**Enterprise Key Management Lab Work**

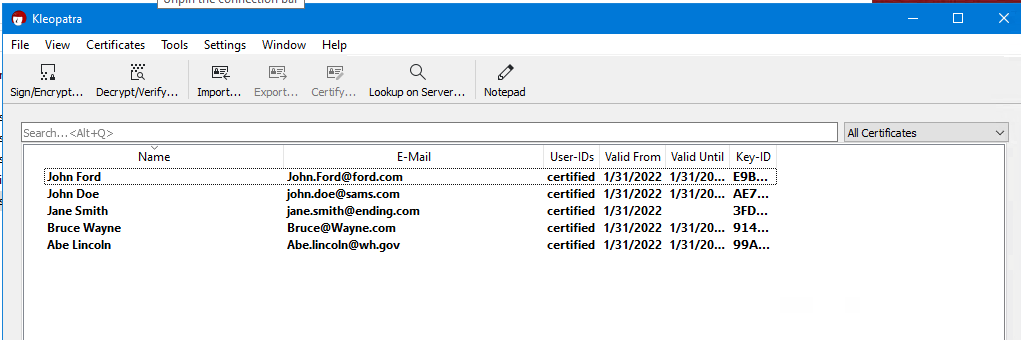
Name: PHILOMINA DORKENOO

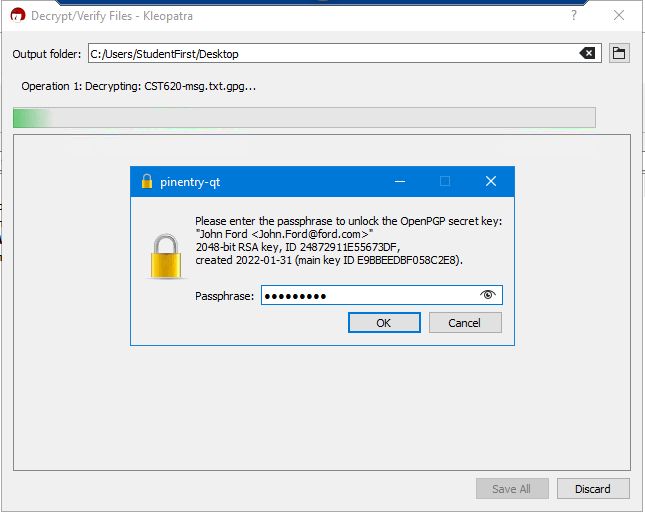
Course: CST 620 Prevention of Cyber Attack Methodologies

Date 1-18-2022

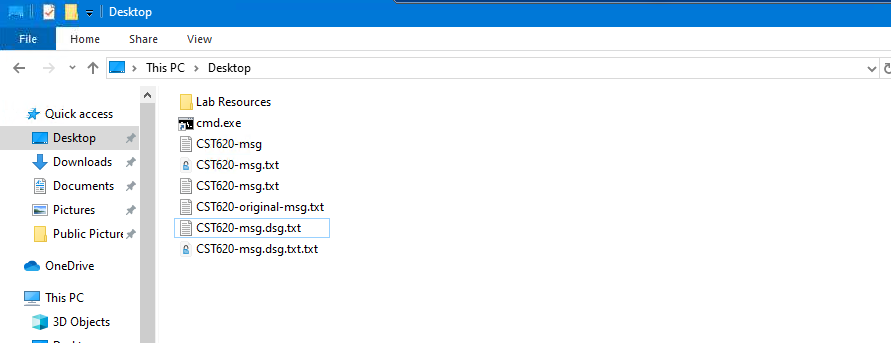
**Kleopatra**

Some of the results’ screen shots are illustrated below. Enterprise and certification options are automatically checked since they are mandatory in digital certificate process unlike Signing, Valid Until, and Authentication, which could be altered accordingly.

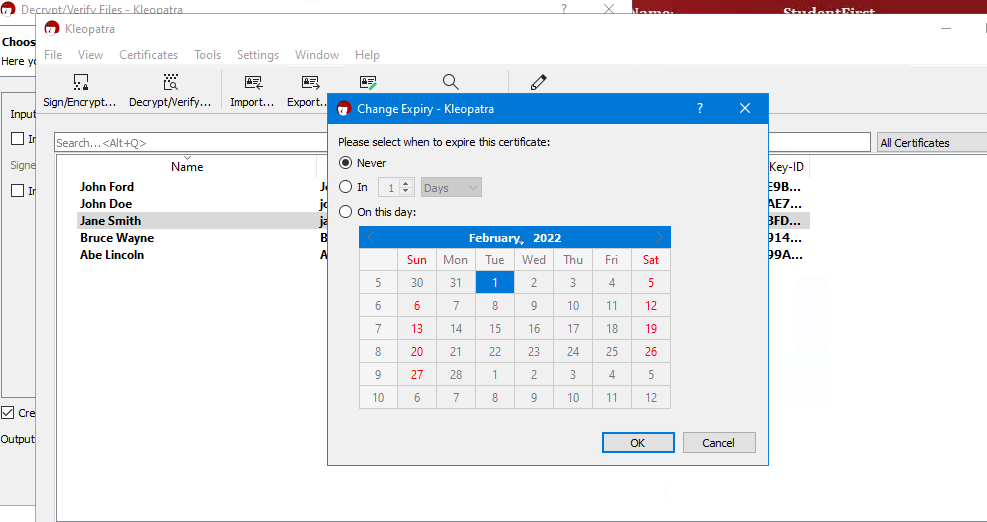


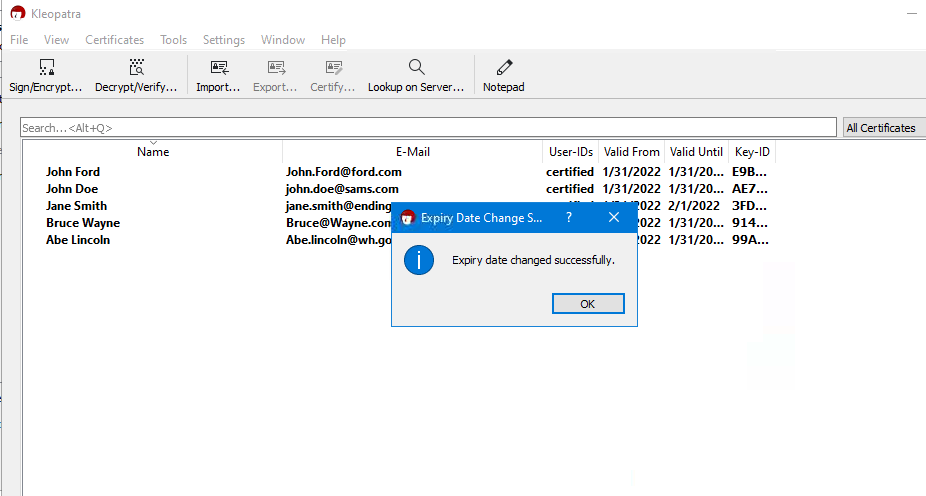


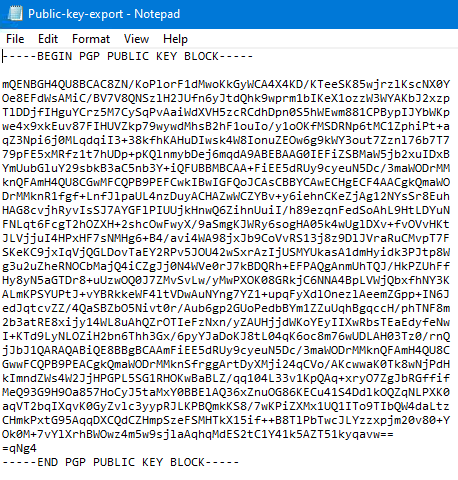
The original messages and decrypted messages are the same and they record similar sizes, but saved under separate names.

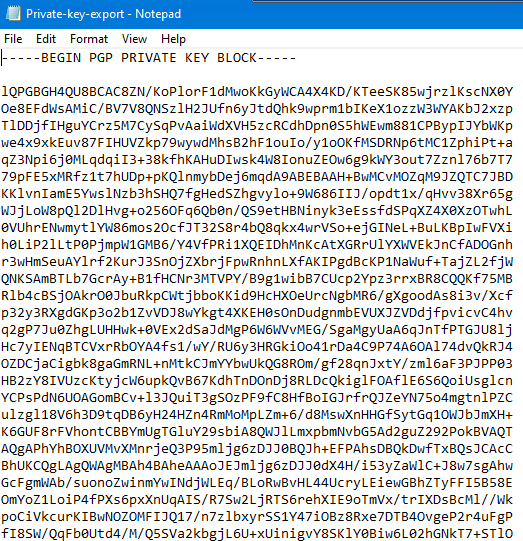


CST620-msg.txt and CST620-original-msg.txt files matched and encryption and decryption options are found on the file option of Kleopatra software. Also, CST620-msg-dsg.txt and CST620-original-msg-dsg.txt files matched and Kleopatra was utilized to sign the message, which ensures data integrity, authentication, and non-repudiation. Whenever a wrong certificate or key is utilized to decrypt and encrypt an error message pops up that inhibit accessibility. Whenever a message is tampered with, the encryption and decryption processes will generate an error code inhibiting accessibility based on initial passwords. Whenever message is tampered during transit, its accessibility is limited and encryption will generate errors.

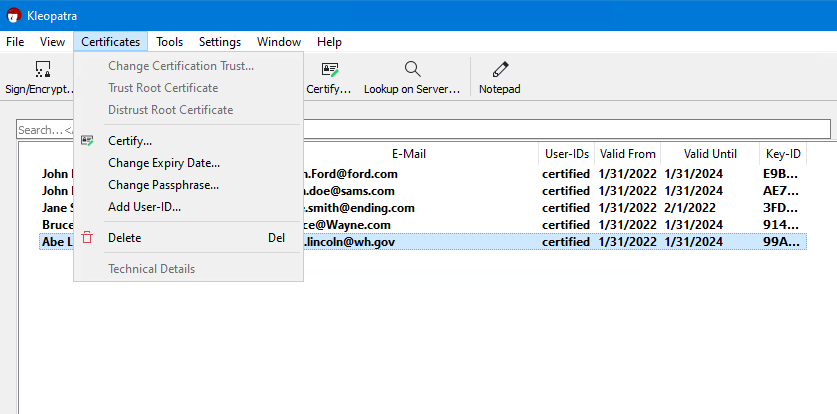


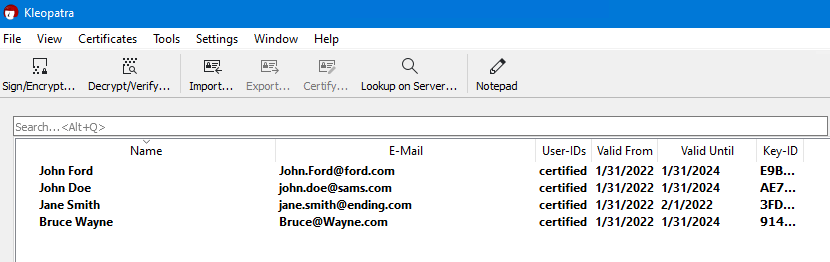


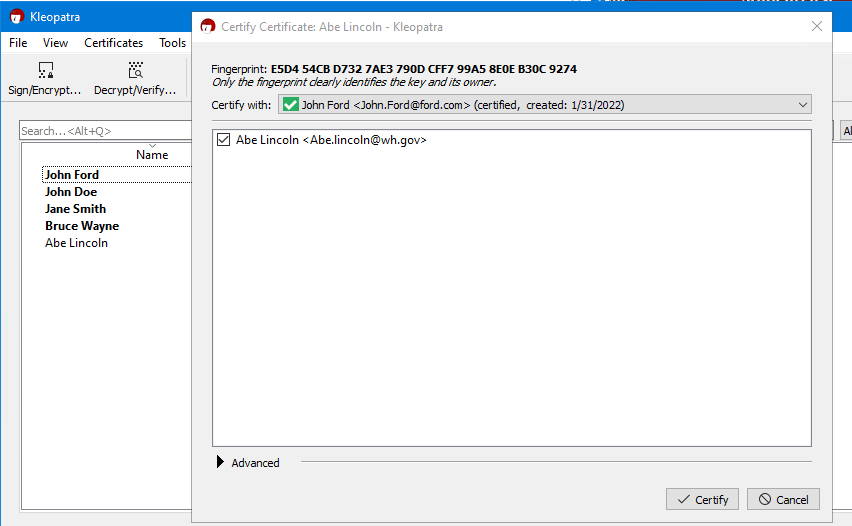






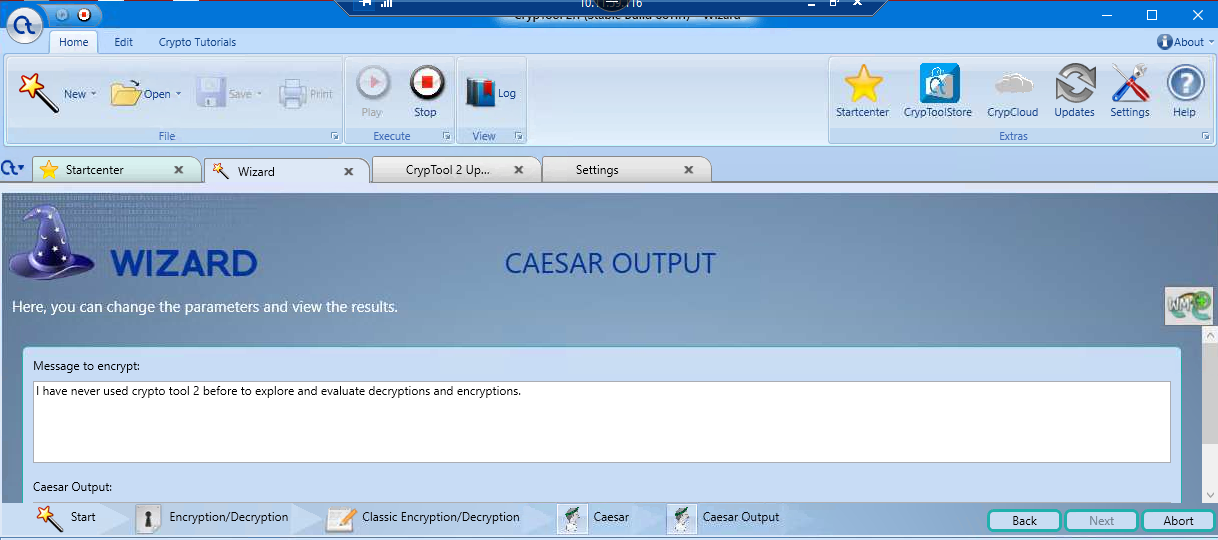


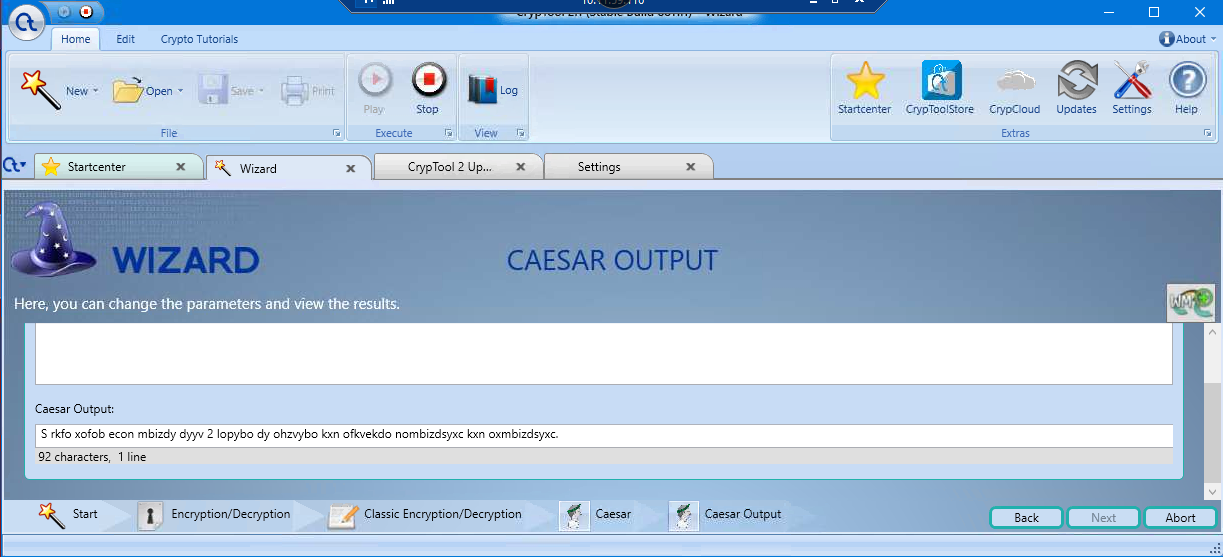


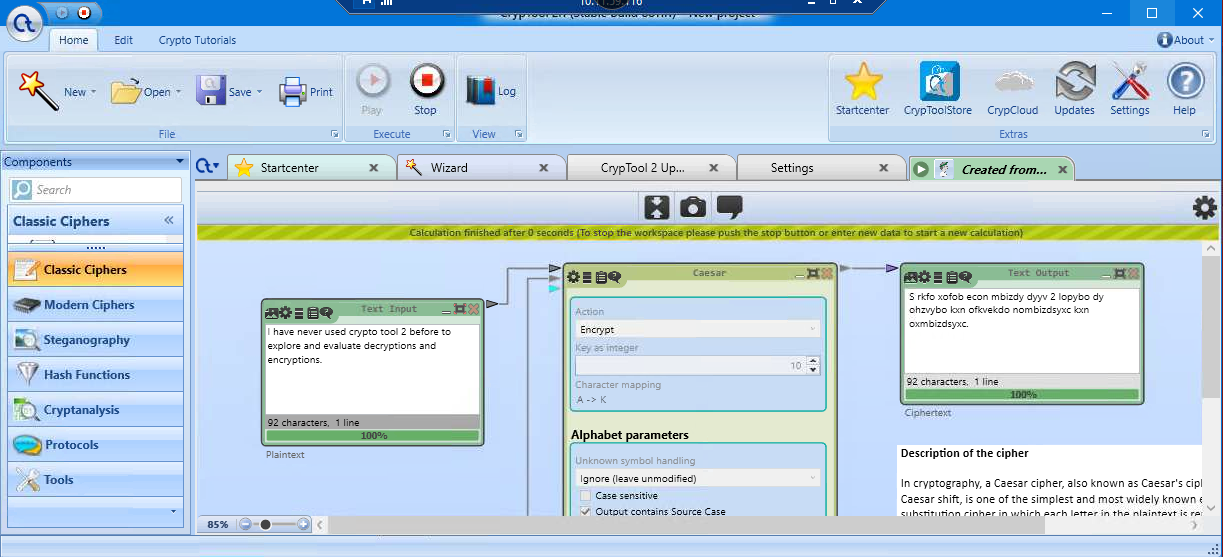


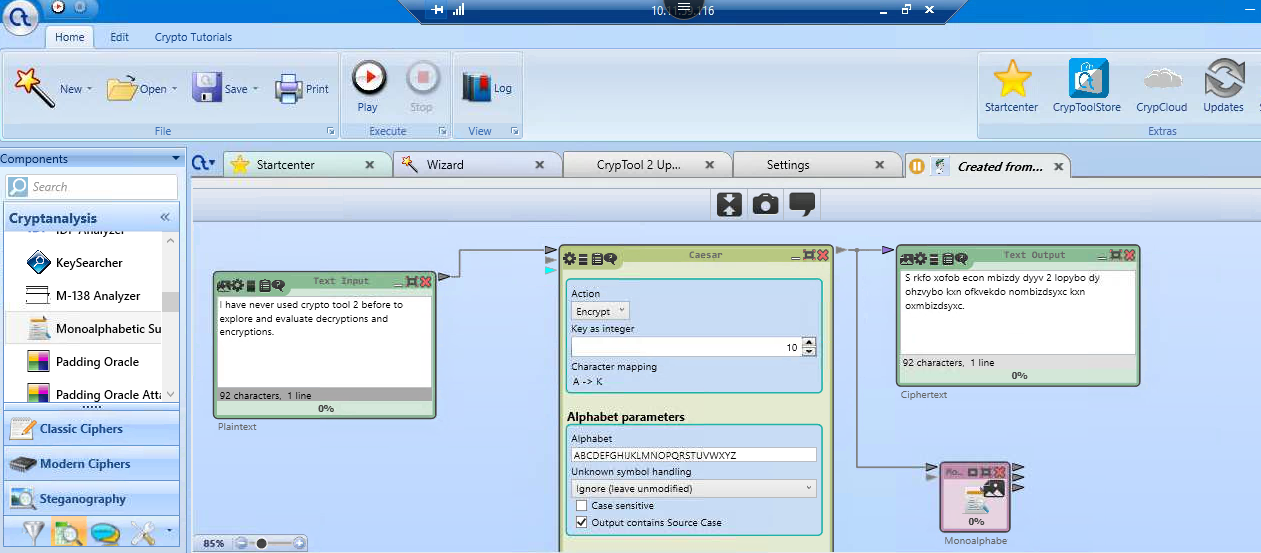
Expiry date for certificate are important since they demonstrate the validity of the keys and certificates. Whenever wrong passcodes are used access to the message becomes limited. It is essential to regularly change passphrase to ensure high level of security for the stored data or information. The management of pair key depends on encryption and decryption of the data. The management of certificate relies on expiry date and passcode update and management.

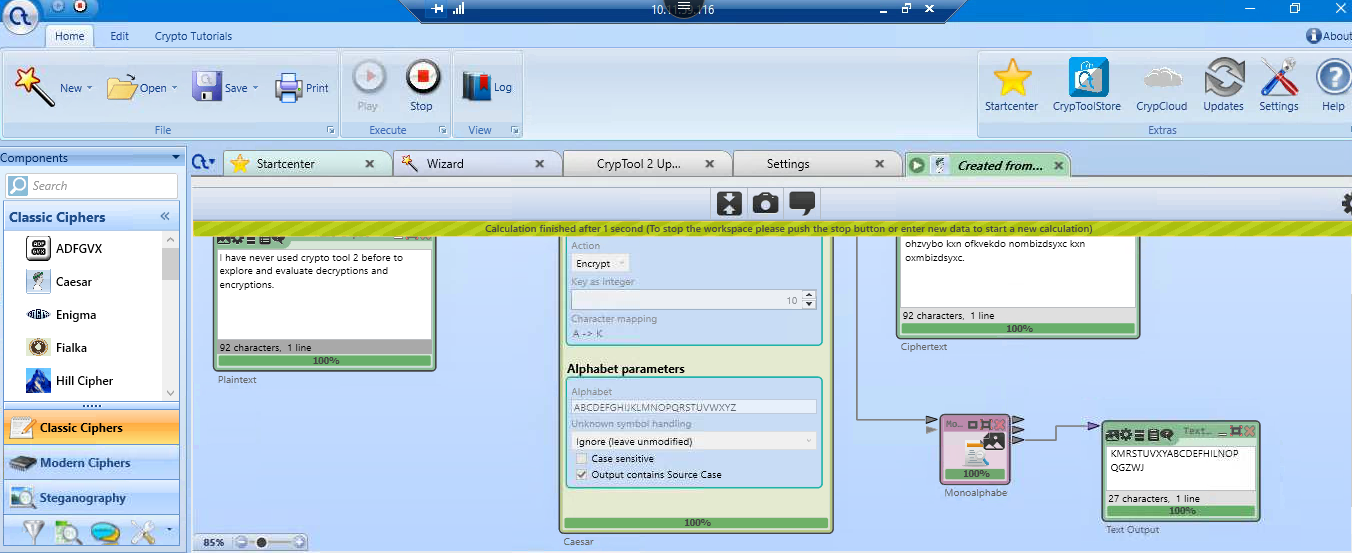
## ***Crypt Tool***

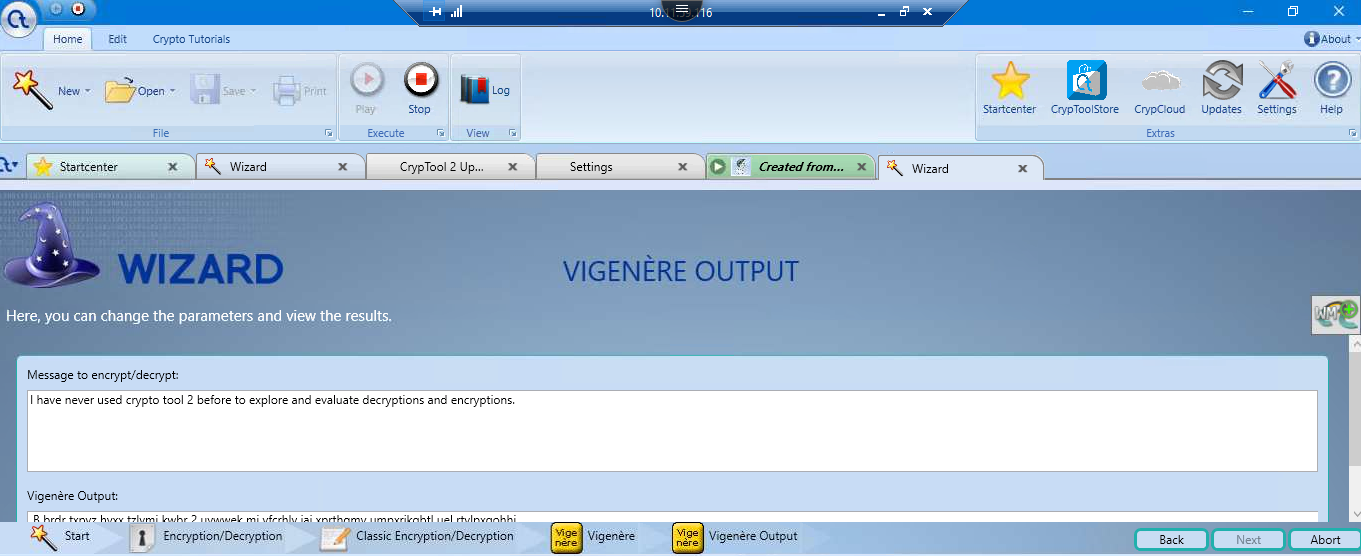


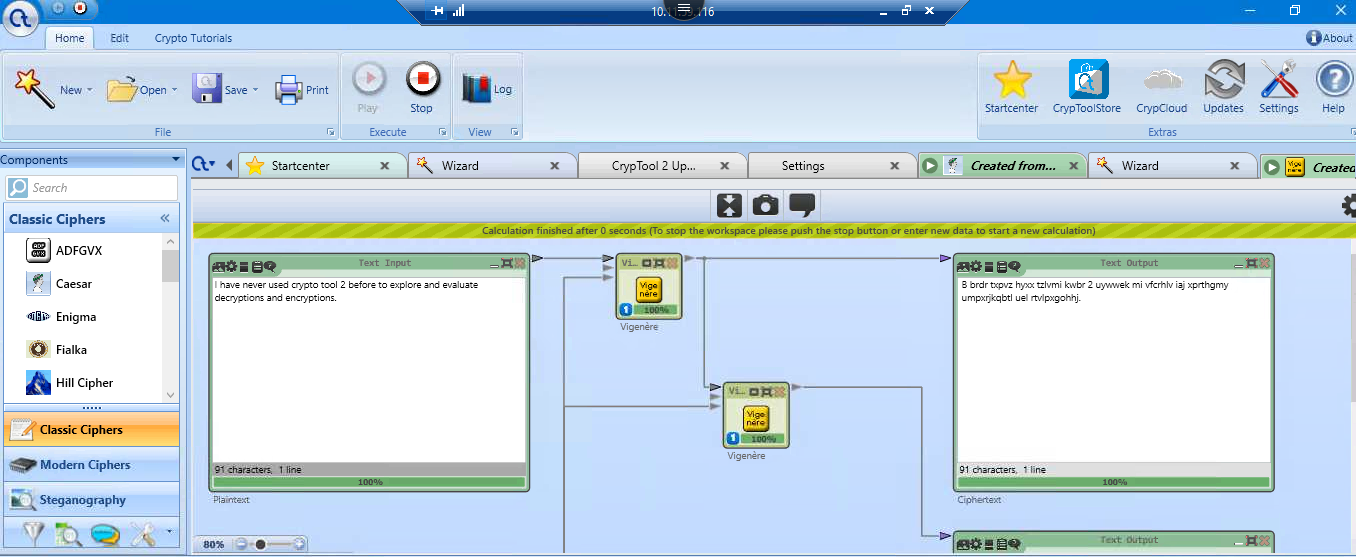


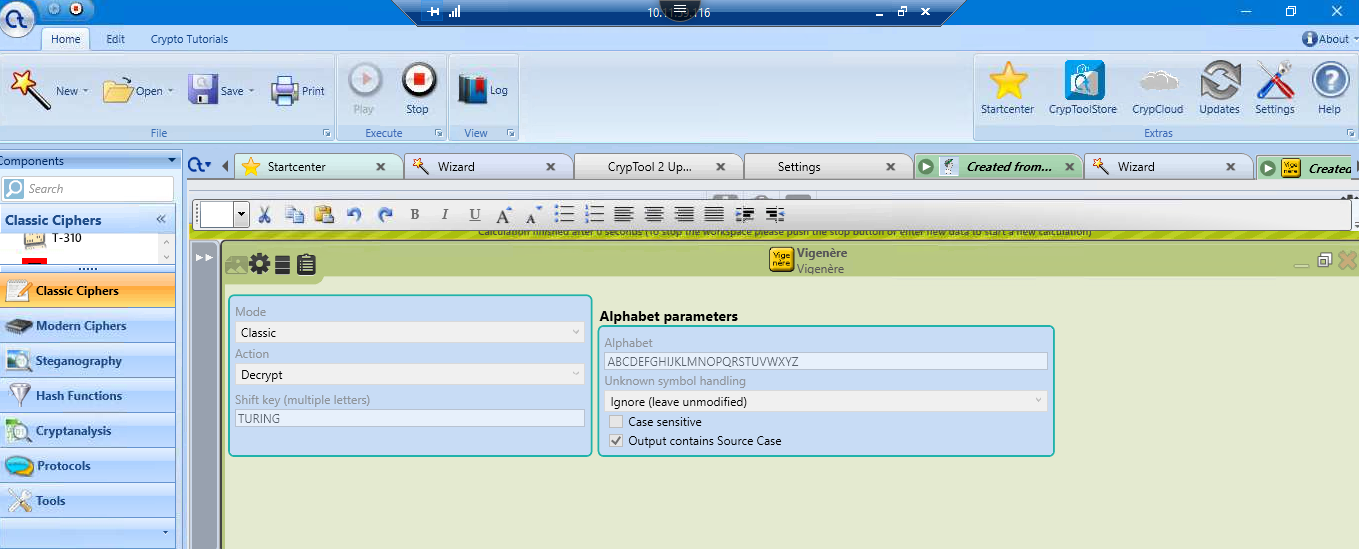


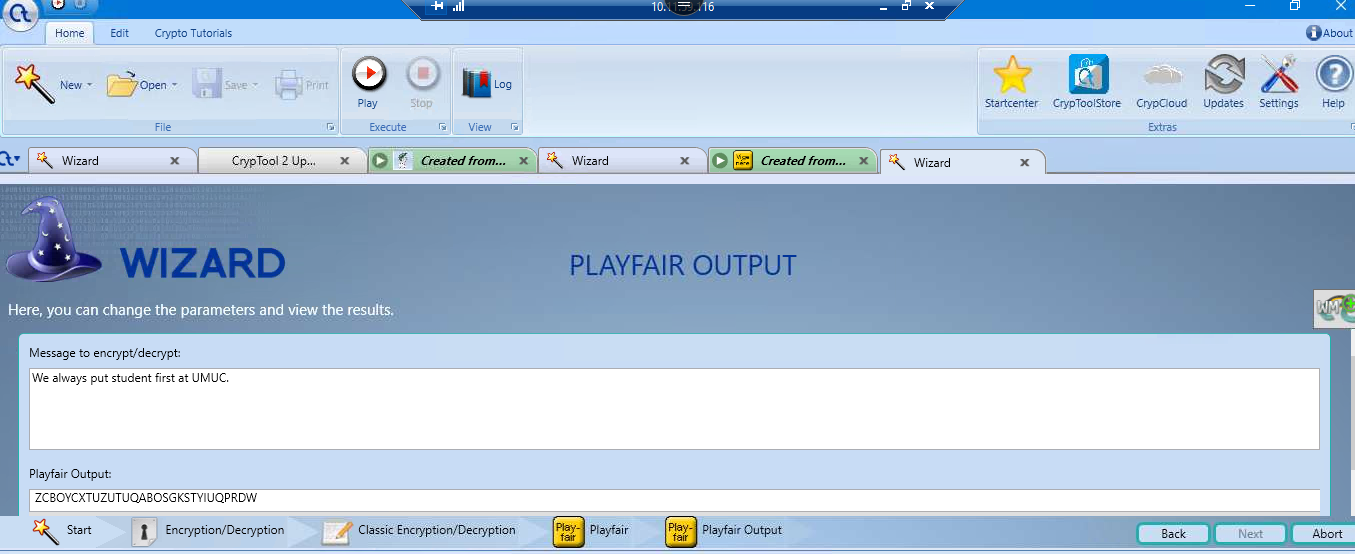


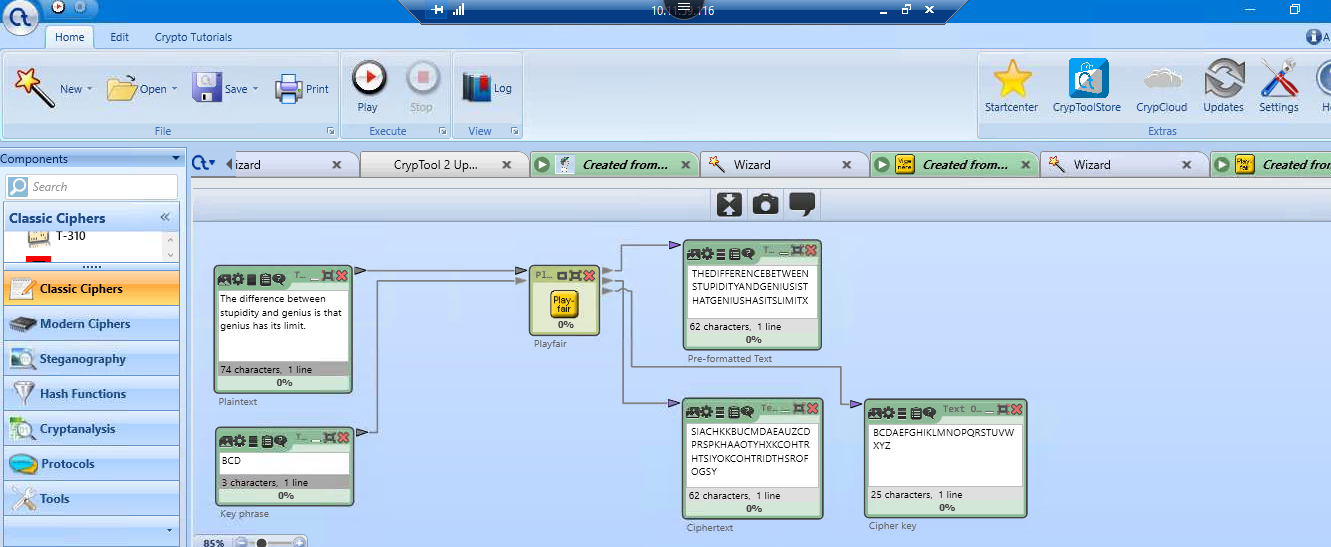






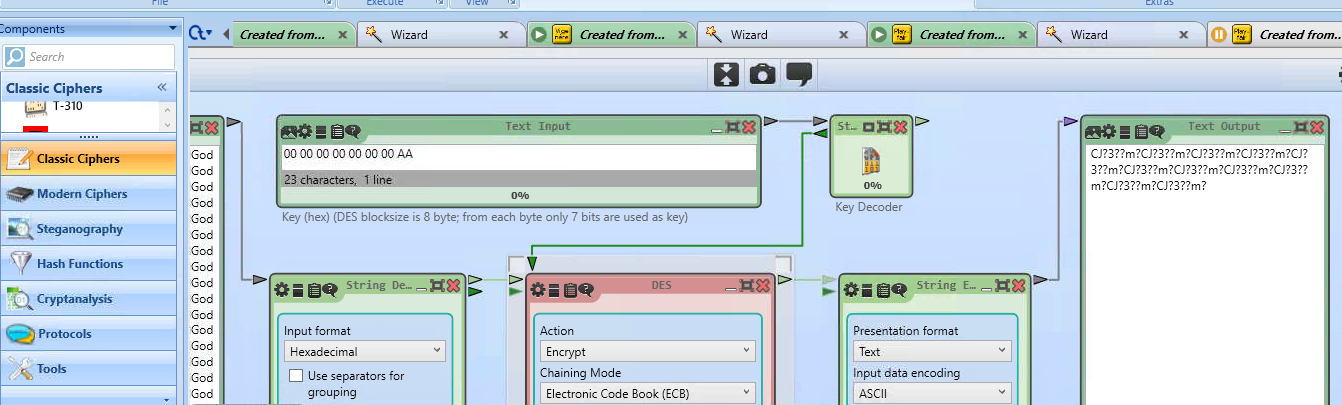


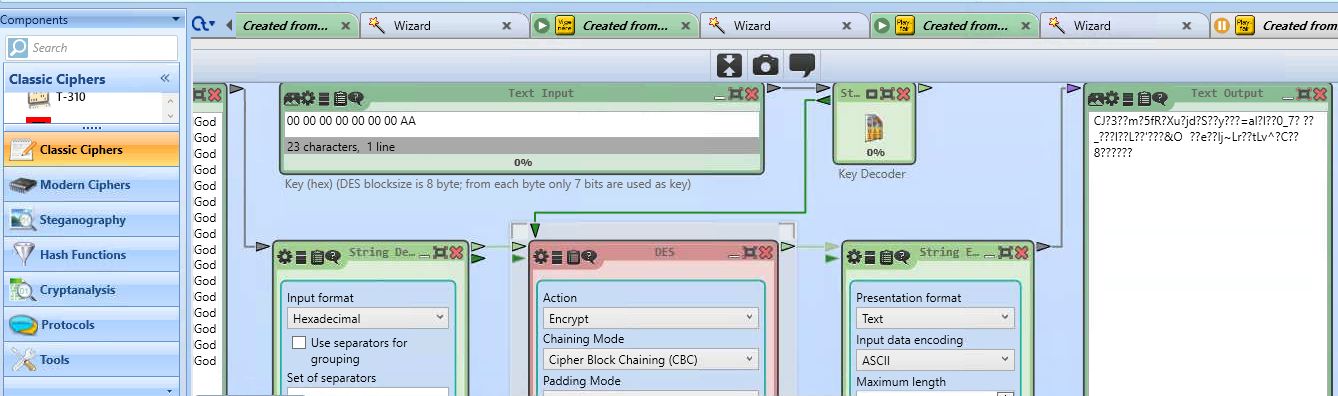




















# **References**

Alassaf, N., & Gutub, A. (2019). Simulating Light-Weight-Cryptography Implementation for IoT Healthcare Data Security Applications. *International Journal of E-Health and Medical Communications*, 1-4.

Ali, R., & Pal, A. K. (2018). Cryptanalysis and Biometric-Based Enhancement of a Remote User Authentication Scheme for E-Healthcare System. *Arabian Journal for Science and Engineering*, 1-16.

Aparna, P., & Kishore, P. V. (2017). An Efficient Medical Image Watermarking Technique in E-healthcare Application Using Hybridization of Compression and Cryptography Algorithm. *Journal of Intelligent Systems*.

Consulting, E. (2022, January 31). *What is Cryptography in security? : Asymmetric, Symmetric, and Hashing*. Retrieved from Encryption Consulting: https://www.encryptionconsulting.com/education-center/what-is-cryptography/

Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. *Multimedia Tools and Applications*, 21165–21202.

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer Networks*, 113-131.

Douse, C. H., Bloor, S., Liu, Y., Shamin, M., Tchasovnikarova, I. A., Timms, R. T., . . . Modis, Y. (2018). Neuropathic MORC2 mutations perturb GHKL ATPase dimerization dynamics and epigenetic silencing by multiple structural mechanisms. *Nature Communications*.

Kaur, P., Sharma, M., & Mittal, M. (2018). Big Data and Machine Learning Based Secure Healthcare Framework. *International Conference on Computational Intelligence and Data Science (ICCIDS 2018)*, 1049-1059.

Koreff, J., Weisner, M., & Sutton, S. G. (2021). Data analytics (Ab)use in healthcare fraud audits. *International Journal of Accounting Information Systems*, 1-51.

Masuda, Y., Shirasaka, S., Yamamoto, S., & Hardjono, T. (2018). Architecture Board Practices in Adaptive Enterprise Architecture with Digital Platform: A Case of Global Healthcare Enterprise. *International Journal of Enterprise Information Systems (IJEIS)*, 1-20.

Matheny, M., Israni, S. T., Ahmed, M., & Whicher, D. (2019). *Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril. NAM Special Publication.* Washington, DC: National Academy of Medicine.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 1-10.

Mbunge, E., Muchemwa, B., Jiyane, S., & Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. *Global Health Journal*, 169-177.

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 62-75.

Tandon, A., Dhir, A., Islam, A. K., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*, 103290.

Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., . . . Toka, L. (2020). 5G Support for Industrial IoT Applications— Challenges, Solutions, and Research Gaps. *Sensors*, 1-43.