COMP 417-INTRODUCTION TO CRYPTOGRAPHY

GROUP HOMEWORK 1

NOTE: The groups are announced on CANVAS under People section. If any person is not participated in the project, do not include his/her name in the project document. Write down the names in the project report who participate in the project. **Submit your report in pdf format.**

Alice and Bob want to communicate with each other (over an insecure channel) that provides the following 5 conditions:

1. They want to be sure that their data is not modified during their communication.
2. They want to be sure that they communicate with each other not someone else.
3. They have limited resources such as memory and CPU.
4. They have some documents to share with each other.
5. Their communication should be secure with at least 128-bit security level.

You are supposed to include the following points in your project.

1. Create the communication process step-by-step. Explain each step, why, how, what etc.
2. Create a communication system that has some of the cryptographic tools (that we covered so far) as needed.
3. You have to specify which cryptographic tool is used for which condition. Specify the cryptographic tool with the version/model/type.
4. Explain why you prefer this cryptographic tool and how it provides 128-bit security.
5. Draw your 1. scheme that includes Alice, Bob, Eve(bad guy) and the cryptographic tools you used. Show the communication steps you propose for your project. Your scheme should include one file sharing step.
6. Apply 2 different attacks (of the attacks we covered so far) and show your system is secure against these 2 attacks. Explain how/why your system is secure for these attacks.
7. Show your 2 attacks on the 2. scheme
8. Name your system.

IMPORTANT NOTE: The steps of your system should be clear and each of them should be well-explained. Keep in mind that this project does not have only one solution. If your scheme provides the 5 conditions above, it is acceptable.

The 1. scheme you will draw will look like this: (You may use different tools to create this scheme.)

Alice Eve Bob

Alice calculates this: c1----------→ c1 Bob gets c1 and calculates something

c2<---------- Bob sends c2 to provide condition 1.

. . .
. . .
. . .

Explain how to calculate c1, c2 in a mathematical way.

The 2. scheme you draw will look like this: (You may use different tools to create this scheme.)

Alice Eve Bob

Alice calculates this: c1----------→ Eve conducts attack 1 --------→ c1 Bob gets c1 and calculates c2

c2<---------- Eve conducts attack2 <---------- Bob sends c2.

. . .
. . .
. . .

Explain how to calculate c1, c2 in a mathematical way.
Explain how to Eve conducts attack 1, 2 in a mathematical way.