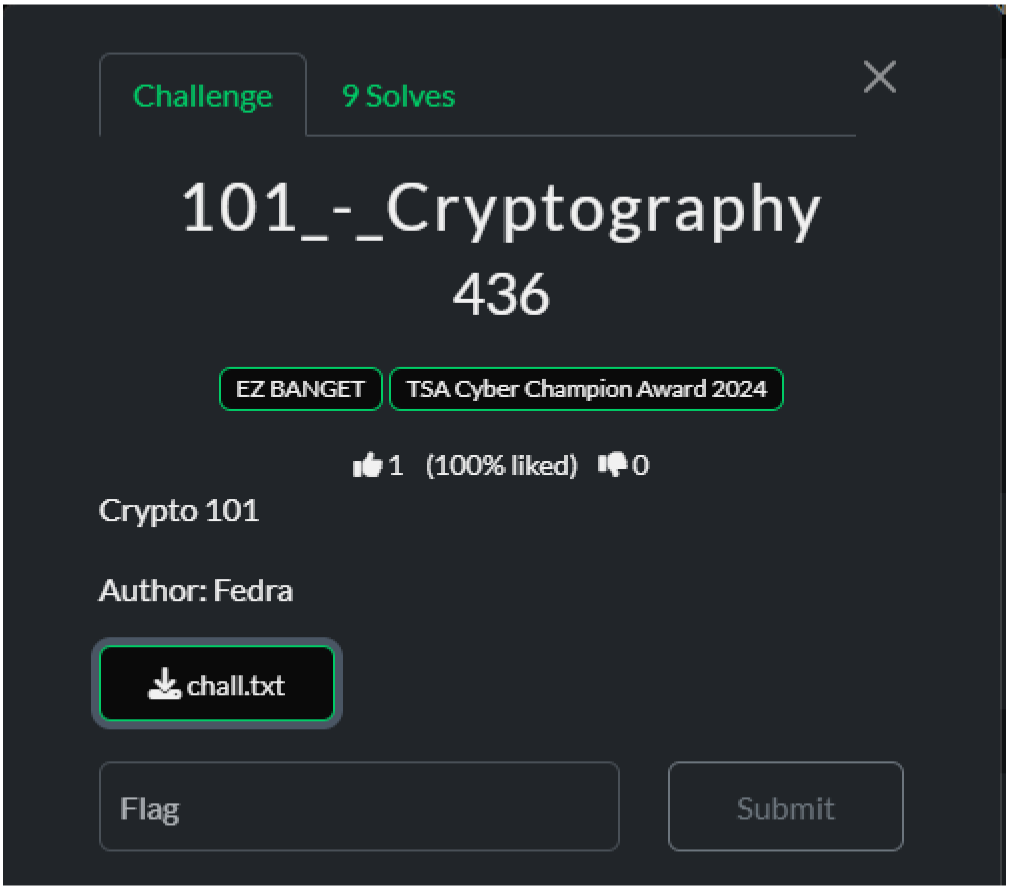
101_-_Cryptography

WriteUp by KxnZ



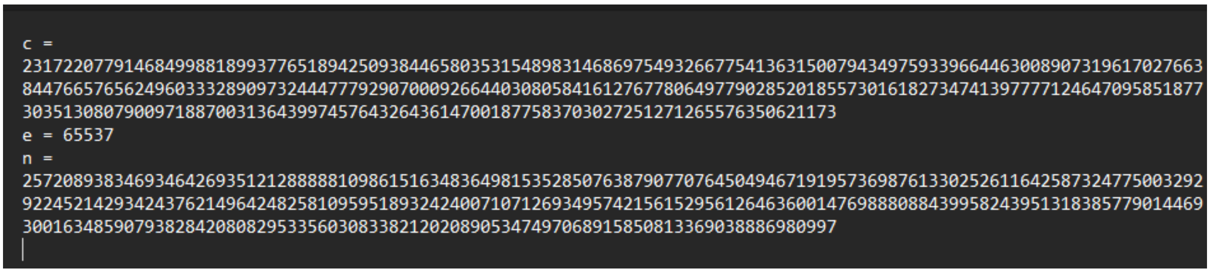
101_-_Cryptography

436

Crypto 101

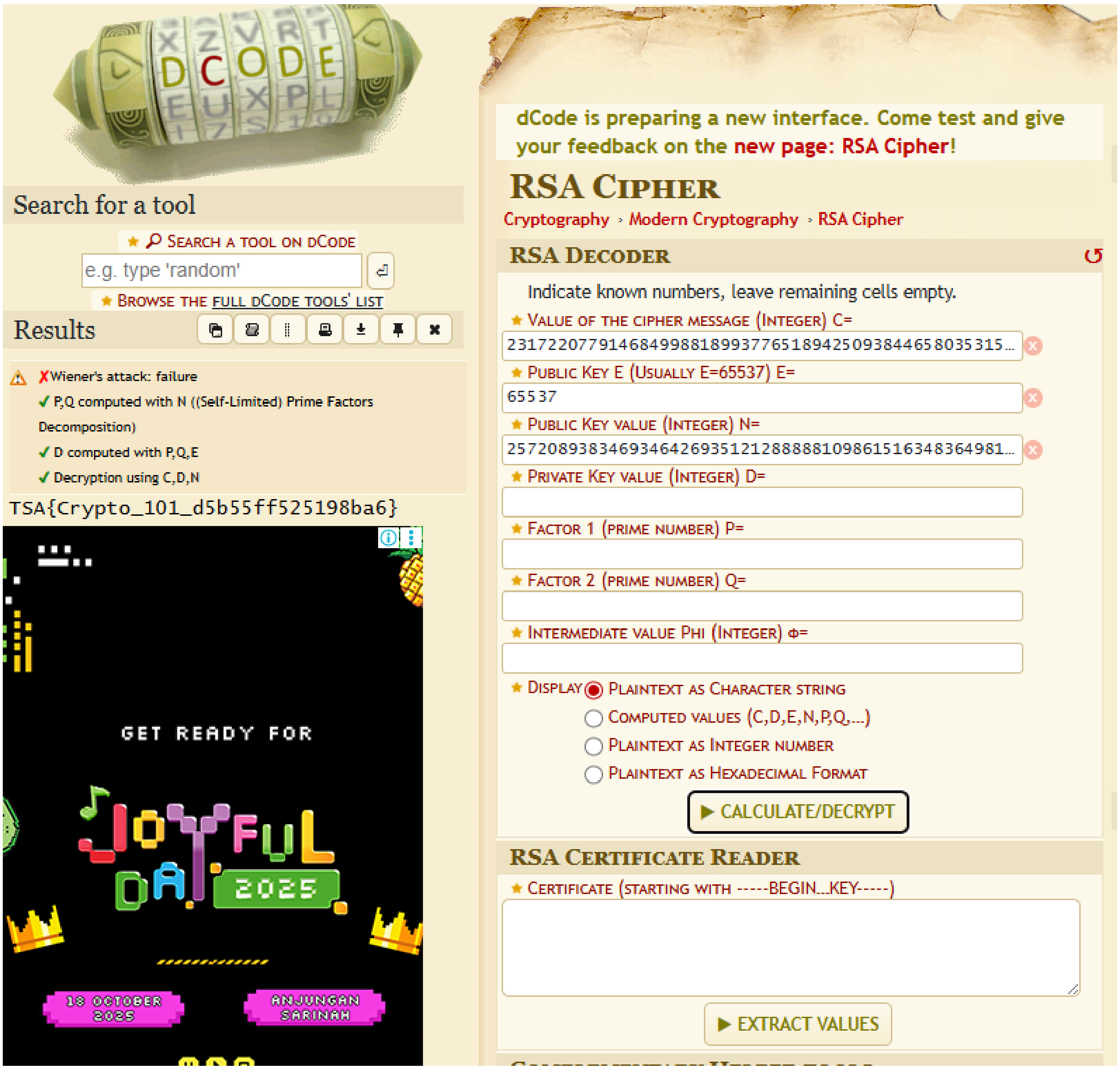
Author: Fedra

Lets download the file



```
c =
23172207791468499881899377651894250938446580353154898314686975493266775413631500794349759339664463008907319617027663
84476657656249603332890973244477792907000926644030805841612767780649779028520185573016182734741397777124647095851877
303513080790009718870031364399745764326436147001877583703027251271265576350621173
e = 65537
n =
25720893834693464269351212888881098615163483649815352850763879077076450494671919573698761330252611642587324775003292
92245214293424376214964248258109595189324240071071269349574215615295612646360014769888088439958243951318385779014469
30016348590793828420808295335603083382120208905347497068915850813369038886980997
```

The file seems to contain a RSA Cipher, so lets try to decode it with a tool called “dcode” which is a tool to decrypt/encrypt RSA Cipher



Search for a tool

★ Search a tool on dCode

e.g. type 'random'

★ Browse the full dCode tools' list

Results

⚠ ✗ Wiener's attack: failure
✓ P,Q computed with N ((Self-Limited) Prime Factors Decomposition)
✓ D computed with P,Q,E
✓ Decryption using C,D,N

```
TSA{Crypto_101_d5b55ff525198ba6}
```

dCode is preparing a new interface. Come test and give your feedback on the new page: RSA Cipher!

RSA Cipher

Cryptography › Modern Cryptography › RSA Cipher

RSA Decoder

Indicate known numbers, leave remaining cells empty.

★ Value of the cipher message (Integer) C=
2317220779146849988189937765189425093844658035315…

★ Public Key E (Usually E=65537) E=
65537

★ Public Key value (Integer) N=
2572089383469346426935121288888109861516348364981…

★ Private Key value (Integer) D=

★ Factor 1 (prime number) P=

★ Factor 2 (prime number) Q=

★ 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

▶ CALCULATE/DECRYPT

RSA Certificate Reader

★ Certificate (starting with -----BEGIN...KEY-----)

▶ EXTRACT VALUES

And there we go, we instantly got the Flag

TSA{Crypto_101_d5b55ff525198ba6}