IEDS 3525: Intrusion Detection and Prevention Systems

Lab4: Digital Envelope implementation on a socket communication (6%)

Digital Envelope

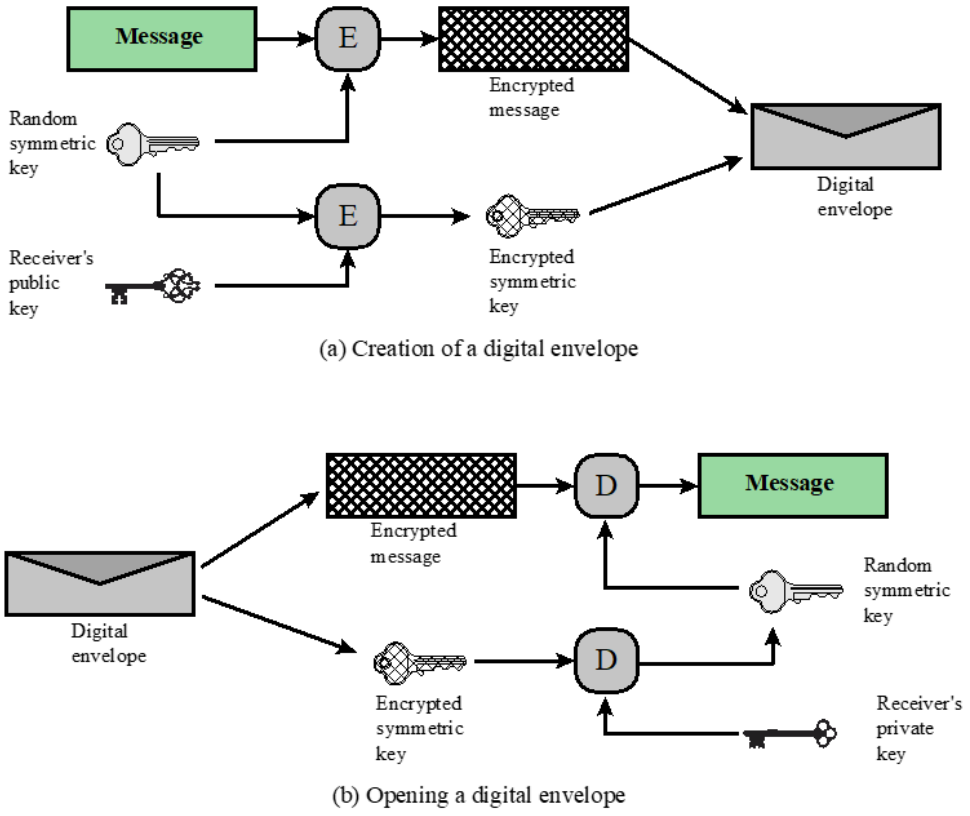
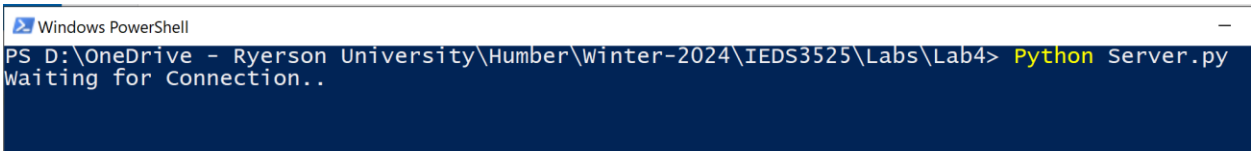


Figure 1: Creation and Opening of a digital envelope

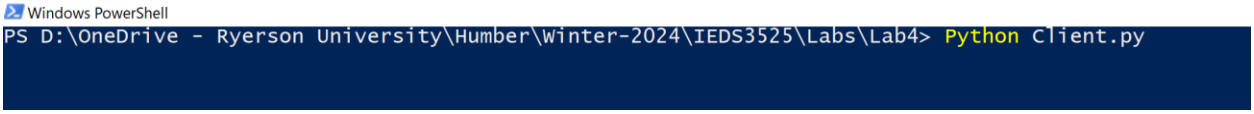
As discussed during the lecture, figure 1 shows the steps the sender and receiver take to create and open a digital envelope.

I have attached two Python files: Server.py and Client.py

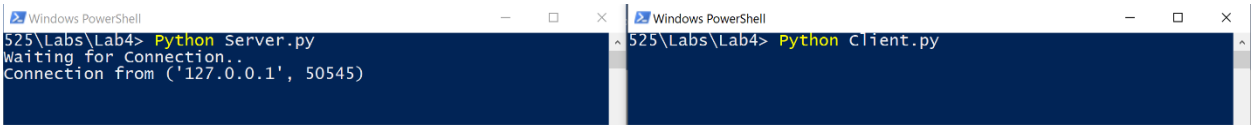
From the command prompt, first run the Server.py file as shown in the screenshot:



Now open another command prompt to run Client.py as shown in the screenshot:



Now adjust the two windows so that they are visible at the same time as the following screenshot:



Now, type" Hello" from the client window, then you will get the following:

So, basically, these two files are used to demonstrate Client-to-server communication (this is one-way communication; only the client is sending the messages). Your task is to implement the following:

1. Update the files so that the communication is both ways, meaning the server should be able to send and receive messages, similar to a chat application. **(2 Points)**
2. Generate two private key and public key pairs for both the Client and Server
   You can use the following package and function to generate the key pairs (you can use any other package if available):
   import rsa
   publicKey, privateKey = rsa.newkeys(512) **(1 Point)**
3. Update the program so that digital envelope creation and opening steps are applied, i.e., any messages sent should follow the steps of digital envelope creation, and any messages opened should follow the digital envelope opening steps. **(3 Points)**

Submission & Demonstration

1. Please upload all the Python files to the Blackboard folder. Please do not upload a **ZIP** folder.
2. **Important**: The lab must be demonstrated during the lab hour; without a demonstration, a grade of Zero will be assigned.