Network Security WS17/18
Challenge 06

Exercise 6 is hosted at `netsec.net.in.tum.de` at port 20006. Bob learned from his failure of exercise 5 so he wrote another simple FTP server. The FTP service supports the following commands: `"SEND ME THE DATA ENCRYPTED"` and `"SEND ME THE DATA"`.
Bob doesn't want unauthorized persons to get the data. Unfortunately, you don't have the key to decrypt the encrypted data. Also, Bob does not want unauthorized persons to send commands to his server so he claims "the commands must be encrypted, so only authorized persons can send commands." We provide you with an example run of the encrypted protocol (`alice.py`).

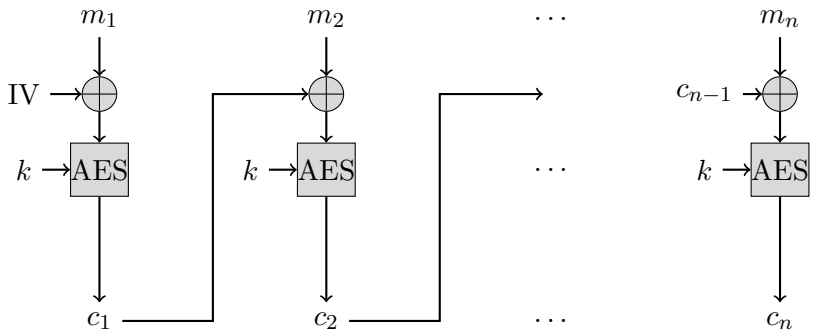
Alice sends:

```
S256,8f6f27b5dbfa2ba8367262bda7154d95,798e0ff8b06cc27c1591a4088531a64a9b76a9be87a3e944c6e7000f24f5b9f9,d29dc....
```

which corresponds to `"SEND ME THE DATA ENCRYPTED"`

Details

Bob knows about Kerckhoff's principle, consequently, there is no security problem with telling you about the used encryption algorithm and mode. Bob even publishes his server's code (but not the encryption key!).
For encryption, Bob uses the block cipher AES in CBC mode. AES operates on data blocks of fixed length of 16 Bytes. Recall the CBC mode:



Alice's message consists of four parts, separated by a comma:

`S256` , `8f6f27b5dbfa2ba8367262bda7154d95` , `798e0ff8b06cc27c1591a4088531a64a` `9b76a9be87a3e944c6e7000f24f5b9f9` ,
HSel *IV* c_1 c_2
`d29dc...`
H

As you can see from the message format, Bob does not only apply encryption, but in order to be safe from your attacks, he added an integrity check using strong hash functions like SHA256 and SHA512. HSel is a selector field to specify which hash function to use (SHA256, SHA512). H is the hash value of the ciphertext in hexlified form.
Please remember that the protocol is text- and line-based. New line is need to end a message.
Can you get the data? Hint: Block ciphers. Try do draw the CBC encryption/decryption for the example data first (do it!). Additional note: you do not need the old hash value.

More Details

All the binary data is hexlified for convenience. For example, the string `"8f"` corresponds to the byte 0x8f; one byte is represented by two characters. In this example, the IV and all AES blocks are 16 bytes long. However, the string representing them as hexlified data is 32 characters long.

Note: to run `bob.py`, on debian/ubuntu, you need to install `python3-crypto`.