|  |
| --- |
| Zorg Industries |
|  |

# Memorandum

To: Andrew Ryan

From: Hari Seldon

CC: Chad Ballay; Hunter Goncalves; Jordan Smelser; Diane Yablonski

Subject: Enterprise Direction on Hashing/Encryption Standards

Wanted to give you the initial status report and onboard you onto the executive steering committee for the Hashing/Encryption Initiative. This initiative will impact our technical side of the house with the implementation as well as the business side of the house with our compliance process changes. I look forward to your input and advocacy from the insights you garnered in your previous business operations role.

# Goals and Requirements

As part of our last cycle of audits we have found that our runway for additional waivers has been shortened such that business performance would be impacted. To remediate these short comings, we are forced to paydown technical debt on our legacy systems so that they can be modernized to implement the processes and controls we need for our next audit. Several key technologies are the long poles in the Gantt Chart. Once we updated these technologies, we will have better controls in place around ensuring Confidentiality, Integrity, and Availability. (Kim, 2018)

# Background

**Overview**

A screenshot of a cell phone

Description automatically generated

(Difference Between Encryption & Decryption, n.d.)

* Encryption is a two-way function where keys are used, Hashing is a one-way function where no keys are used.
* Encryption encodes text in a way that only authorized parties can access; Hashing uses hash functions on data to map it to a fixed size output.
* Encryption the encryption string is variable, hashing it’s fixed
* Encryption you can always decrypt using the decryption key, hashing can’t be reverted to the original massage.
* The purpose of encryption is to transmit data securely; the purpose of hashing is to verify data.

(The Real Difference Between Hashing and Encryption, n.d.)

**Encryption**

Encryption also uses an algorithm but to encode plaintext. It is a two-way process instead of a one-way process. It starts with plaintext and encrypt it to make ciphertext. The thing about encryption is anyone can decode it with the right key, but you must have the right key. Encryption can either be Symmetric or Asymmetric. Asymmetric encryption has two different keys. One key encrypts, called the public key, the other decrypts, called the private key. RSA, ECC and Diffie-Helman are most widely used. Symmetric encryption uses the same key to encrypt and decrypt, this is faster but not as secure.

**Hashing**

Hashing is one-way encryption method. This means it can’t use a predetermined key to decode the information when you hash data. The finalized data doesn’t give you the information to unencrypt it. There are numerous hashing algorithms and they are most effective when they are collision resistant. One way is to have a hash be complex enough to prevent multiple inputs to the same output. You also don’t want to make it so complex that it’s inefficient. Our company uses MD5 which gives a 128-bit value in the form of 32 hexadecimal digits, and SHA-3, which uses a permutation-based algorithm.

# Initial Recommendations

We are still actively researching and implementing several proofs of concepts to ensure no implementation shortcomings. So far, the GAP analyses are going well and we have some tentative selections made. We are using the existing NIST recommendations to ensure regulatory compliance and ease of future upgrade paths. (Guideline for Using Cryptographic Standards in the Federal Government, n.d.) *These are not ready for broader socialization outside of the project communications as they are only the initial draft solutions.*

|  |  |  |
| --- | --- | --- |
| Technology Area | Recommendation | Explanation |
| Mobile Encryption | AES-GCM-256 | SP 800-38D |
| Hashing Algorithm | SHA-3 | FIPS 202 |
|  |  |  |

**Comment**

The reason it is more important to utilize the security of encryption versus the verifying of data that hashing offers is because a mobile network is generally more exposed than even a computer network. Phones and other mobile devices generally travel more than a work computer and are almost always active during their circuit. Unless a mobile data is utilizing its data option, it will search for the nearest wi-fi to lock into, and public wi-fi networks are not secure. Thus, it is fundamental that any work-related information that is shared from a mobile device is done so securely to keep it out of the wrong hands, and this can be done with asymmetric encryption; especially a data link layer encryption.

Types of attacks that encryption can prevent is basically anything that keeps trying to use different passwords till it guesses. It would take years of constant trying to break one encrypted key. Brute-force, Dictionary attacks, and Denial of service attacks all are protected using encryption. Birthday attacks focus on hashed passwords, not encrypted passwords. Dictionary password attacks is another attack that won’t work with encryption. (Kim, 2018)

# Bibliography

*Difference Between Encryption & Decryption*. (n.d.). Retrieved from SSL2Buy - Global SSL Provider: https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption

*Guideline for Using Cryptographic Standards in the Federal Government*. (n.d.). Retrieved from NIST Special Publications: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf

Kim, D. a. (2018). *Fundamentals of Information Systems Security.* Burlington: Jones & Bartlett.

*The Real Difference Between Hashing and Encryption*. (n.d.). Retrieved from Solarwinds MSP: https://www.solarwindsmsp.com/blog/hashing-vs-encryption%C2%A0