|  |  |
| --- | --- |
|  |  |

CS 305 Module Four Assignment Algorithm Ciphers  
Brandon Coulter  
Southern New Hampshire University

# CS 305 Module Four Assignment Algorithm Ciphers

**Consider security protection best practices to defend against various types of security attacks.**

Some of the many security protection best practices include, cryptographic certificates and signatures, public and private keypair generation, and hash functions that are utilized to create message digests and more. These various security practices help prevent attacks such as man-in-the-middle and data breaches. Take for example the cryptographic certificates; these are certificates that essentially ensure a TLS clients that their connection to a given server is secure thus their information is encrypted. This is validated by the server sending the certificate to the user which has been signed by a certificate authority. Once corroborated, a secure connection is established. (Manico et al., 2015) An algorithm typically utilized for data security is the AES or Advanced encryption standard. This cipher algorithm utilizes a symmetric block cipher meaning it can convert data into unintelligible information and subsequently utilize the same cipher to revert back to readable data. (*FIPS 197, Advanced Encryption Standard (AES) – CSRC*, 2001) Algorithms such as secure hash algorithm or SHA-256 use hash functions to create message digests. The power of the SHA-256 algorithm as defined by the National Institute of Standards and Technology in the publication titled, *Secure Hash Standard (SHS)*, “For a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.” (*Secure hash standard (SHS)*, 2015) These are utilized in tandem with digital signatures algorithms to ensure a valid signature is in use.

**Consider and identify all of the risks in your recommendation.**

The risks associated with the long term storage of archival data include the retrieval of said data during a data breach. Failure to use a cipher or even failure to implement proper cryptography in general could result in breach data whether that be sensitive to the company or to the customer. Regardless, the risk of sensitive data leaks is a real and significant risk that shouldn’t be taken lightly. Because of this, it is critical to implement a cipher algorithm that is not only appropriate but also secure and not vulnerable to known attacks. For instance, the above mentioned AES cipher algorithm would work well, especially the cipher algorithm AES-256 which utilizes a 256-bit key to encrypt the data to be stored. This effectively garbles the data such that an attacker could not gain any insightful use out of it.

**Consider the most current government regulations and how they will be met.**

Regulations wise, the U.S government has relatively low requirements for encryption, however they do require encryption to be decrypted if legally obligated for a criminal investigation by a provider if a provider encrypted the information. This is similar in multiple countries such as all countries in the European union. (*World map of encryption laws and policies*, N.D.) Although the U.S may require providers to assist authoritative figures in decryption, the U.S has no regulation that requires an individual to do such an act; this is unlike Canada, the United Kingdom, and various other countries around the world. Differences such as a general right to encryption vary from country to country as well. It is important to consider the regulations and what may or may not be breaking them with Artemis Financial encryption system. (*World map of encryption laws and policies*, N.D.)

**How will this algorithm cipher be used?**

Implementing the cipher of choice such as the AES-256 bit cipher algorithm would allow Artemis Financial to encrypt sensitive banking information related to the company itself as well as banking information for their clients, such as bank statements and personally identifiable information. Utilizing a 256 bit encryption/decryption key, Artemis Financial would be highly protected from data leaks from a data breach. The AES algorithm uses a large key specifically of 128, 192 or 256 bits to jumble the information the algorithm is given, thus encrypting the files with protected information in them.

**What is the best cipher and why?**

The best encryption for Artemis fool would be AES-256 bit cipher algorithm. Algorithms that are less than 128 bits are not secure enough for the sensitive nature of the data to be stored. Considering vulnerability exploits exist for encryption algorithms such as DES, it is important to choose a highly secure algorithm, of which AES-256 is one of them. The symmetric nature of this algorithm means the same algorithm and 256 bit key is utilized for encryption and decryption meaning it is easier on the computation of the trusted computers. Adopted and used by the U.S Government since 2001, the AES algorithm is proven and most definitely an appropriate choice to secure delicate banking information. (*NIST's encryption standard has minimum $250 billion economic benefit, according to New Study*, 2018)

**What are the reasons why you might not choose the most secure cipher?**

Choosing not to implement the most secure cipher could stem from weighing the pros and cons of the cipher. For example, an exceptionally secure cipher may look good on paper because it is virtually impossible to crack with the current computing power, however, those ciphers may take exponentially longer with regards to time to decrypt and thus encrypting and decrypting with these types of ciphers may lead to long encryption and decryption times. This in turn would not work for accessing data on a web application that is meant to be swift and easy to use. Additionally, choosing the proper cipher is dependent not only on the needs but the regulations that may be imposed from external entities, thus a more secure cipher may be off the table if regulations are not met.

**What is the purpose of the hash functions and bit levels of the cipher?**

Hash functions and hash algorithms such as the SHA-256 algorithm are vital for verification of data integrity. Using a hash function, this algorithm creates a message digest, essentially a compressed version of the original message. Due to the ability to ensure data integrity, this algorithm is highly sought after for validation of digital signatures. (*Secure hash standard (SHS)* 2015) A problem however with hash algorithms is the potential for collision which can weaken security and stability of the cipher.

**Explain the use of random numbers, symmetric vs non-symmetric keys, and so on.**

Although they are called random, computers can only generate “fake” or pseudorandom numbers based on a given seed or key. This means that knowing the key of a random number algorithm, could lead to the decryption of said algorithm. “To provide more randomness, seeds are often pulled from the system’s source of actual random data, and then the CPRNG is reseeded frequently as it runs. This supplies a reliable pool of pseudorandom data while minimizing the likelihood of blocking.” (Manico et al., 2015) A symmetric algorithm means that the encryption and decryption keys are the same; this differing from an asymmetric or non-symmetric key pair such as a public and private key which are different. In this methodology, a private key is kept secret as the name implies and used to confirm the data whereas a public key is utilized to authenticate the signature itself. (Manico et al., 2015) The combination of keys required to encrypt and decrypt data has a higher computational requirement than that of the symmetric system which is also something to consider while choosing a cipher.

**Describe the history and current state of encryption algorithms.**

Algorithms have come quite a long way from the early ciphers such as the Caesar cipher utilized by the Romans. In modern days, ciphers are calculated by computers allowing for far more secure data than a hand done cipher. Nevertheless, vulnerabilities still arise such as the cracking of the DES cipher which lead to stronger ciphers like 3DES and now the AES cipher which has excellent security with a 256-bit key. Ciphers that are strong such as the AES-256 bit cipher are nearly impossible to crack given current technology and computational power which is why the U.S government has adopted it. Again however, as time goes on cybercriminals find new and improved ways of cracking ciphers and thus the encryption algorithms of the future will only grow stronger.

**References**

Manico, J., Detlefsen, A., & Kenan, K. (2015). *Iron-clad Java*. O'Reilly Online Learning. Retrieved July 20, 2022, from <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch01.html#ch01lev2sec3>

National Institute of Standards and Technology. (2001, November 26). *FIPS 197, Advanced Encryption Standard (AES) - CSRC*. CRCS. Retrieved July 20, 2022, from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

National Institute of Standards and Technology. (2015, August 4). *Secure hash standard (SHS)*. CSRC. Retrieved July 20, 2022, from <https://csrc.nist.gov/publications/detail/fips/180/4/final>

*NIST's encryption standard has minimum $250 billion economic benefit, according to New Study*. NIST. (2018, December 11). Retrieved July 21, 2022, from https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

*World map of encryption laws and policies*. Global Partners Digital. (n.d.). Retrieved July 21, 2022, from https://www.gp-digital.org/world-map-of-encryption/