Final Assignment

Cryptography and Cyber Security Module
Spring Semester 2024

Task 1: Record a video of 2 minutes maximum presenting what you learned through this module, what was the most exciting part and what is its added value for your studies and future career. You can use slides (maximum 2). Try to switch the camera on and respecting the GDPR regulations, the videos won't be distributed or used outside Brightspace platform and are for the evaluation purpose.

Task 2: Perform frequency analysis on the following text to try to decrypt this text step by step

CI FUANGEVUZNOA, QUHXWHIFA ZIZRALCL CL GOH LGWMA EQ GOH QUHXWHIFA EQ RHGGHUL EU VUEWNL EQ RHGGHUL CI Z FCNOHUGHTG. GOH BHGOEM CL WLHM ZL ZI ZCM GE SUHZKCIV LWSLGCGWGCEI FCNOHUL (H.V. BEIE-ZRNOZSHGCF LWSLGCGWGCEI FCNOHU, FZHLZU LOCQG FCNOHU, PZGLAZAZIZ FCNOHU). QUHXWHIFA ZIZRALCL FEILCLGL EQ FEWIGCIV GOH EFFWUUHIFH EQ HZFO RHGGHU CI Z GHTG. QUHXWHIFA ZIZRALCL CL SZLHM EI GOH QZFG GOZG, CI ZIA VCPHI NCHFH EQ GHTG, FHUGZCI RHGGHUL ZIM FEBSCIZGCEIL EQ RHGGHUL EFFWU JCGO PZUACIV QUHXWHIFCHL. QEU CILGZIFH, VCPHI Z LHFGCEI EQ HIVRCLO RZIVWZVH, RHGGHUL H, G, Z ZIM E ZUH GOH BELG FEBBEI, JOCRH RHGGHUL Y, X ZIM T ZUH IEG ZL QUHXWHIGRA WLHM.

Task 3: Bob is trying to communicate with Alice, and we want to make sure that the authentication and secrecy are both verified. Draw the most appropriate scheme to do so and pick the highly secured technique of encryption/decryption with giving an explanation. Then use RSA technique through the online tool previously seen to extract the two keys and ciphertexts for sending the following messages:

- **Hi, how are you today?**
- **Spring vibes are fabulous**
- **See you then.**

Task 4: Attached to this pdf document, you will find a text file containing Python code using a technique. Try to extract what technique exactly does the code implement, what part is for encryption, and which one refers to decryption. It uses an image as well (attached). There are two different modes that can be used in this technique, one is already implemented, try to use another one.

Task 5: Kali questions

1. What is Kali? How is it different from other Linux distributions? How does it support cyber security?
2. What command line is used for sharing your public key in a file?
3. How can you run a brute force attack?
4. How can you create targeted wordlist and run hashcat?
5. How can you get your IP computer address?
6. How can you run python code?

For all the tasks (except the 1st one), make sure you include the screenshots and outputs and relevant information and descriptions in the final submitted document which should be in Pdf Format, and you can include your video and other documents if needed.