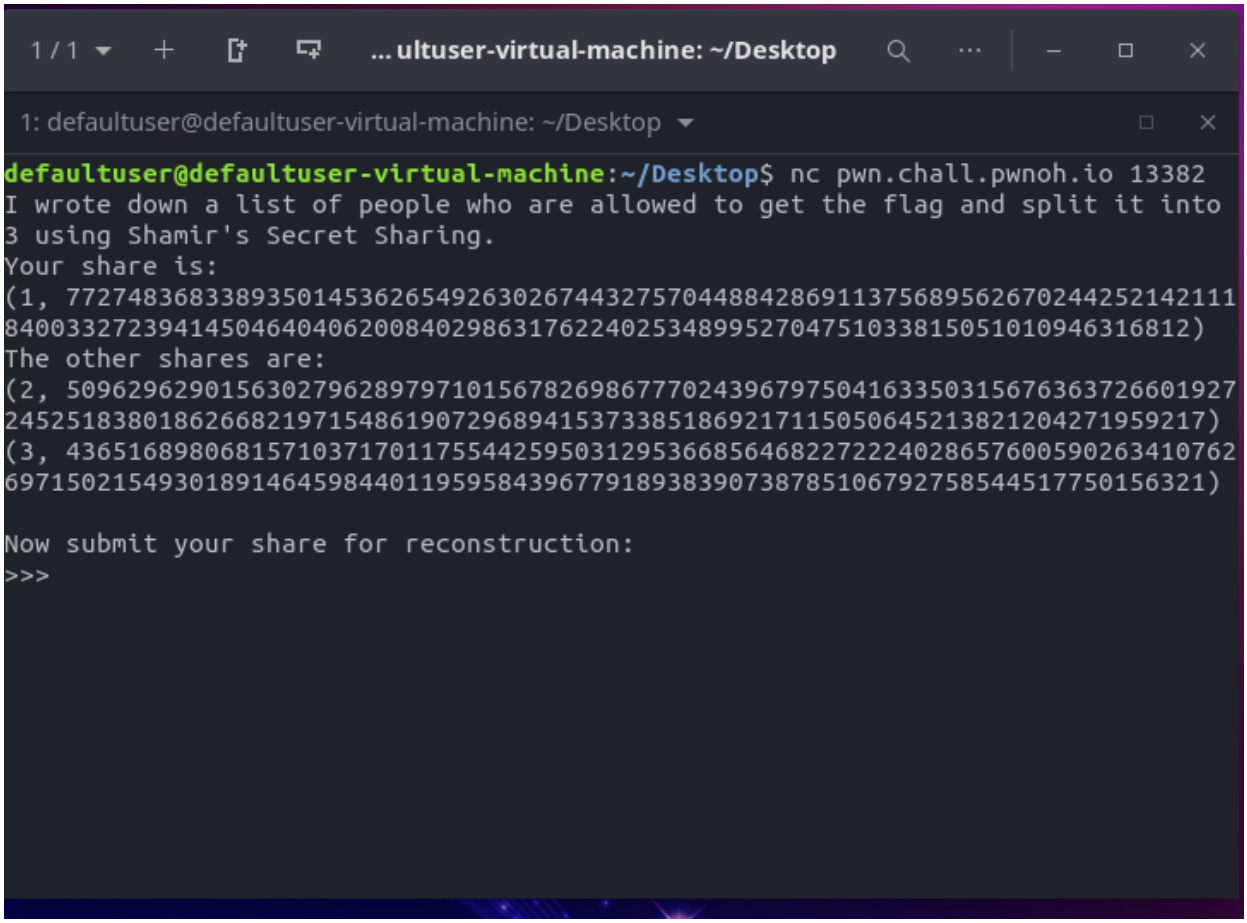
SSSHIT


Command:




About Website:
https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

Entering input 1:

```
defaultuser@defaultuser-virtual-machine:~/Desktop$ nc pwn.chall.pwnoh.io 13382
I wrote down a list of people who are allowed to get the flag and split it into
3 using Shamir's Secret Sharing.
Your share is:
(1, 279681114059079540991472324025938159188805242778933179174854735625523156215
9
18148599193088369973872588150631645345431809444421454683221168258145591807529
6)
The other shares are:
(2, 438230983188561472446941490347261577048900616042888012572072077862278291914
9
67474822669529653781792817914379808722159200377388347670036307633832358853682)
(3, 632714036110270798258265619184973113376478117111287748873878476478745421495
8
63063123465236889455189303932113669432002348229477517677381934084825638024086)

Now submit your share for reconstruction:
>>> (1, 772748368338935014536265492630267443275704488428691137568956267024425214
2
11184003327239414504640406200840298631762240253489952704751033815051010946316
81
2)
Sorry, only these people can see the flag: b'\x1f=\xe7\r\x03\xe0\xf3\xb3\x8a\xbf
\t\x88\xe1\xb4M\x1dn\x8eI$E\xca\xb6\xc5\x17;+\x0eq\xf8\x18\x0b\xde\x0f%\xe8\x0f\
xe7\xfb\xae6\r\xe6\xed=o\x9bY89\x14$?\x88\xbaTE\xae$@\xf6u\xad$'
```

Entering Input 2:

```
defaultuser@defaultuser-virtual-machine:~/Desktop$ nc pwn.chall.pwnoh.io 13382
I wrote down a list of people who are allowed to get the flag and split it into
3 using Shamir's Secret Sharing.
Your share is:
(1, 151502196320743229801291656835349116904301731919013823538662226718957943992
9
64145505907012235097806254318085011808292702394351520247208697916547048592931
1)
The other shares are:
(2, 280912445076900140419038960174917966028000067401512939072731873492815964384
5
33824613577639411294160753427513190025403202700003044899789375753910750585642
4)
(3, 388230746268470731853241910018706547371095006447497346602208940327217217192
3
00714697142362819148530969643549730863545063151681625810352359024957543935748
8)

Now submit your share for reconstruction:
>>> (2, 618201442871921519608211202652908709164895475620779587214043914182141667
2380350694023851885199412095531476591179469590746405541372157901447399336988255
6
11)
Bad input
```

Entering Input 3:

```
defaultuser@defaultuser-virtual-machine:~/Desktop$ nc pwn.chall.pwnoh.io 13382
I wrote down a list of people who are allowed to get the flag and split it into
3 using Shamir's Secret Sharing.
Your share is:
(1, 87154457729233324291082620797815332101027365980507619369810574272229804096
74712453964806156876834717284648222274438056498116582090908730992510246731307
9)
The other shares are:
(2, 160738588870352389209182229914741316138960598965224923145381045586204348595
78117512473629796400748248372686401306097912983052269464483375711275207180141
84)
(3, 187991456370474475603438720497007133119693478642638229885281152866579734157
93478416922982688686266094721409027864601997360330026678570599414945404259561
26)

Now submit your share for reconstruction:
>>> (3, 187991456370474475603438720497007133119693478642638229885281152866579734
157934784169229826886862660947214090278646019973603300266785705994149454042595
6126)
Bad input
```

Entering all three inputs:

```
defaultuser@defaultuser-virtual-machine:~/Desktop$ nc pwn.chall.pwnoh.io 13382
I wrote down a list of people who are allowed to get the flag and split it into
 3 using Shamir's Secret Sharing.
Your share is:
(1, 64637068472805681911169929684425007526908544468318471541248768962185297747
8944015695635068222088255681506510289060007092139683101187924506604739731244574
)
The other shares are:
(2, 21366470393834602745751712977660387227443381276940722524865857424940602604
3669166736575931876150006420639694870168393308725549276874466230154401812616873
4)
(3, 54722093748666502479273647268105921237972870068457957324256847142276862024
0618381788718140730187950944338643012559723362374372413250293425313843386662535
1)

Now submit your share for reconstruction:
>>> (1, 87154457729233324291082620797815332101027365980507619369810574272229804
0964774712453964806156876834717284648222274438056498116582090908730992510246731
3079)
The other shares are:
(2, 160738588870352389209182229914741316138960598965224923145381045586204348595
781175124736297964007482483726864013060979129830522694644833757112752071801418
4)
(3, 187991456370474475603438720497007133119693478642638229885281152866579734157
934784169229826886862660947214090278646019973603300266785705994149454042595612
6)Sorry, only these people can see the flag: b'\x80\xfa\xcf\xd2$D+#\xf7&\xd0G\xb
c!B\xc9\xa0i\xdd\x8a\xec\xf7\x8f\xee\xbe\xe5\xf3\x8a]\xac\x8a\xd0\xe7\x04W\x1f\
xf5\xfd\x8cZ\xb8]J\r\x1e\xff\xf0`\xdb\xe73\xacZ\xa4\xa0(\x8d\xf8\xc44\x00;F '
```

Found this website:
https://simon-frey.com/s4/

## Simple Shamir's Secret Sharing (s4)

Share your secret with a cryptographically secure method. All running locally in your browser. Your secrets never leave your machine!

Your browser is online. Please disconnect from your network to use s4 in a safer way.

You are running s4 from a webserver, this is insecure. Please save the webpage (Ctrl+S) locally and open this file.

Encrypt | Decrypt | Info

Shares: 3

Enter a share here | Enter a share here | Enter a share here

Your decrypted output

Using hex to ASCII for input 1:
https://www.binaryhexconverter.com/hex-to-ascii-text-converter

## Hex to Ascii (String) Converter

To use this **hex to string converter**, type a hex value like 6C 6F 76 65 and into the left field below and hit the Convert button. You will get the according string.

Facebook Twitter

Hexadecimal Value

```
b7ebe90396b3c7dc11e4b8ecde080ca212dffdf9cf
e1bd0a8c2d698fac1e099961c15e7f2e0f73f0
```

Convert

Ascii (String)

```
·ëé³ÇÜäˌìÐ¢ßýùÏá½
-i¬ aÁ^.sð
```

swap conversion: Ascii Text To Hexadecimal Converter

Using hex to ASCII for all three input :

## Hex to Ascii (String) Converter

To use this **hex to string converter**, type a hex value like 6C 6F 76 65 and into the left field below and hit the Convert button. You will get the according string.

Facebook Twitter

Hexadecimal Value

```
b80facfd2Df7d0bcBc9a0dd8aecf78feebee5f38aa
c8ad0e7041ff5fd8cb81efff0dbe73aca4a08df8c4
```

Convert

Ascii (String)

```
ˌ¬ý−÷Ð¼¼
ØŠÏxþëî_8ªÈpAÿ_ØËïÿ
¾s¬¤ ØÃ@
```

swap conversion: Ascii Text To Hexadecimal Converter