Write up Bagian Gare

**Promotional Video – Misc SwirlL**

Pada bagian promotional video ini diputar sebuah video di youtube, jika kita menyalakan captionnya maka akan muncul sebuah flag yang dipisah mnejadi 1 huruf 1 huruf, maka agar mendapatkan flag yang utuh kita hanya perlu mendownload file subtitle dari video tersebut

Graphical user interface, application

Description automatically generated with medium confidence

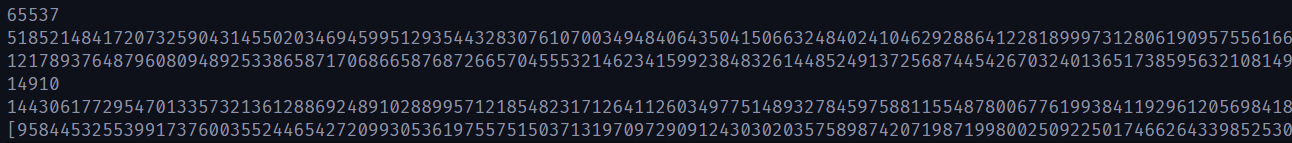
**FLAG: COMPFEST13{c4ptUr3\_Th3\_Fl4g\_cb1217bccd}**

**Snab? Yes, Snab – Cryptography SwirlL**

Diberikan dua buah file, output txt dan Snab.py

A screenshot of a computer

Description automatically generated with medium confidence



Perhatikan bahwa hasil dari potongan kode tersebut adala output.txt sehingga bisa kita cocokkan dengan nilai variabel yang ada di kode tersebut maka kita mendapat nilai s, n, a, b serta value c\_list yang sudah di enkripsi

Perhatikan bahwa

Jika kita menyelesaikan persamaan tersebut dan mensubstitusi nilai s ke persamaan b maka akan didapat bahwa

Setelah itu kit acari faktor faktor dari b menggunakan http://factordb.com/ didapat

P = 8585355817076401598233531634118333310111591335583994461813636725445826748939381988061054123

Perhatikan bahwa sehingga didapat nilai q lalu akan dicari nilai euler totient dari n yaitu

Setelah itu akan dicari nilai d yaitu nilai yang memenuhi de = 1 mod phi(euler totient(n)) dengan menggunakan modul inverse dari pycrypto.

Graphical user interface, text

Description automatically generated

Perhatikan bahwa pesan yang kita kirim berupa m\*r sehingga Ketika kita akan melakuan decrypt, nilai nya harus kita bagi dengan r agar Kembali ke nilai semula

Text

Description automatically generated

Fungsi yang menerima list cipher lalu mendecrpytnya

Setelah di decrypt didapat

A screenshot of a computer

Description automatically generated with medium confidence

Jika kita lihat fungsi tersebut memecah flag menjadi 2 bagian a dan b lalu dirubah ke bentuk bytes lalu dibuat kedalam bentuk prima

Jika kita perhatikan disitu diinisialisasi nilai r = 0, Namun r yang kita dapat pada semula ialah

Maka r ini berfungsi sebagai counter berapakali fungsi telah dilakukan, maka untuk mengembalikan nilai fungsi yang telah kita decrypt kita perlu mengurangkan nilai tersebut dengan r. Perhatikan bahwa halfa mengambil index genap dari flag dan halfb mengambil index ganjil dari flag maka kita perlu Menyusun ulang flag ke bentuk semulanya dengan algoritma berikut

Text

Description automatically generated

Maka didapat Cool! You did it! {y0U\_d1DnT\_3xpEcT\_t0\_FinD\_pQ\_4s\_a\_fl4g\_DiD\_y0u\_7e1877a801}

FLAG : COMPFEST13{y0U\_d1DnT\_3xpEcT\_t0\_FinD\_pQ\_4s\_a\_fl4g\_DiD\_y0u\_7e1877a801}