Tim Jayson

CS-305 Module 4 assignment

9/25/2025

1. **Algorithm Cipher**: Review the scenario and the Java Security Standard Algorithm Names resource, a standard list of algorithm ciphers provided by Oracle for recommending an appropriate encryption algorithm cipher. This resource is linked in the module’s Resources section. Specifically, recommend an appropriate encryption algorithm cipher to deploy, given Artemis Financial’s security vulnerabilities. Consider the following points in your decision-making process:
   1. What security protection best practices do you need to consider to defend against various types of security attacks?

There are a plethora of security practices to consider when attempting to defend against attacks. The first thing to consider is what information are you trying to protect, this will determine the minimum levels of security needed as well as any governmental regulations that need to be considered. It is also important to know how often the data will need to be accessed as well as who will need said access. There is a very real tradeoff when considering security vs accessibility and the needs of the company need to be considered. A few key things to consider are:

* Encryption key management: It needs to be determined how the encryptions keys are stored in the system, who has access to them, and if/how they are rotated
* Strength of encryption: What level of encryption would work in this situation based on company needs and government mandates.
* Unbroken encryption: It is important to choose an encryption that has not been broken or has known vulnerabilities.
* Recovery plan: There should be a recovery plan in place in case the encryption keys are lost/corrupted.
  1. What are the risks of your recommendation?

There are always risks with any security recommendation. A few examples are:

* Recommending too weak of an encryption: If the encryption cypher is too weak, it would be possible for malicious actors to break it and get access to sensitive data.
* Recommending too strong of an encryption: While it may seem counterintuitive, the stronger security gets, the harder it is to perform everyday business functions. The encryption needs to be secure enough to protect sensitive information but also allow all necessary access without too many delays.
* Incorrect analysis of company needs: There is the possibility of recommending the wrong level of security based on incomplete information or assumptions. It is vital to understand the exact business needs before recommending security such as encryption.
* Possibility of recommending a broken encryption: Encryption cyphers have been broken over the years and it is possible that more are broken without our knowledge. Malicious actors are working every day to test security so it is vital to stay up to date with secure encryptions and which have been broken.
  1. What government regulations do you need to consider? How will these regulations be met?

The governmental regulations depend on the country that is being operated in. Some examples of regulations are:

* NIST SP 800-53: This provides guidelines for proper implementation of cryptography in federal government systems.
* FIPS 140: This is a federal government standard for cryptographic implementation to protect sensitive information.
* IRS Publication 1075: This publication gives guidance on the protection of federal tax information that a company manages.
* EU-GDPR: A security framework in the European Union that was implemented to help protect sensitive personal information from compromise.
  1. How will this algorithm cipher be used?

If Artemis Financial went with the recommendation of adopting Advanced Encryption Standard (AES), it would function by converting data into an unreadable format unless the recipient had the proper key. AES uses various key lengths of 128, 192, or 256 bits that help to provide strong protection against unauthorized access.

* 1. What is the best cipher, and why?

The best cipher in terms of strength/usability that would be ideal for Artemis Financial would be Advanced Encryption Standard (AES). This is an extremely secure cipher that does not slow down the transactions speed, allowing the company to continue its operations uninterrupted. Since it is widely implemented it can be considered reliable and secure.

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

The latest or cutting edge ciphers that are generally “more secure” can also have serious drawbacks. Some of these concerns are:

* Overcomplexity: If a cipher is overly complex, it is easier to misconfigure steps which could result in a less secure system or the loss of data.
* Performance: Extremely complex algorithms can slow down the system which could negatively impact the business needs
* Regulation issues: It is important to ensure that the cipher used meets the requirements of governmental regulations and new top of the line ones may not have been approved.
* Reliability: New or cutting edge ciphers may not be as thoroughly tested as other options like AES and can result in unsecure or lost data.

1. **Justification**: You have been asked to give a brief overview of the encryption algorithm cipher to justify your recommendation to Artemis Financial. Consider the following points:
   1. Explain the purpose of the cipher's hash functions and bit levels.

Hash Functions: These are mathematical algorithms that convert input data into a fixed length out that is commonly known as a hash value. Hash functions add a level of integrity checking since any alteration to the data will result in a different hash value. This helps to ensure that the data has not been tampered with. Hash functions are also used in digital signatures and to securely store passwords making it difficult for attackers to access them even if they breach the system.

Bit Levels: The output of the hash function is determined by the specific bit level they operate at. Common levels that hash functions operate on are 256 and 512 bit hashes which help to provide security against brute force attacks. As the bit level increases in size, it makes the hash function more secure.

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

Random numbers: Random numbers are extremely important in securing data with encryption. It helps to ensure that the cipher is harder for malicious attackers to break.

Symmetric Keys: This is a version of encryption where data is both encrypted and decrypted with a single key. Both the sender and receiver have the same key. The sender uses the key to encrypt the data before transit and once it is received, the recipient uses the key to convert it back to plaintext.

Non-symmetric keys: This type of encryption uses 2 separate but related keys. One key is known as the public key and the other is known as a private key. The public key encrypts the data and the private key decrypts the data.

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

The current state of encryption algorithms sees ciphers such as Advanced Encryption Standard (AES) as secure and reliable options for companies to properly protect their data. In the near future, advances such as post-quantum cryptography could completely change the minimum requirements that a company needs to adopt to protect their data. Older ciphers such as DES are no longer used since many have been broken over time.

Sources:

Barker, E. (n.d.). *Guideline for Using Cryptographic Standards in the  Federal Government: Cryptographic Mechanisms*. NIST. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf>

Crane, C. (n.d.). *Symmetric vs asymmetric encryption: A guide for non-techies*. HackerNoon. https://hackernoon.com/symmetric-vs-asymmetric-encryption-a-guide-for-non-techies-p03c316t

GeeksforGeeks. (2025c, August 8). *Advanced encryption standard (AES)*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/advanced-encryption-standard-aes/

*General Data Protection Regulation*. General Data Protection Regulation (GDPR). (2024, April 22). https://gdpr-info.eu/

*Publication 1075 tax information security guidelines for federal, State*. IRS.GOV. (n.d.). https://www.irs.gov/pub/irs-pdf/p1075.pdf

Mehta, M. (2020, December 4). *Hash function in cryptography: How does it work?*. InfoSec Insights. https://sectigostore.com/blog/hash-function-in-cryptography-how-does-it-work/

Saini, H. (n.d.). *8 strongest data encryption algorithms in Cryptography | analytics steps*. AnalyticSteps. https://www.analyticssteps.com/blogs/8-strongest-data-encryption-algorithms-cryptography

Scott, A. P., & Tierno, P. (n.d.). *Banking, Data Privacy, and Cybersecurity Regulation | congress.gov | library of Congress*. Congress.Gov. https://www.congress.gov/crs-product/R47434

*Wolfcrypt FIPS 140-2 and FIPS 140-3: Licensing*. wolfSSL. (2025, August 1). https://www.wolfssl.com/license/fips/