Network Security Challenge 05 - Hard

With your help Nolan managed to convince his supervisors to trust his expertise on MACs. They have tasked him with designing a data storage solution that authenticates the messages requesting a stored secret using a MAC.
The server stores secrets and openly accessible facts, both of which are identified by a unique id. A client can request the secret or fact associated with an id by sending a message in the following format:

```
msg = b'type=funfact&number=1'
# msg = b'type=secret&number=1'
msg_enc = base64.b64encode(msg).decode()
iv_enc = base64.b64encode(iv).decode()
mac_enc = base64.b64encode(mac).decode()
return f'{msg_enc};{iv_enc};{mac_enc}\n'
```

The MAC is a CBC-MAC calculated over the message using a secret key and the IV.
Your task is to retrieve the secret that stores the flag.

Exercise 5–2 is hosted at `netsec.net.in.tum.de` at port 20205.
You don't need to use any MAC libraries to solve this challenge.
We recommend connecting to the server using `netcat (man nc)` first.
It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.