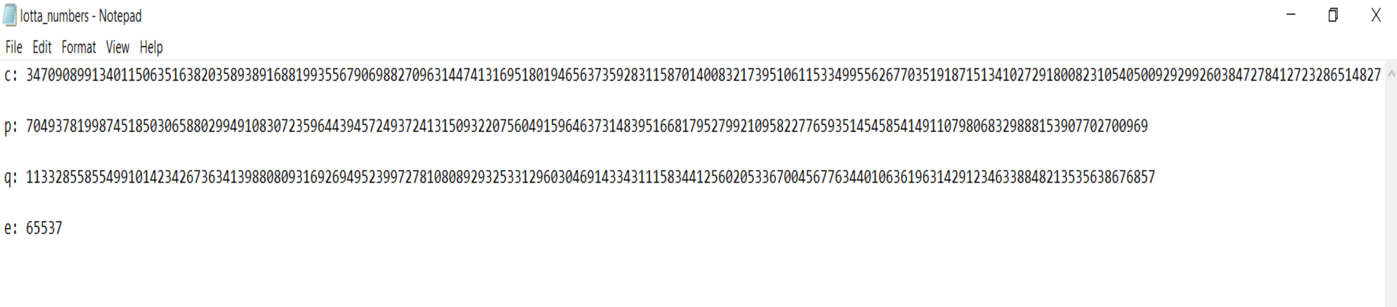
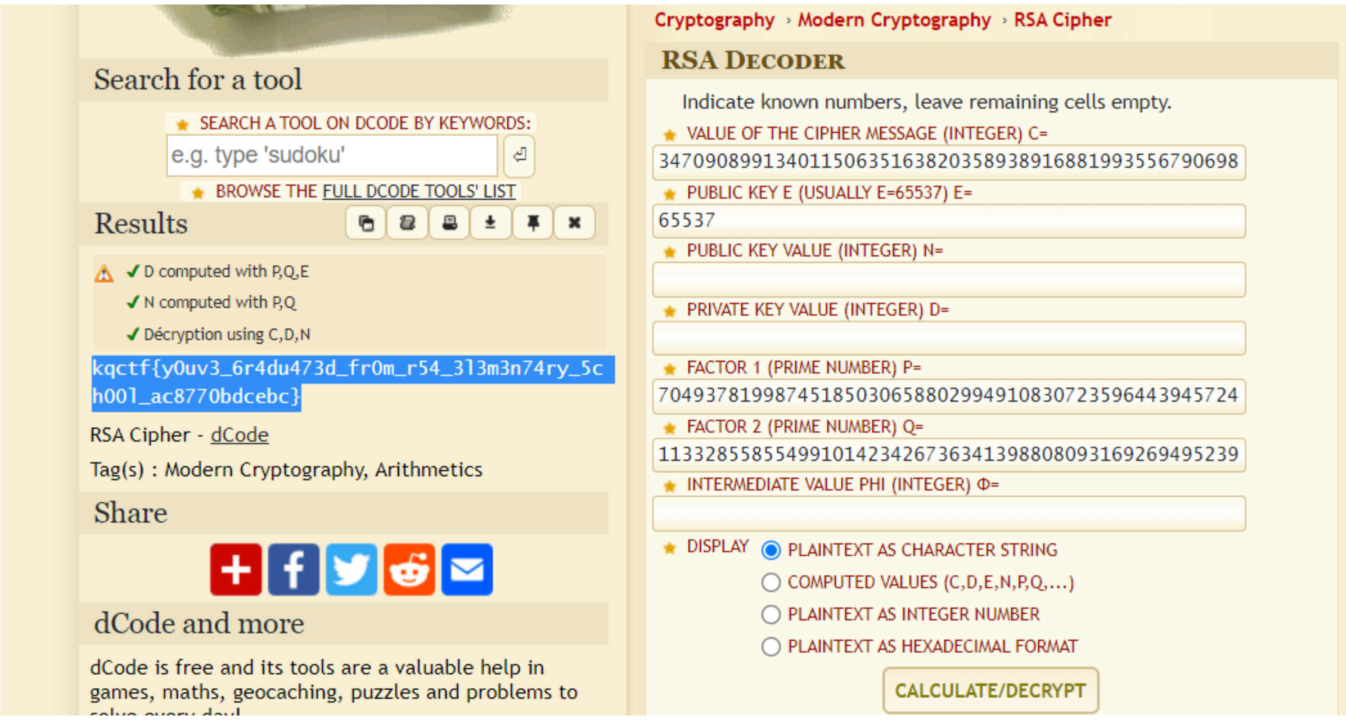
Cryptography:

ROAD SAFETY ASSOCIATION



```
c: 347090899134011506351638203589389168819935567906988270963144741316951801946563735928311587014008321739510611533499556267703519187151341027291800823105405009292992603847278412723286514827

p: 7049378199874518503065880299491083072359644394572493724131509322075604915964637314839516681795279921095822776593514545854149110798068329888153907702700969

q: 11332855855499101423426736341398808093169269495239972781080892932533129603046914334311158344125602053367004567763440106361963142912346338848213535638676857

e: 65537
```

Decrypting using dcode.fr:



Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'
BROWSE THE FULL DCODE TOOLS' LIST
Results

✓ D computed with P,Q,E

✓ N computed with P,Q

✓ Décryption using C,D,N

kqctf{y0uv3_6r4du473d_fr0m_r54_3l3m3n74ry_5ch00l_ac8770bdcebc}

RSA Cipher - dCode

Tag(s) : Modern Cryptography, Arithmetics

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!

Cryptography › Modern Cryptography › RSA Cipher
RSA DECODER

Indicate known numbers, leave remaining cells empty.

VALUE OF THE CIPHER MESSAGE (INTEGER) C= 34709089913401150635163820358938916881993556790698

PUBLIC KEY E (USUALLY E=65537) E= 65537

PUBLIC KEY VALUE (INTEGER) N=

PRIVATE KEY VALUE (INTEGER) D=

FACTOR 1 (PRIME NUMBER) P= 70493781998745185030658802994910830723596443945724

FACTOR 2 (PRIME NUMBER) Q= 11332855855499101423426736341398808093169269495239

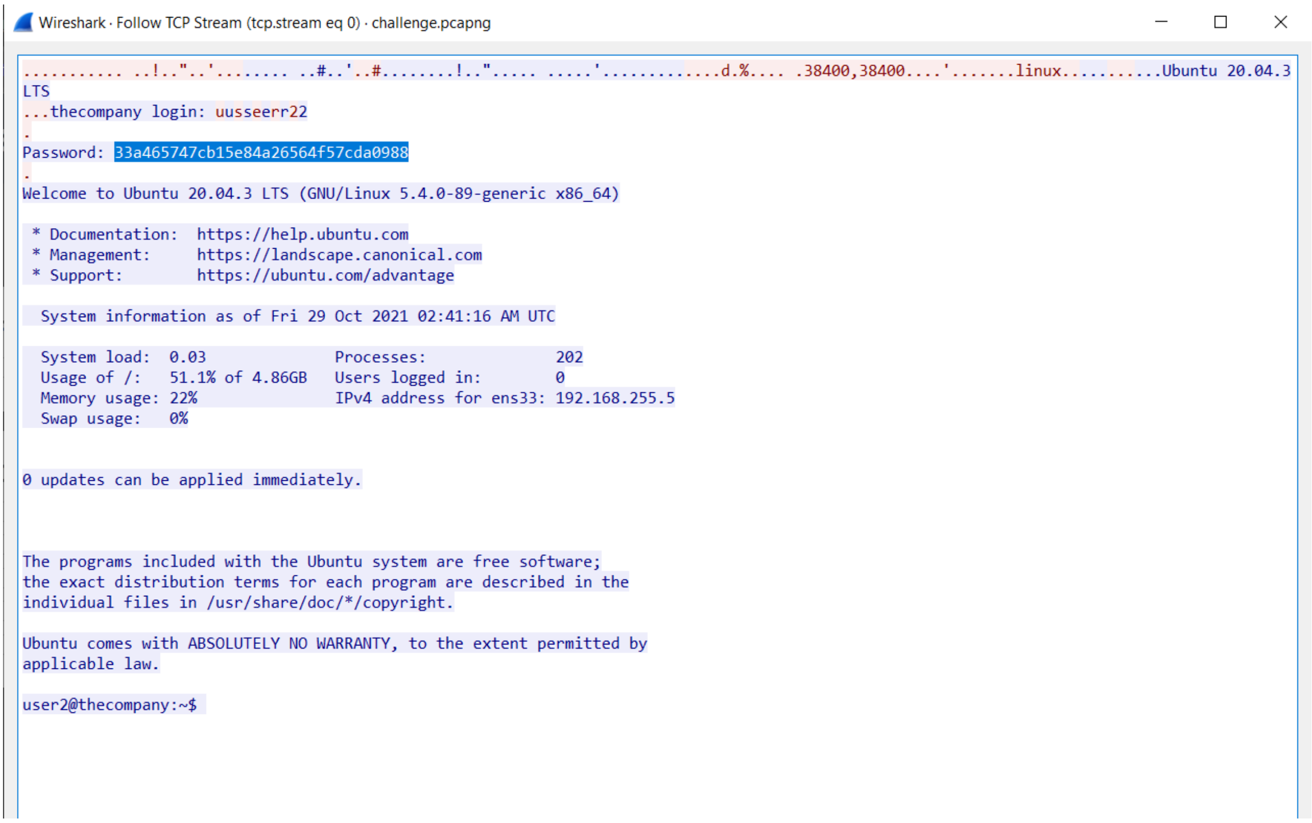
INTERMEDIATE VALUE PHI (INTEGER) Φ=

DISPLAY
● PLAINTEXT AS CHARACTER STRING
○ COMPUTED VALUES (C,D,E,N,P,Q,...)
○ PLAINTEXT AS INTEGER NUMBER
○ PLAINTEXT AS HEXADECIMAL FORMAT

Forensics:

OBLIGATORY SHARK

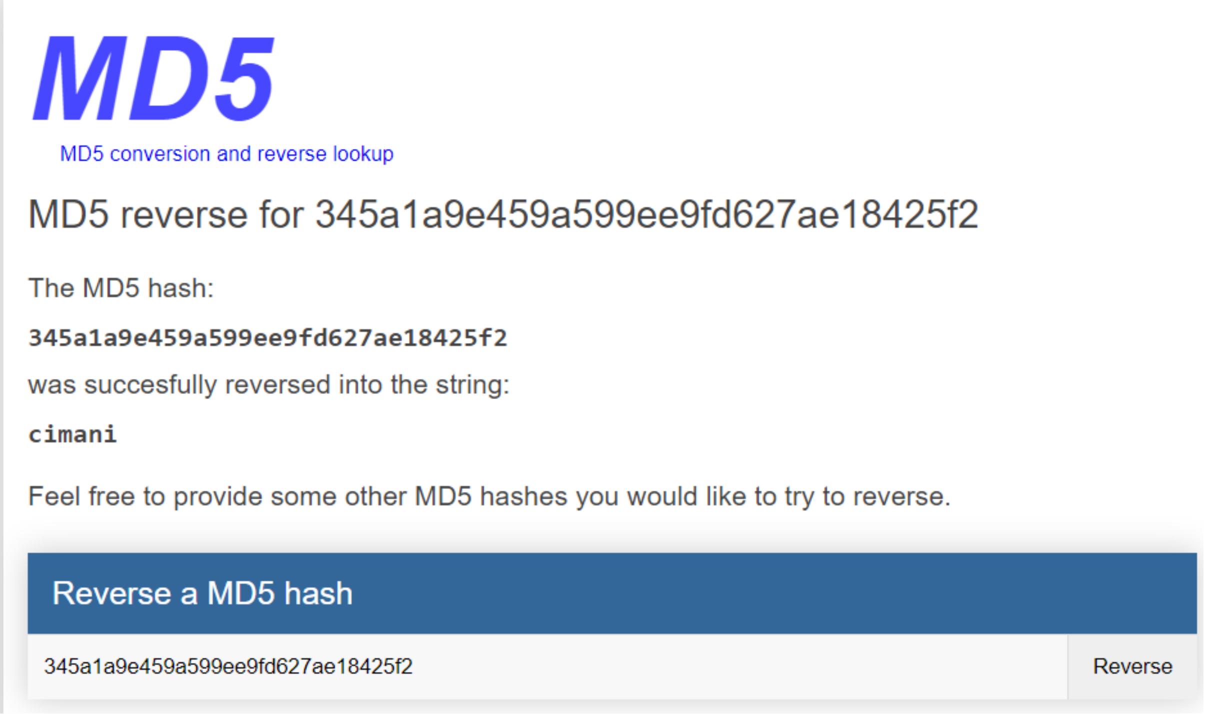
Following a TCP stream ended up in a SSH connection log:



Wireshark · Follow TCP Stream (tcp.stream eq 0) · challenge.pcapng

```
.......... ..!.."..'....... ..#..'..#........!.."..... .....'.............d.%.... .38400,38400....'.......linux............Ubuntu 20.04.3
LTS
...thecompany login: uusseerr22
.
Password: 33a465747cb15e84a26564f57cda0988
.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 29 Oct 2021 02:41:16 AM UTC

  System load:  0.03              Processes:             202
  Usage of /:   51.1% of 4.86GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for ens33: 192.168.255.5
  Swap usage:   0%


0 updates can be applied immediately.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

user2@thecompany:~$
```

On googling password, got the reversed hash but it was a false lead:



MD5 reverse for 345a1a9e459a599ee9fd627ae18425f2

The MD5 hash:

345a1a9e459a599ee9fd627ae18425f2

was succesfully reversed into the string:

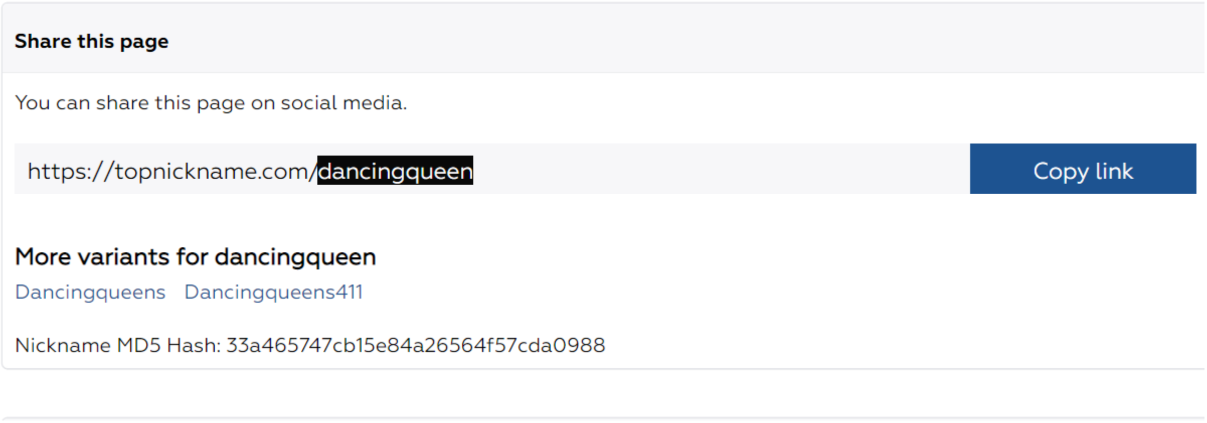
cimani

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

345a1a9e459a599ee9fd627ae18425f2

Later, went for other google results and got something interesting which was the flag:



Share this page

You can share this page on social media.

https://topnickname.com/dancingqueen

More variants for dancingqueen

Dancingqueens Dancingqueens411

Nickname MD5 Hash: 33a465747cb15e84a26564f57cda0988