Network Security Challenge 05 - Easy

The government is beginning to doubt the competence of their "IT-Security Consultant" and has requested a demonstration of his skill. They requested implementations of the three MAC algorithms `HMAC`, `CBC-MAC`, and `CMAC`.
However, Nolan misinterpreted the HMAC task and tried to find the connection between Hash[1] and MACs. Now he is not in a condition to implement the correct HMAC algorithm, which is why you need to help him out.
The server sends you a challenge message. You need to compute all three MACs for this message using the key `KEY = b'1337133713371337'`. The server expects the MACs in the following format, where each MAC has been base64 encoded:

```
answer = f'{hmac};{cbc_mac};{cmac}'
```

> Exercise 5–1 is hosted at `netsec.net.in.tum.de` at port 20105.
> The Crypto.Cipher (pycryptodome) and hashlib (standard library) modules are allowed for this challenge.
> The Crypto.Hash and hmac modules are **forbidden** and using them will result in zero points for 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.

[1] https://en.wikipedia.org/wiki/Hashish