38e57d90dd409de1c2e867a5b6a3962a83aa330b12516c313b0ba4820887fc7761c673d223b51f4f97ed1a7a9
0a009a880f7317b3681a8ca64b53f2416d7daf43b8da2358d19d7e38d10c22bf7c55cf8fb587d33b9ee8749214
9ad959c0154b4708c5961705f08a45423d4f5cabcb3b2ec43266589ac3dbaf72a88377b9fe2afa84be2feacdb
622f508d5d2874fa3106334bbd

e = 0x010001
```

```
def xgcd(a,b):
    """xgcd(a,b) returns a list of form [g,x,y], where g is gcd(a,b) and
    x,y satisfy the equation g = ax + by."""
    a1=1; b1=0; a2=0; b2=1; aneg=1; bneg=1
    if(a < 0):
        a = -a; aneg=-1
    if(b < 0):
        b = -b; bneg=-1
    while (1):
        quot = -(a // b)
        a = a % b
        a1 = a1 + quot*a2; b1 = b1 + quot*b2
        if(a == 0):
            return [b, a2*aneg, b2*bneg]
        quot = -(b // a)
        b = b % a;
        a2 = a2 + quot*a1; b2 = b2 + quot*b1
        if(b == 0):
```

```
        return [a, a1*aneg, b1*bneg]

def invmod(a,n):
    """invmod(b,n) - Compute 1/b mod n."""
    return xgcd(a,n)[1] % n

p = b / xgcd(a,b)[0]
d = invmod(0x010001, p - 1)
m = pow(c, d, p)
print ("%0256X"%m).decode("hex").rstrip("\x00")
```