Vietnam National University HCM
International University
School of Computer Science and Engineering


# REPORT

## FINAL EXAMINATION

## Demo app: Attacking the key exchange protocol

**Subject:** *Fundamental Concepts of Data Security*
**Lecturer**: *Dang Tran Khanh*
**Semester/Year**: *Sem1/2021-2022*

**Student name:** *Lê Thị Thu Trà*
**Student ID:** *ITDSIU19058*

The source code includes 4 files .py:

- ***nonce.py***: This file is to generate the nonces randomly for Alice and Bob.
- **RSA.*py***: Since this is an attack on a public-key exchange protocol, I use the RSA algorithm and the `rsa` package in python to generate both public key and private key for Alice, Bob, and Malice.
- ***test.py***: This is the file for testing all the steps without GUI.
- ***app.py***: The attack involves 6 steps, so I design the demo application to display all these steps with the order below:
    - **Step 1-3**: I set Alice's identity as `Alice123` as the default. Then I create the nonce NA for Alice randomly. Alice uses Malice's public key to encrypt her identity and her nonce and sends them to Malice.
    - **Step 2-3**: Malice uses his private key to decrypt the message and then, he re-encrypt them with Bob's public key and sends it to Bob.
    - **Step 2-6**: Bob uses his private key to decrypt the message and he also generates his nonce NB randomly. Then, he uses Alice's public key to encrypt both NA and NB and tries to send it back to Alice.
    - **Step 1-6**: Malice intercepts the communication between Bob and Malice. He gets the message but he can't decrypt it since he does not have Alice's private key. Therefore, Malice takes advantage of Alice to decrypt this message for him by sending the message to her.
    - **Step 1-7**: Alice uses her private key to decrypt the message and obtain NB, then, she encrypts NB with Malice's public key and sends it to Malice.
    - **Step 2-7**: Malice obtains NB by using his private key to decrypt the message, and he re-encrypts it with Bob's public key. The result is that Bob thinks he is sharing secrets NA, NB with Alice while actually sharing them with Malice.

Each step is designed to be opened in a new window so that I can compare easily whether each step works well as I expected. You can run this demo with the command `python app.py`.