cryptohack Diffie_Hellman 部分wp by crumbling

目录

- DIFFIE-HELLMAN
  - STARTER
    1. Diffie-Hellman Starter 1
    2. Diffie-Hellman Starter 2
    3. Diffie-Hellman Starter 3
    4. Diffie-Hellman Starter 4
    5. Diffie-Hellman Starter 5
  - MAN IN THE MIDDLE
    1. Parameter Injection

DIFFIE-HELLMAN

STARTER

Diffie-Hellman Starter 1

求乘法逆元

```
from gmpy2 import*
g=209
p=991
print(gmpy2.invert(g,p))
```

Diffie-Hellman Starter 2

遍历求本原根

```
p=28151
def getg(g,p):
    for i in range(2,p):
        if pow(g,i,p)==g:
            return i
    return p
for g in range(2,p):
    r=getg(g,p)
    if r==p:
        print(g)
        break
```

Diffie-Hellman Starter 3

求g^a mod p

```
g=2
p=241031242692103258855207602219756607485695054850245994265411694195810883168261
222889009385826134161467322714147790401219650364895705058263194273070680500922300
627347453410734066962460145893616597740410271692494532003787294341703258437786591
981437631937768598695240889401955773461198435453015470437472077499697637500843089
263392955599688824578724129938101291302945929999479263652640592846472097303849472
116814344647144384885209401274598442888593365268963209196339192
a=972107443837033796245864316200458246846904598488981605856765890478853088246897345
487328491037710219222038930943365848626194109830309179393018216763327572120124760
140018038673999837643377590434413866611132403979547150659053897355593394492586978
400044375465657296027592948349589216415363722668361328689588996541370097559090335
137676411595949335857341797148926151694299575970292809805314431441447043469447485
957669949989090202320234337890323293401862304986599884732815
print(pow(g,a,p))
```

Diffie-Hellman Starter 4

求shared secret

```
nist=
{g:2,p:241031242692103258855207602219756607485695054850245994265411694195810883168
261222889009385826134161467322714147790401219650364895705058263194273070680500922
306273474534107340669624601458936165977404102716924945320037872943417032584377865
919814376319377685986952408894019557734611984354530154704374720774996976375008430
892633929555996888245787241299381012913029459299994792636526405928464720973038494
721168143446471443848852094012745984428885933652689632091963391919,'A':70249943
217595468278554541264975482909289174351516133994495821400710625291840101960595720
462672604202133493023241393916394629829526272643847352371534839862030410331485087
487331809285533195024369287293217083414424096866925845838641840923193480821332056
735592483730921055532222505605661664236182285229504265881752580410194731633895345
823963910901731715743835775619780738974844840425579683385344491015955892106904647
602049559477279345982530488299847663103078045601,'b':1201923325290399034459852
253577496302039577040944529672403437843349797684016780597058996096222194829095187
338772810211599683145448229924322683949099971376344041217796586150877342053226648
461912671056641491422756010371533669619321037985057504773038837834826618093494613
910047983133983589658344369152937270395458907150771791713690677012207773981426229
848866213808560873610341860175086169841734026421386775383467935919142709819588711
206450310451048961044829442072 0,'B':5183869567900415799280568159142218375992345516551445851334147278389771457772133830180966625168143025838418589010218222735051207284517884129679718090388540906707432651871382081693551554118830635418812092889677356841524732606877966413095696945029740702792600918276162780018190172184055787082801984021854818848726044182933360343271402344702994286307697948788956945218625733351235572472594139049896654668279060812561316674482030769106856338735493673264356965401717 2}
print(pow(nist['A'],nist['b'],nist[p]))
```

Diffie-Hellman Starter 5

求出shared secret后再decrypt文件中解密就好。

```
from hashlib import *
g=2
p=24103124269210325885520760221975660748569505485024599426541169419581088316826122288900938582613416146732271414779040121965036489570505826319427307068050092230627347453410734066962460145893616597740410271692494532003787294341703258437786591981437631937768598695240889401955773461198435453015470437472077499697637500843089263392955599688824578724129938101291302945929999479263652640592846472097303849472116814344647144384885209401274598442888593365268963209196339191
A=11221873913954290888056435953437342401301624977293196269223790757199033448352887751380927262561051206115906173760854728855866287968508668429962448174286501692406500055526797783014474036446797720655591478123639721603380588220764021968601164346827516571813288848902468884610194364245965542360911197636331608062047192823687973794421750346226561577477431898637587844097881923834607790886411615683187469581747777247712123282082772842489084576915272602752077290142378 4
b=19739508381490702899178577271492088590824934192565095155521904941129843621719060519082493478733627922878580978353181450766138511122063932935804819633962606567686911973797917553177076886180858111031190354856742403926448566133099522190780330082416546997709949428472283184565398539279148026471209129358027494713248040231981211046264114388457770633585919066824069468026116021060950689184279386829767261962592400140303567687218945576794407754219806449948616443145194 4
B=12419724605220753447833375566607005377603311083327356778638628136665786395188992932263999212520496550315636129053951452368544433347745559822048578957163832157054989703953795266987614689321472006505136260282634496057556611895255213431429792650440684094056675492411255973871730064601453797599862721919906759888738942089568517733310397478403124552213545899107269828192034219927297382964528203655537591825472559989848821583936881196296090676474947626167190474669735814 4
iv=0x737561146ff8194f45290f5766ed6aba
encrypted_flag=0x39c99bf2f0c14678d6a5416faef954b5893c316fc3c48622ba1fd6a9fe85f3dc72a29c394cf4bc8aff6a7b21cae8e12c
shared_secret=pow(A,b,p)
print(shared_secret)
```

MAN IN THE MIDDLE

Parameter Injection

中间人。

此题中通过中间人攻击的方式让A、B获得一个简单且被中间人已知的shared secret然后获得alice需要发送的信息

解题：同时修改A和g为0x01

Intercepted from Alice: {"p": "0xffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca237327ffffffffffffffff", "g": "0x02", "A": "0xa6f552a04ee8d9f51824ef01ff798675fe9e2eb3c474d7ad1853bbf73d2707fdc7505529f32353da

54611875c6278b95c2b8a7a88a38390ae1aede13ff72657f51d2aa7f04fae5dc6e5c4c85e0ab2de3844a2cad2a49f89fac0aadf19f28e3f280bb381cc7b4e02ab1c5f2c9a7195e7153ad359e9e0772350fcfbae13b8cb23f5d2d14f1879a2bbddec12c3792efca515d1242d03489fd3e33104534e485b2a21a9b99f8a828e60b66d07194bcd4657cc08a2a30fa48ab65b23b88d8fe4e7fe3"}

Send to Bob: {"p": "0xffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece45b3dc2007cb8a163bf0598da48361c55d39a69163fa8fd24cf5f83655d23dca3ad961c62f356208552bb9ed529077096966d670c354e4abc9804f1746c08ca237327ffffffffffffffff", "g": "0x01", "A": "0x01"}

Intercepted from Bob: {"B": "0x1"}

Send to Alice: {"B": "0x1"}

Intercepted from Alice: {"iv": "8991999995f0487e74501e5cc0516963", "encrypted_flag": "92c3e930c7062661556l8b15542be91ad254ea4969fdac1ecc46769f53c52185"}

Bob获得的共享密钥是A^b mod p=0x01

Alice获得的共享密钥是B^a mod p=0x01

共享密钥一致，获得flag