After attending Com 301 lectures, Alice decides that she will only communicate with others using encrypted messages. To achieve this, she has given each of her friends a secret key in a USB and has asked them to create their own scripts to encrypt and decrypt messages using the AES symmetric block cipher.

One of TAs heard about this story and said: "**Remember, do not implement your own crypto protocols to communicate! It is hard to get all the properties right!** You must convince Alice to use one of the well-known secure messaging apps".

Since Alice is not responding to clear text messages, you need to use her encrypted channel to talk her out of her idea. To alleviate your load, the TA developed 'AliceGram' a script that creates a connection between you and Alice so that you can easily send the messages, but you are tasked with handling the encryption part. Since convincing people to use secure messaging is a hard task, 'AliceGram' includes an artificial TA which helps you creating messages addressing Alice's concerns.

**Warning:** You are not allowed to share your code with other students.

# Part 1

When she gave you your secret key, Alice told you that she will use use AES-128-bit in cipher block chaining mode (CBC). Alice encodes strings as 'utf-8' and uses PKCS padding to allow messages whose size is not dividable by the block size. *note:* usually libraries handle the padding implicitly.

Start your conversation with Alice, receiving her first encrypted message. Use the artificial TA to get convincing arguments to rely to Alice. You may need to exchange more than one message with her. You will know she is convinced when she sends you a unique "I'm convinced" message that has a token. Submit this token and your code to our grading system to pass this task.

# Part 2

Even though she said you she is convinced, Alice does not install a secure messaging app. Instead, she decides that the solution is to consider the messages in a conversation as a stream of data, and use a block cipher mode of operation which allows her to encrypt streams.

Start a new conversation with Alice as you did before. Again, use the artificial TA to get convincing arguments to rely to Alice until she is convinced and gives you a new token.

# Hints and suggestions

**Suggestion 1** : We have installed "petlib" library on the com301's VM. You can use this library for encryption.

**Hint 1** : "petlib" handles the padding on its own.

**Hint 2** : pay close attention to IVs.