**Decoder**

Chuỗi kết thúc , đây có thể là base64

Base64 decode ra được:

I think the flag is encoded in base(64/2): JBBU2VKTFVBVIRT3NJKXG5C7KNUW24DMIVPUIZLDN5SGK4T5

Base32 decode ra được:

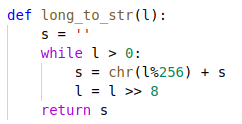
HCMUS-CTF{jUst\_SimplE\_Decoder}

**Factorization**

Parse file public.pem tìm được và

Factor tìm được và

Giải ra , viết hàm để giải ra flag:



HCMUS-CTF{smaLL\_NumbeR}

**Smalle**

Parse file public.pem tìm được và

nhỏ,

Do nhỏ nên ta thử với từng sao cho nguyên

Chạy code thử với thì nguyên

Tìm được , hexdump file xorkey ra được:

abaca4adb0c4bfaab18295849b8191b6849c9192b2959e86b59b828f998a39ee7ca4e1e25abc704452d5c6a6852c93335f043791b69d2306e06b312b

Xor với m, tìm được:

HCMUS-CTF{hello\_from\_the\_other\_sidezzzzzzzzzzzzzzzzzzzzzzzz}

Nộp thử, fail, bỏ đống z đi, flag:

HCMUS-CTF{hello\_from\_the\_other\_side}

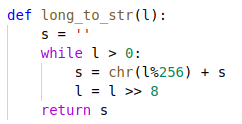
**Factorization Revenge**

Ta có:

Giải phương trình , được 2 nghiệm là và

Từ và tìm được , giải ra

Dùng hàm để giải ra flag

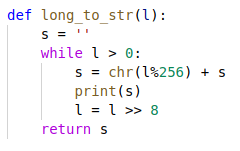


HCMUS-CTF{haaaaah\_what\_do\_you\_really\_want\_from\_meeeeeee}

**Very Secure RSA**

Dùng tool attack RSA <https://github.com/Ganapati/RsaCtfTool>, tìm được

Dùng hàm để giải ra flag



HCMUS-CTF{c775e7b757ede630cd0aa1113bd102661ab38829ca52a6422ab782862f268646}