**TOPIC : ENTERPRISE KEY MANAGEMENT ANALYSIS OF SYSTEMS IN SUPERIOR HEALTHCARE SYSTEMS**

**ABSTRACT**

Nowadays companies are moving from using simple systems in the IT department to utilizing complex systems that have various varying components used such as the operating systems used and the technological infrastructures used. With the change in complexity comes the need to create more secure systems thus necessitating the need for data encryption and decryption metrics systems to ensure the integrity and fidelity of the data and information in motion in the system.

The aim of this paper is to explore and exploit the Enterprise Key Management Plan of a collective of enterprise systems for the purpose of concluding which are the best methods in this field.

**Keywords**: Enterprise Key Management Plan, Enterprise Key Management Policy, Cryptography, Data in Motion, Ciphers, Digital Certificates

**INTRODUCTION**

Authentication is the process by which credentials are presented and validated to enable access. There are a number of different methods of authentication. Passwords are the most common type of authentication and are usually coupled with user identification (user IDs). Tokens and certificates are often used in place of passwords to provide a higher level of security. Tokens can contain unique identifiers (e.g., digital signatures or keys). Tokens can also store biometric data—for example, fingerprints.

There are several different types of combinations of authentication. Higher levels of security are generally associated with more levels of authentication (multifactor). For example, two-factor authentication might include a token and a password. Kerberos is a protocol for authentication made up of two components: a ticket (distributed by a service) for user authentication and a key that is developed from the user's password. Another authentication scheme is the Challenge-Handshake Authentication Protocol (CHAP), which uses a representation (hash) of the user's password to authenticate

**CHAPTER 1: ENTERPRISE KEY MANAGEMENT PLAN**

This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.

Access control is the process by which permissions are granted for given resources. Access control can be physical (e.g., locked doors accessed using various control methods) or logical (e.g., electronic keys or credentials). There are several access control models, to include:

* **Role-based access control:**Access is granted based on individual roles.
* **Mandatory access control:**Access is granted by comparing data sensitivity levels with user sensitivity access permissions.
* **Attribute-based access control:**Access is granted based on assigned attributes.
* **Discretionary access control:** Access is granted based on the identity and/or group membership of the user.

The access control model used is determined based on the needs of the organization. To determine the best model, a risk assessment should be performed to determine what threats might be applicable. This information is then used to assess which model can best protect against the threats.

Application security testing is performed by organizations to ensure that their applications and software contain no errors or vulnerabilities and interact with users and other applications securely. According to the National Institute of Standards and Technology's guideline document (Scarfone et al., 2008):

Application security assessment should be integrated into the software development life cycle of the application to ensure that it is performed throughout the life cycle. For example, code reviews can be performed as code is being implemented, rather than waiting until the entire application is ready for testing. Tests should also be performed periodically once an application has gone into production; when significant patches, updates, or other modifications are made; or when significant changes occur in the threat environment where the application operates. (p. C-1)

The application security testing techniques can be broadly classified into white box and black box techniques. White box techniquesare implemented by directly analyzing the source code, whereas black box techniques are implemented using the binary executable code.

**CHAPTER 2 : ENTERPRISE KEY MANAGEMENT PLAN POLICY**

Encryption has been used for decades, and much has changed in the last few years. In today's ultramodern tech world, system security is any entity's most essential and efficient aspect. Every piece of data is valuable in its own right, and we cannot afford to leave it vulnerable and exposed in the absence of any security or encryption mechanisms. Cyber-attacks are common in both government and private companies and agencies. These attacks endanger the infrastructure of information security systems. It is critical in the cyber world to prevent these types of attacks to ensure data integrity and authentication. These threat actors are known as hackers, and they can come from anywhere. Financial gain, blackmail, making a political or social point, and intellectual challenge can all motivate these attacks (Andreasen & Organization, 2014).

**Purpose**

This paper will go over the enterprise key management gaps, rules, and risks in Superior Healthcare's cryptographic keys system. In the healthcare industry, information security is critical. Nonetheless, because of the vulnerability in most cryptographic keys, many collaborations, such as SHC, are responsible for implementing security strategies. This is why a certified technologist is now available, allowing administrators to encrypt data at rest, data in use, and data in motion. To that end, there are numerous sophisticated access control and authentication mechanisms in place to ensure that only authorized users can encrypt and decrypt sensitive data. The primary goal of enterprise key management is to identify any flaws in critical management systems and recommend risk mitigation for electronic healthcare software.

**Key Management**

Enterprise Key Management is a term used to describe the provision of encryption keys across a wide range of operating systems and databases. According to Townsend, encrypting the data is the best way to protect the integrity of sensitive data. Many operating systems now make it simple to encrypt data. Some do it automatically, and if you have a small database or sensitive data stored in one location, it becomes elementary and straightforward. Superior Healthcare is one of the leading healthcare providers in the United States of America. Data availability, integrity, authentication, and protection are required when implementing an e-PHI web-based electronic healthcare application system (Parkinson, Crampton, & Hill, 2018).

Data encryption is a significant safeguard in databases, file systems, and applications that transmit data. Best practices and their responsibilities, according to Pal, are critical for system security architects. These procedures will protect billing, payments, and insurance claim processing confidentiality and integrity. It will safeguard patient information protected by the Health Insurance Portability and Accountability Act (HIPAA). Within Superior Healthcare's cryptographic system, enterprise key management can identify critical management gaps, risks, solutions, and challenges.

The issue with crucial management cryptography is that it cannot be altered or corrupted in any way. This helps to validate the message's authenticity, confidentiality, and integrity. Cryptography encrypts data by converting it into random alphanumeric characters using complicated algorithms. Many of the complex cryptography algorithms are known to the public, which resides in privacy and critical protection. Superior Healthcare (SHC) faces more Enterprise Key Management challenges in protecting sensitive information because it stores, transmits, and shares data via media with insecure network systems. Cryptography, in this opinion, is the most effective tool for increasing confidentiality and preventing unauthorized data disclosure. Cryptography's goal is to conceal information from unauthorized individuals. This is not to say that cryptography is impenetrable or completely secure. In fact, with the right tools and enough time, it is possible to break into an encrypted cryptography system.

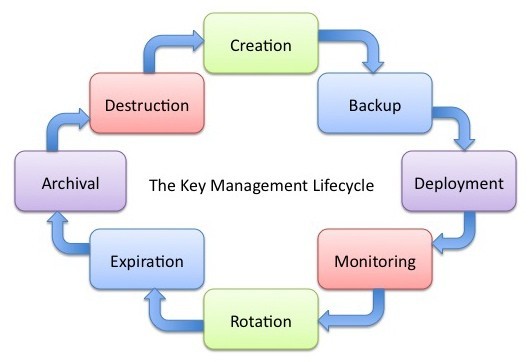
**Rules for Key Management**

When discussing fundamental management rules within an enterprise, it is necessary to consider the decentralization process of encryption and decryption. This is the first step in developing and implementing a data security strategy for Superior Healthcare (SHC). In this case, the decision has been made to implement it locally or centrally on a separate encryption server and distribute it throughout the enterprise. If the processes are distributed, the critical manager must ensure the safe and secure distribution and management of keys. This encryption and decryption approach has some advantages. These include increased performance, increased availability, and improved data transmission (Andreasen & Organization, 2014).

Supporting multiple encryption mechanisms is another best practice or rule for key management. Although implementing the best available encryption mechanism was beneficial, it is always preferable to support numerous encryption technologies. This is especially important for Superior Healthcare (SHC) during mergers and acquisitions. For example, business partners in the same ecosystems, such as Kaiser Permanente and SHC, must collaborate to create a security system that supports the healthcare standard of the encryption algorithm. This ensures that the organization accepts any new government regulations and rules.

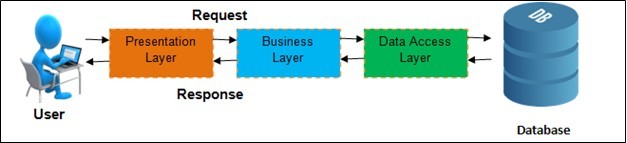
**Key Management Lifecycle**

A key is a number that allows for variation in encryption. It is either kept private or changed regularly. To ensure that the key is not compromised, it should be managed using proper procedures and protocols from the beginning to the end of its lifecycle. As a result, the key must be generated in a secure environment (Hardened System) and may be required to comply with requirements for separation of duties (Sion, 2010).



In most cases, the keys generated during the lifecycle are symmetric and should be of sufficient strength and dependability. The number of bits in a critical measure its power (Gibson, 2017). Data protection, according to the National Institute of Standards and Technology (NIST SP 80057),

The strength of the key and the mechanisms and protocols used in conjunction with those keys are all factors in cryptography (Strokes,2017).



The Data Tier can be technologically, linguistically, logically, and platform-independent but must constantly interact with one another for the software application to function.

**Key Components**

To begin, SHC used a variety of operating systems and network devices to enable remote access to all business functions. This necessitates properly securing permits and distributions and authentication mechanisms and modernizing vital in-depth concepts and best practices for crucial enterprise management. Each department has distinct IT requirements and, as a result, different vulnerabilities. To properly assess and demonstrate each departmental business's capabilities, weaknesses, and associated risks, they must first be well-defined to function. These departmental business functions include subsets and complexities that are best summarized in the following categories: Administration, finance, clinical, and management are all areas of expertise. Human resources, healthcare staffers, payroll, IT support, and scheduling are all part of the administration. Finance encompasses the organization's logistical and economic functions, including budgeting, billing and collections, and procurement. There are numerous organizational components in the healthcare business function. These organization divisions handle medical records, patient intake, and care plans.

Consider the CIA triad first for a high-level, top-layer network view diagram of systems at SCH. Confidentiality, Integrity, and Availability (CIA) are acronyms for Confidentiality, Integrity, and Availability. It is a model intended to guide information security policies within an organization. To avoid confusion with the Central Intelligence Agency, this model is sometimes called AIC (Availability, Integrity, and Confidentiality) (Rouse 2014).



CIA Triad

**Data at Rest**

The primary fundamental aspect of SHC is data. The movement of data across multiple networks with encryption is critical for SHC. Encryption data is stored in an unreadable ciphertext format. An attacker cannot read encrypted network traffic or encrypted data stored on a system. In contrast, if the information is sent in cleartext, an attacker can intercept and read it using a protocol analyzer. Any data stored on end-user devices such as computers, phones, and other electronic devices is data-at-rest (NIST, 2017). Human error and other motives, such as identity theft and other fraud, pose unintentional and intentional threats to this data. Data loss and theft are two common threats to end-users. Other hazards include insider attacks, which occur when an employee attempts to access sensitive information. Sensitive data on another employee device, or an attacker installs malicious malware on the device, giving attackers access to the information on the device and jeopardizing its confidentiality (NIST, 2007). The main security measures that can help maintain confidentiality are encryption, authentication, backup, and disaster recovery systems.

**Data in Use**

The term "data in use" refers to an end user's data on a computer, phone, or other electronic devices. While in use, data is not encrypted. If the information is encrypted, the application will decrypt it and store it in its memory while it is running (Gibson, 2017). Malware attacks sent by attackers to end users are the most common threat to end-users. Furthermore, data can be deleted while being exploited. They maintain data consistency, accuracy, and trustworthiness throughout their life cycle (Rouse 2014). This process ensures that unauthorized individuals cannot alter data while in transit, storage, or use. Furthermore, including checksums and cryptographic checksums with some data may aid in data integrity verification (Roebuck, 2012).

**Data in Motion**

Data in motion or transit refers to information that has been sent over a network or the internet. When multiple users access the transmitting resources, it is common to encrypt the data. The availability of data is critical. This means that data must be accessible at all times and from any location when needed. According to Vesperman, as multiple users access the transmitting resources, data may be exposed to various threats, and it is critical to ensure that the data is only accessed by the intended users (Vesperman, 2002). Encryption and authentication can be used to reduce data-in-transit attacks. Furthermore, additional security software and hardware, such as firewalls and proxy servers, prevent malicious actions, including denial-of-service (DoS) attacks and network intrusions

# Implementation

There are two approaches to key management. They form two types of keys: public and private. Asymmetric encryption algorithms are used by both public and private keys to ensure the creation of match pairs (Gibson, 2017). When a public key encrypts information, only the matching private key can decrypt it, and when a private key encrypts information, only the matching public key can decrypt it (Gibson, 2017). The private key is always kept confidential and is never shared, whereas the shared certificate freely shares the public key (Sion, 2010).

Public Key Infrastructure (PKI) refers to a collection of technologies used to request, create, manage, store, distribute, and revoke digital certificates (Gibson,2017). Asymmetric encryption, in other words, is dependent on the use of certification for purposes such as protecting emails and internet traffic with SSL and TLS. SHC must safeguard sensitive data from a doctor's office, on-site and off-site laboratories, and patient information such as medical records, billing, and other logistics (Gibson,2017).

A digital certificate is required for PKI to function. This certificate works similarly to a license, forming electronic identification of the website and organization. PKI ensures that the identities of the two parties are verified by certificates when securing the connection between two communicating devices (Gibson,2017). These certificates can be obtained for internal use, commercial sites, or larger scale. During PKI, only the digital certificate owner has access to the private key, and they have complete control over where and who has access to the public key. The certificate is required to distribute the public key to the owners (Parkinson, Crampton, & Hill, 2018).

Root CAs, in my opinion, must be installed by two or more people who lack the necessary knowledge to make the changes on their own (Microsoft,2003). A trusted root CA is another name for a root CA. Before installing the trusted origin, a file for SHC must be created and placed in the c: windows directory; this file will perform basic configuration settings during installation. This is the procedure that SHC would follow, according to Microsoft (Sion, 2010).

**Operation**

SHC has identified the need to secure their data, and some methods and procedures can assist them. All of this boils down to two ideas: hashing and encryption. A hash is a number generated by performing a calculation on data such as a patch, massage, or file. Gibson (2017) defines formal Hashing produces a fixed-length string of bit or hexadecimal characters that cannot be reversed back to the original data. MD5 and the Secure Hash Algorithm (SHA) are popular hashing algorithms (Gibson, 2017). MD5 is a popular hashing algorithm that generates a 128-bit hash commonly displayed in the hexadecimal format of a stream of 1s and 0s. SHA is yet another hashing algorithm. Furthermore, passwords are frequently stored as hashes. When a user creates a new password, the system computes and stores the password's hash (Andreasen & Organization, 2014).

Encryption ensures the authenticity and confidentiality of data. There are two types of encryption: asymmetric and symmetric. Most symmetric algorithms encrypt data using a block cipher or a stream cipher. Block ciphers encrypt data in specific block sizes, such as 64-bit blocks (Gibson, 2017). There are numerous cipher modes of operation. These include Electronic Codebook (ECB), the most basic type of cipher operation in which the algorithm divides the plaintext into blocks and encrypts each block with the same key. Cipher Block Chaining (CBC) encrypts data using symmetric block ciphers, IV, and OXR. Effectively, counter mode (CTM) converts block cipher to stream cipher (Roebuck, 2012).

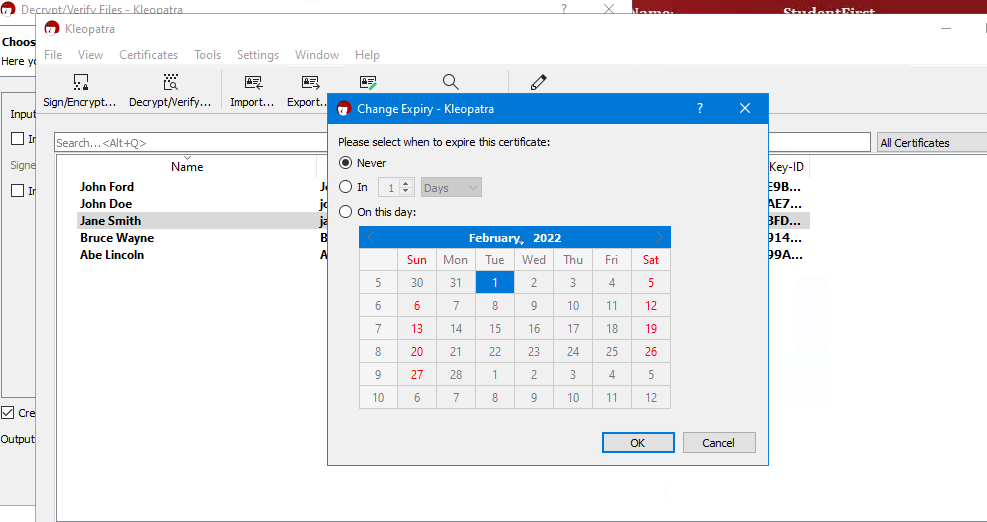
The Data Encryption Standard (DES) and Triple DES are two other symmetric block ciphers. For many years, DES was widely used. It encrypts data in a 64-bit block and a 56-bit key to generate ciphertext (Gibson, 2017). 3DES is another symmetric block cipher designed to improve on the weaknesses of DES. It encrypts data in three passes using the DES algorithm and multiple keys. 3DES employs keys with 56 bits, 112 bits, or 168 bits (G.

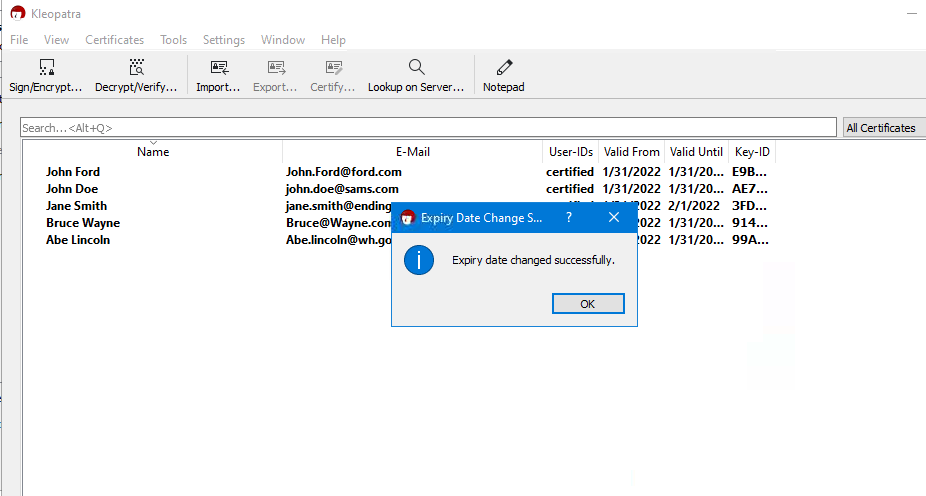
**Maintenance**

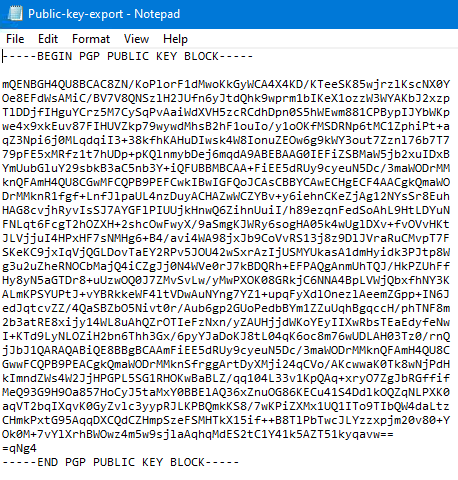
Securing personal health information (PHI) is critical for SHC employees. SHC must ensure their client's network resource's confidentiality, authenticity, integrity, and availability. SHC network access permissions may need to be modified and updated/patched regularly to prevent vulnerabilities in both client and employee systems. Electronic healthcare records are on the rise in SHC (EHR). During an outpatient visit, physicians directly enter patient information into computers. This creates new threats and security concerns. Strong encryption and access control measures are required to address these new threats and problems. ACLs (Access Control Lists) are a system of explicit and implicit permissions that are directly placed on a file or program to limit access. Another approach is to use role-based access control (RBAC), which defines network access based on the roles of individual users within an enterprise. It allows the right employees to access the information they need to do their jobs while preventing them from accessing information that does not apply to them.

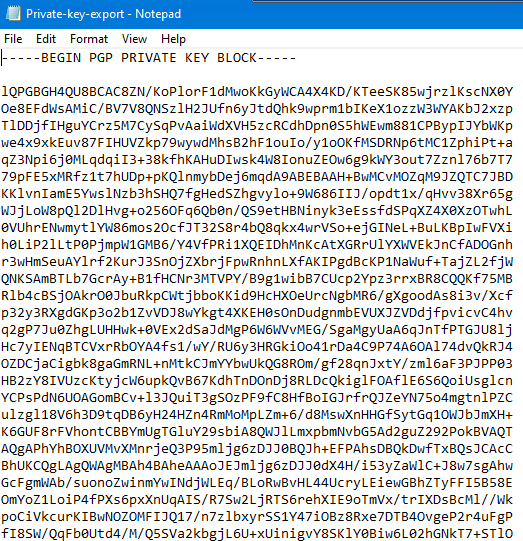
CHAPTER 3 : LAB EXPERIENCE REPORT

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.

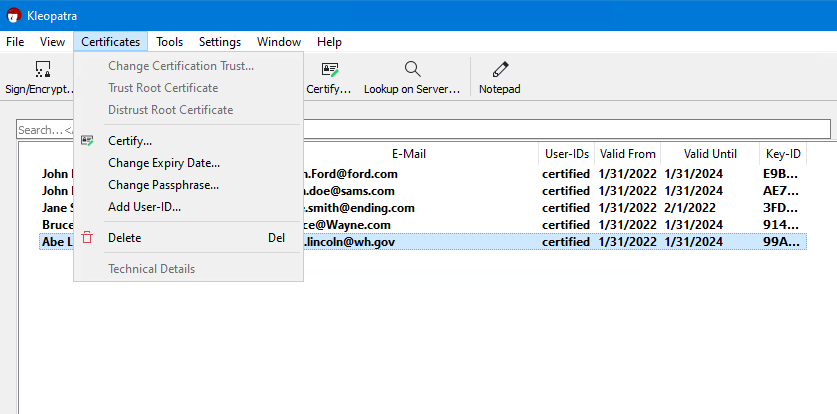


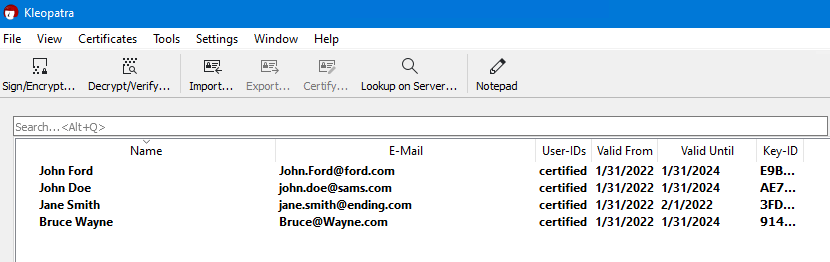


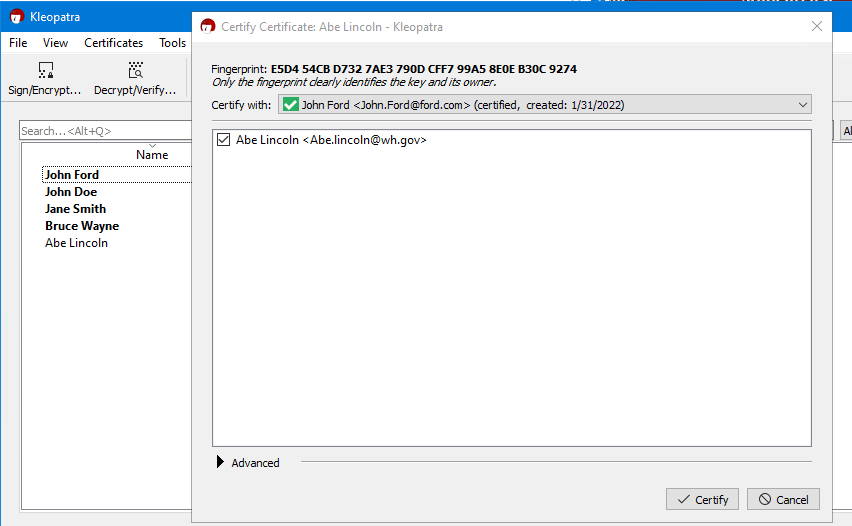






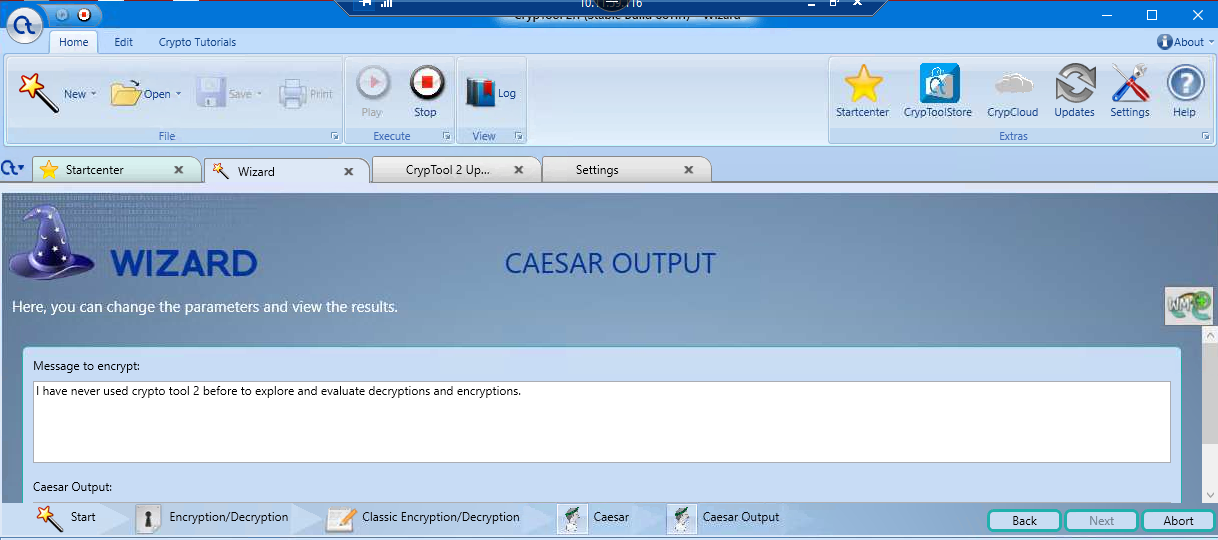


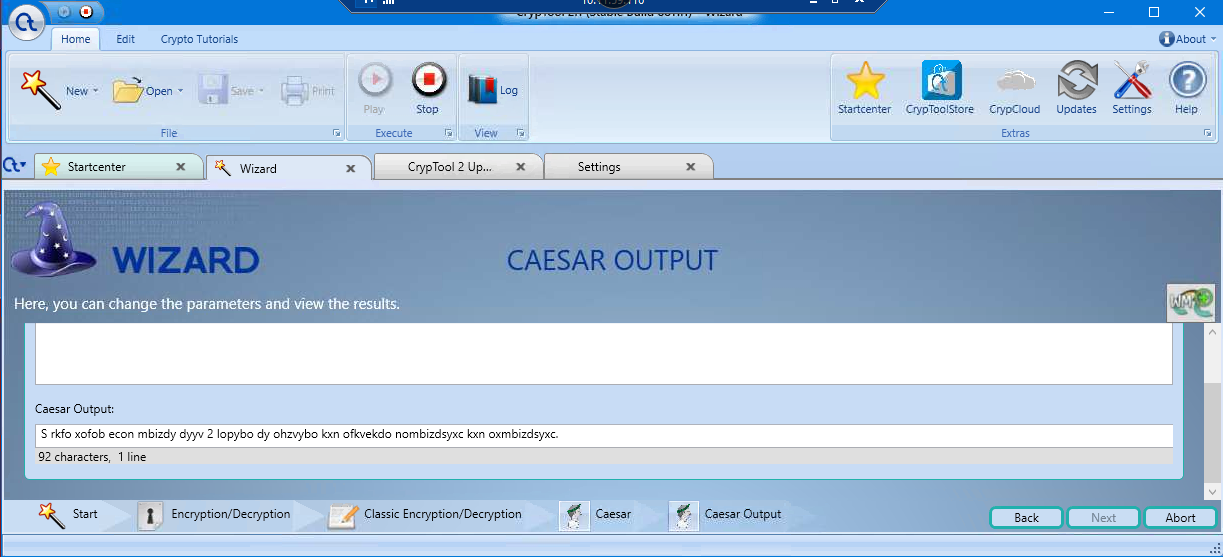


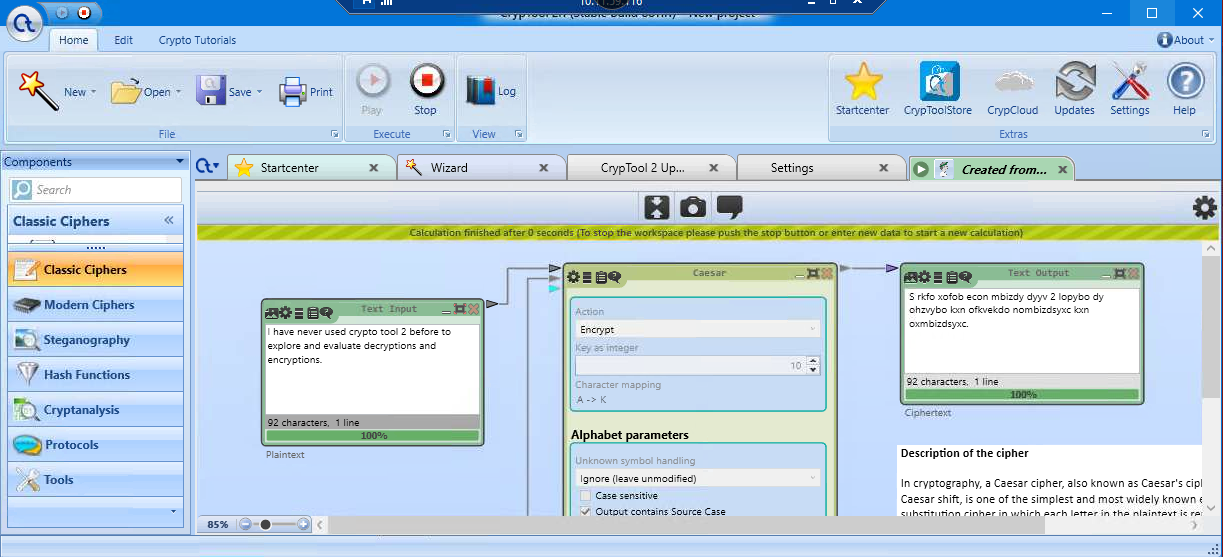


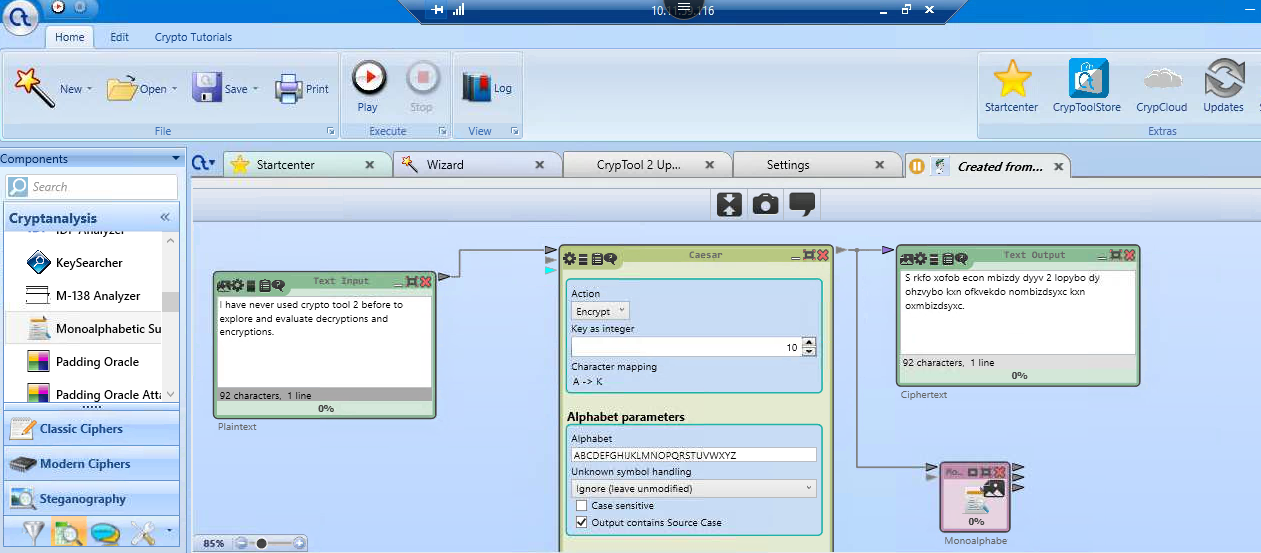
Expiry date for certificate are important since they demonstrate the validity of the keys and certificates. Whenever wrong passcodes are used access to the message becomes limited. It is essential to regularly change passphrase to ensure high level of security for the stored data or information. The 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.

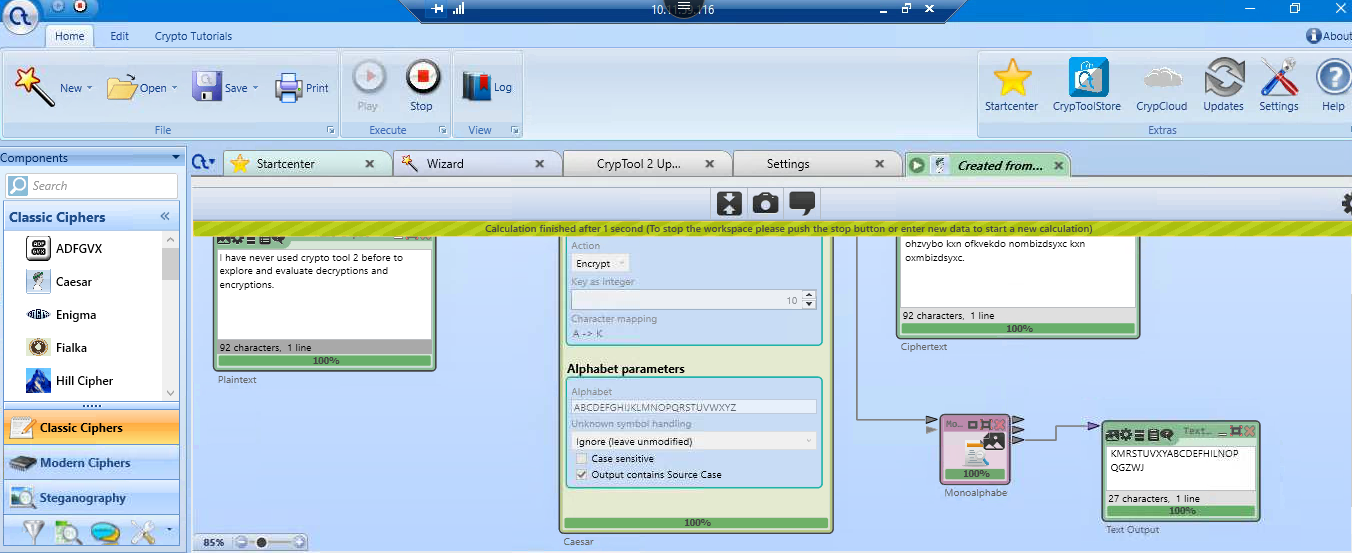
## ***Crypt Tool***

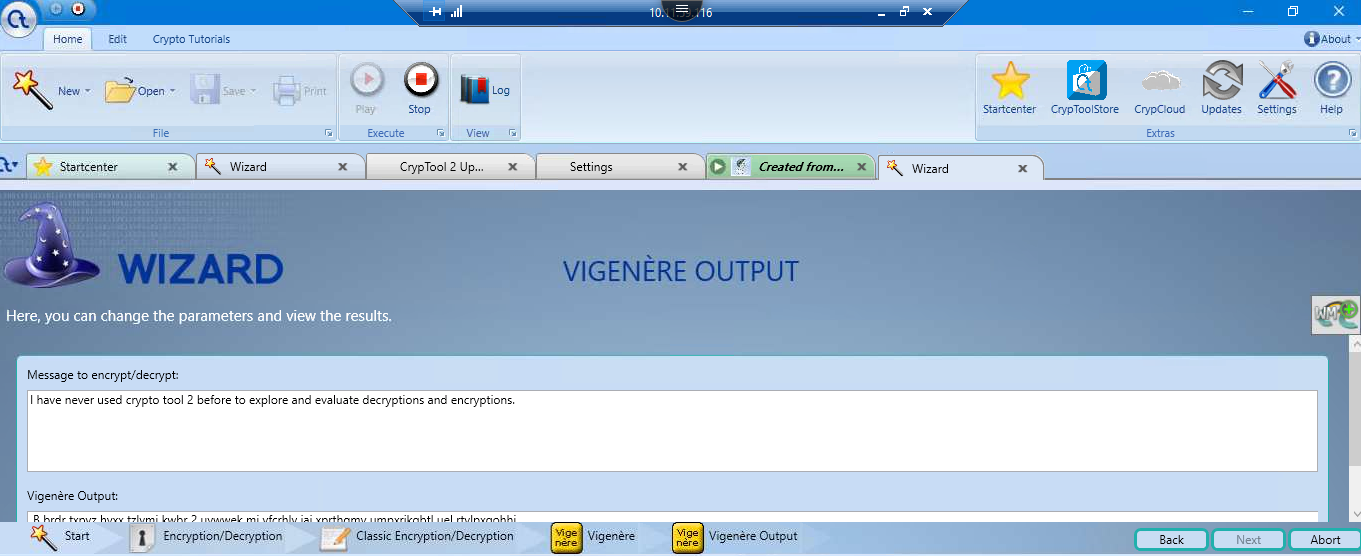


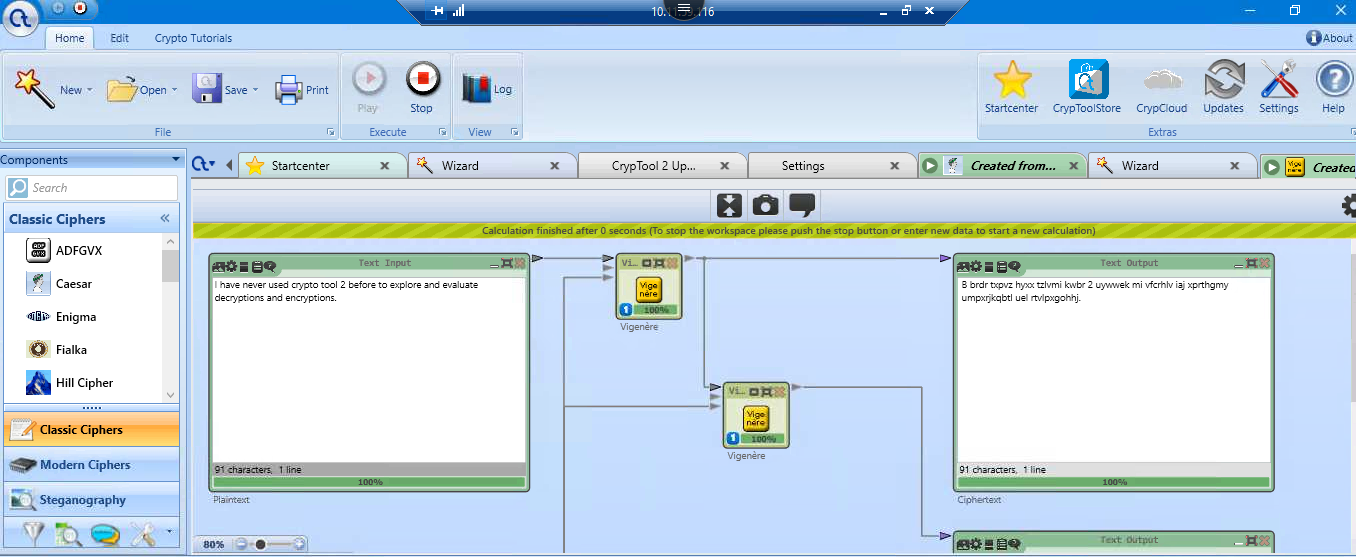


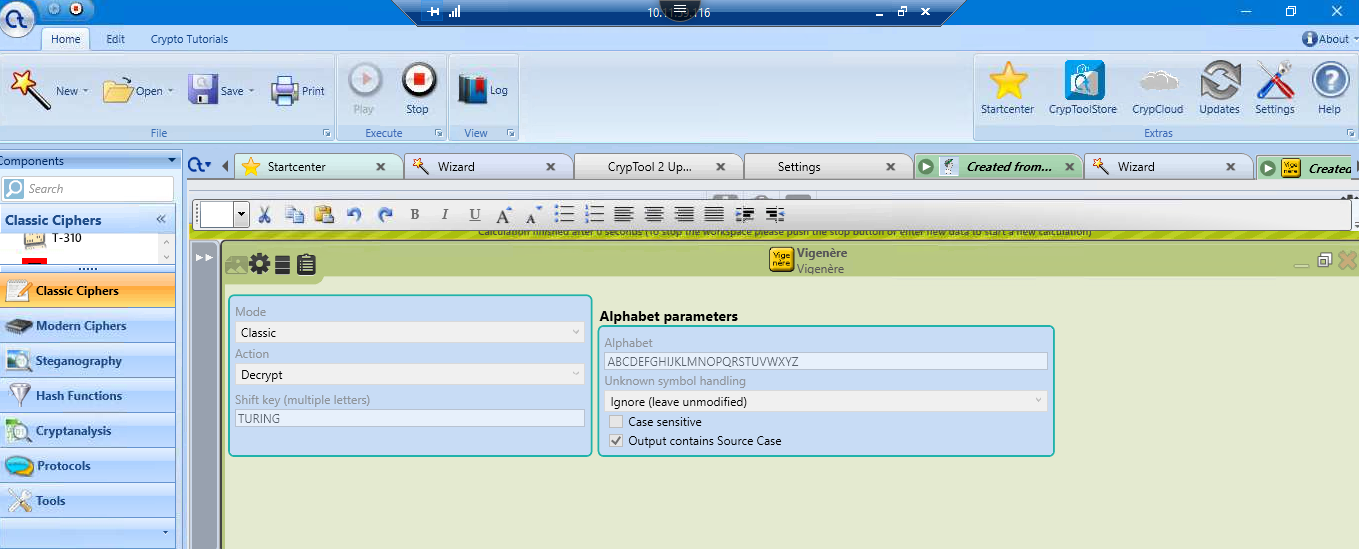


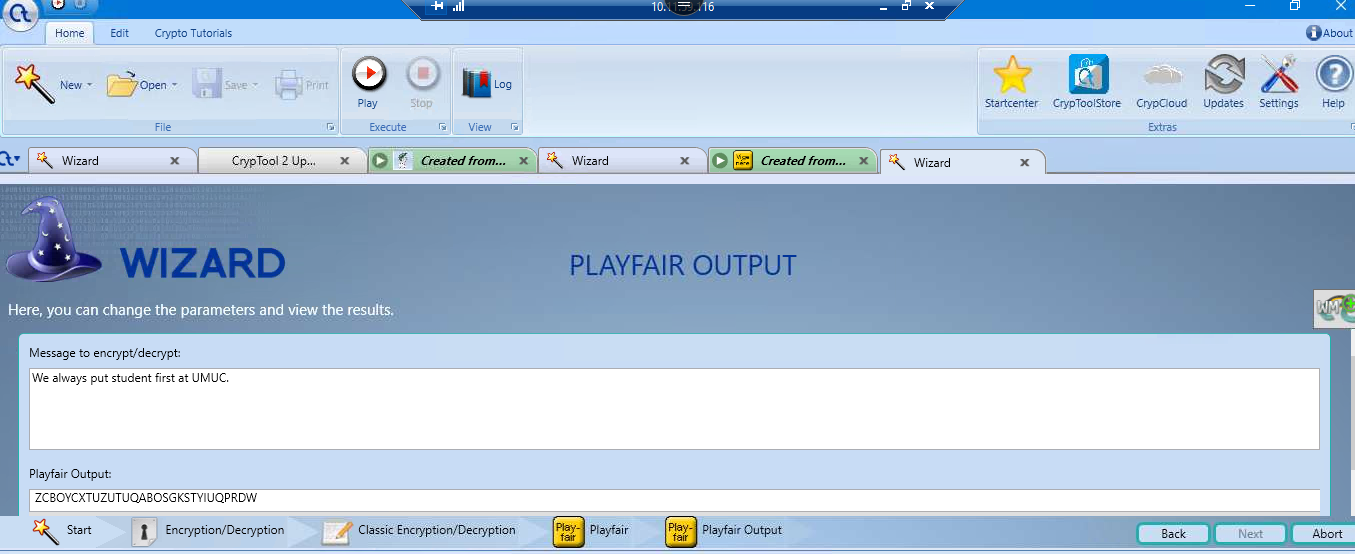


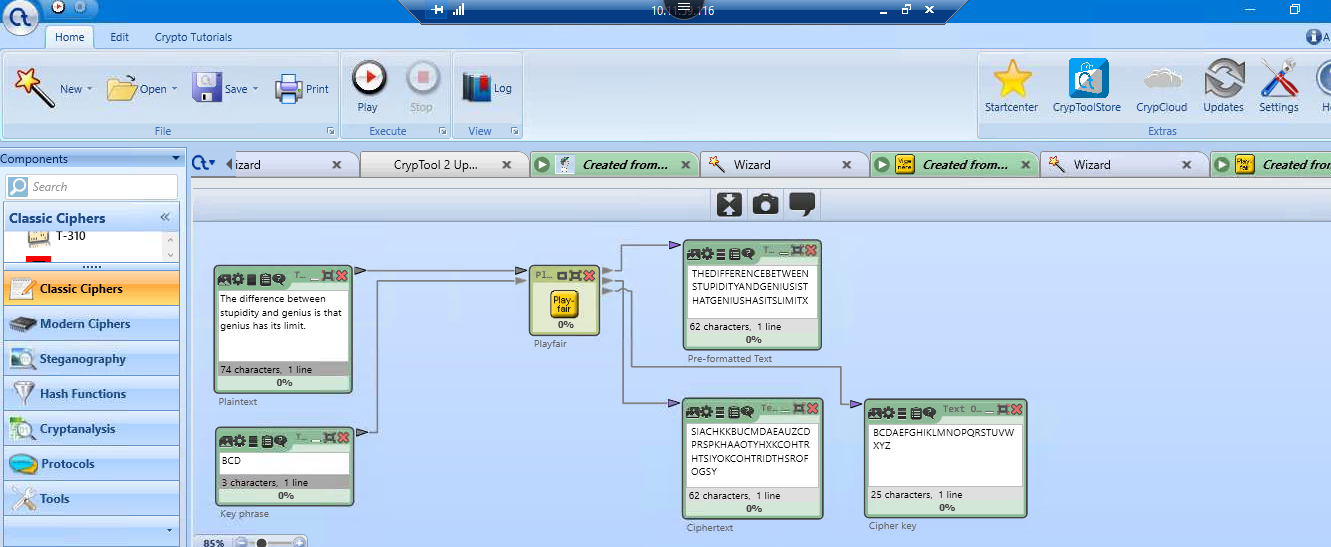






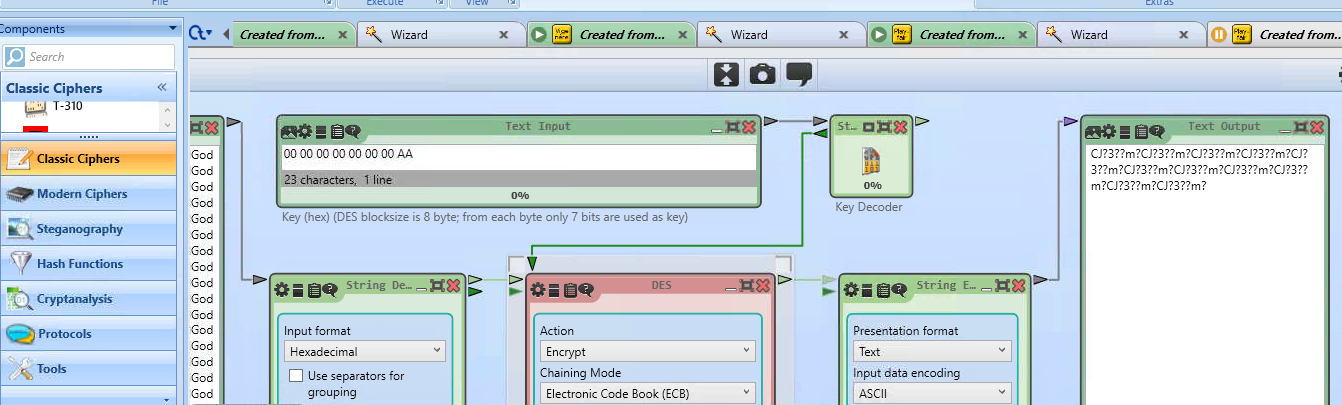


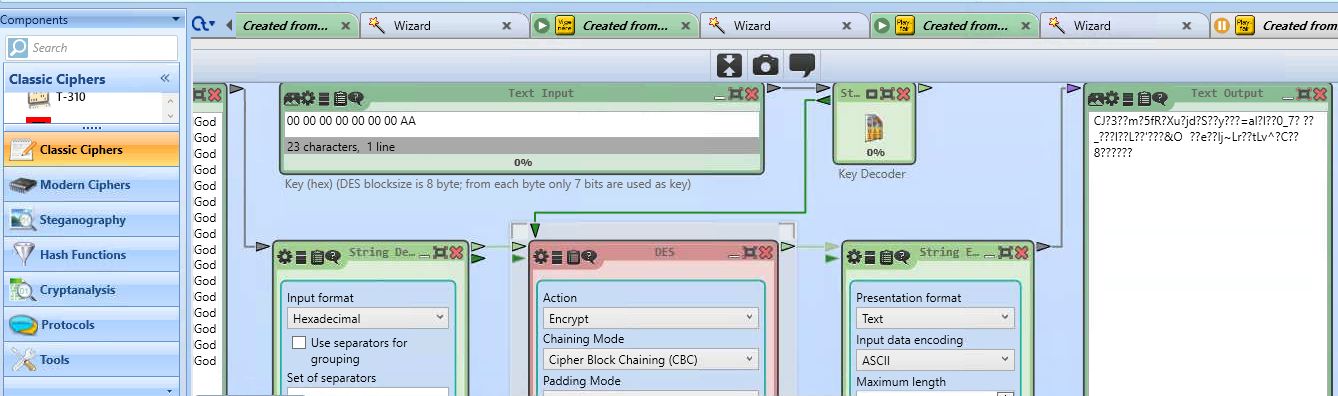
















**Conclusion**

As security breaches in the healthcare industry continue to rise, enterprise key management is necessary and mandatory for hospitals and businesses to protect their data and information. As a result, many organizations have shifted their security efforts to data encryption. The PKI application is the most important and versatile in the enterprise. This application necessitates meticulous planning before it can be implemented. Superior Healthcare (SHC) will focus on any critical decisions if they have a clear understanding of the used cases, requirements, and dependencies. Each decision is based on previous decisions as a history of what has happened and its effects on current and future events. The approach to Enterprise Key Management implementation must always be methodical.

# **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.