

QUESTION:

Solve the challenge in the file !

SOLUTION:

- Open not_RSA file you will get p and n value
- Visit <https://www.tausquared.net/pages/ctf/rsa.html>, paste p and n value calculate q value

RSA

Clear all fields

Key generation

Choose two distinct prime numbers p and q .

p : 95279255905855272447
74428396301334

q :

Calculate $n = p * q$.

n : 25041937166092478951
23

Calculate n Calculate $p = n / q$ Calculate $q = n / p$

- Now you got q value then visit <https://gchq.github.io/CyberChef/> you will see multiple operations select (To Hex) operation and paste the value of q in input field and fetch the output

Operations

Search...

Favourites ★

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Recipe

To Hex

Delimiter: Space Bytes per line: 0

Input

919899554282618045161040188599929935213911330064790112629078167578535803925165312606
492784807389800924140801500604479166938376934981652124323286790726567426266929126589
987741639592918343067412825074380159795995949249366205795218212925665064758928200813
828436750571194337688677075438930864427847716213506516d

Output

39 31 39 38 39 39 35 35 34 32 38 32 36 31 38 30 34 35 31 36 31 30 34 30 31 38 38 35
39 39 39 32 39 39 33 35 32 31 33 39 31 31 33 36 30 36 34 37 39 30 31 31 32 36 32
39 30 37 38 31 36 37 35 37 38 35 33 35 38 30 33 39 32 35 31 36 35 33 31 32 36 38 36
34 39 32 37 38 34 38 38 37 33 38 39 38 30 30 39 32 34 31 34 30 38 30 31 35 30 38 36
30 34 34 37 39 31 36 36 39 33 38 33 37 36 39 33 34 39 38 31 36 35 32 31 32 34 33 32
33 32 38 36 37 39 30 37 32 36 35 36 37 34 32 36 32 36 36 39 32 39 31 32 36 35 38 39
39 30 37 37 34 31 36 33 39 35 39 32 39 31 38 33 34 33 30 36 37 34 31 32 38 32 35 30
37 34 33 38 30 31 35 39 37 39 35 39 39 35 39 34 39 32 34 39 33 36 36 32 30 35 37 39
35 32 31 38 32 31 32 39 32 35 36 36 35 30 36 34 37 35 38 39 32 38 32 30 38 31 33
38 32 38 34 33 36 37 35 30 35 37 31 31 39 34 33 33 33 37 36 38 38 36 37 37 30 37 35
34 33 38 39 33 30 38 36 34 34 32 37 38 34 37 31 36 32 31 33 35 30 36 35 31 36 36

- Atlast delete the (To Hash) recipe and select (SHA1) operation and paste the previous output in the new input field, now you can see the flag in output section

Operations

sha

SHA0

SHA1

SHA2

SHA3

Shake

Compare SSDEEP hashes

Sharpen Image

Recipe

SHA1

Rounds

80

Input

39 31 39 38 39 39 35 35 34 32 38 32 36 31 38 30 34 35 31 36 31 30 34 30 31 38 38 35

39 39 39 32 39 39 33 35 32 31 33 39 31 31 33 33 36 30 36 34 37 39 30 31 31 32 36 32

39 30 37 38 31 36 37 35 37 38 35 33 35 38 30 33 39 32 35 31 36 35 33 31 32 36 38 36

34 39 32 37 38 34 38 38 37 33 38 39 38 30 30 39 32 34 31 34 30 38 30 31 35 30 38 36

30 34 34 37 39 31 36 36 39 33 38 33 37 36 39 33 34 39 38 31 36 35 32 31 32 34 33 32

33 32 38 36 37 39 30 37 32 36 35 36 37 34 32 36 32 36 36 39 32 39 31 32 36 35 38 39

39 30 37 37 34 31 36 33 39 35 39 32 39 31 38 33 34 33 30 36 37 34 31 32 38 32 35 30

37 34 33 38 38 31 35 39 37 39 35 39 39 35 39 34 39 32 34 39 33 36 36 32 30 35 37 39

35 32 31 38 32 31 32 39 32 35 36 35 30 36 34 37 35 38 39 32 38 32 30 38 38 31 33

38 32 38 34 33 36 37 35 30 35 37 31 31 39 34 33 33 33 37 36 38 38 36 37 37 30 37 35

34 33 38 39 33 30 38 36 34 34 32 37 38 34 37 37 31 36 32 31 33 35 30 36 35 31 36 36

hex 923 1

Raw Bytes

Output

6c55ec2e4cee366d29bfa2f73ddbc0e37e50f624

Flag: BFF{6c55ec2e4cee366d29bfa2f73ddbc0e37e50f624}