CHAPTER 1
INTRODUCTION

1.1 Background

Defense science is one of the many types of science that are currently being developed in the scientific world. Defense science, like many other sciences, employs multidisciplinary, interdisciplinary, and transdisciplinary scientific principles. This principle inspires the study of national resilience in the field of defense science (Virgiawan, 2018).

National resilience is founded on Pancasila, The 1945 Constitution, and The Archipelago Concept. On this basis, national resilience implies the following characteristics: independence, dynamic, unity, authority, and cooperation. In addition to these characteristics, national resilience is founded on welfare and security, inward and outward, kinship, and integral comprehensiveness. National resilience has eight gatra or Astagatra aspects, including: geography, demography, natural resources, ideology, politics, economy, social - culture, and defense – security (Safarudin, 2022).

Defense - security has different definitions and are carried out by different agencies. However, in order to achieve national resilience, defense and security must be integrated. Many scientists have voiced their thoughts on defense theory. Some well-known defensive theories are Absolute Defense Theory, Total Defense Theory, Integrated Defense Theory, Cooperative Defense Theory, and Self Defense Theory. The debate over defense theory gave rise to national defense (Dwi Sulisworo et al, 2012).

National defense is carried out by the main component, in this instance The Indonesian National Military (TNI). In addition to the main component, there are reserve components and support components charged with bolstering the ranks of the main component. National defense has strategic goals that must be realized, such as maintaining the sovereignty and territorial integrity of the Republic of Indonesia and protecting the safety of the entire nation from all forms of threats, constructing an integrated and

modern Universal People's Defense and Security System (Sishankamrata), realizing National Resource Management (PSDN) for National Defense, and implementing defense area management (Ministry of Defense, 2020).

In order to establish an integrated and contemporary Sishankamrata, cyber defense is required to counter cyber attack that interfere with national defense. Cyber defense is implemented in stages, which are as follows: attack prevention, information security monitoring, attack analysis, defense, counterattack, and information security enhancement. The goal of cyber defense is to protect Critical Information Infrastructure (IIV). In national defense, IIV is an electronic system that must be secured. Government administration, Energy and Mineral Resources (ESDM), transportation, finance, health, Information and Communication Technology (TIK), food, defense, and other areas selected by the President are among the IIV protected sectors. Cyber teams implement IIV protection at the national, sectoral, and organizational levels (Permenhan RI No 82 Tahun 2014).

National Cyber and Crypto Agency (BSSN) summarized various occurrences that posed a danger to IIV security in Indonesia, including 399 cases of cyber threat intelligence, 27.956 cases of darknet exposure, and 245 cases of data breach. That recapitulation resulted in projections of the sorts of cyber dangers that may emerge in the next year. Ransomware, data leaking, Advanced Persistent Threat (APT), phishing, cryptojacking, Distributed Denial of Service (DDoS), Remote Desktop Protocol (RDP), social engineering, and site defacement are among the forecasts. To minimize the incidence of these cyber threats, a national cyber security policy and cyber crisis management are necessary. One of the major aspects on the national cyber security plan is national cryptographic independence (BSSN, 2022).

Cryptography is a mathematical area that examines the topic of information security with the goals of confidentiality, integrity, authentication, and non-repudiation. In addition to cryptography, the word cryptanalysis refers to the study of code breaking in cryptography. Both are

related to cryptology. There are various words in the cryptosystem that enchiper and dechiper actors are aware with, including: plain message, cipher message, encrypt, decrypt, key, sender, receiver, and interceptor (Menezes et al, 1997).

Cryptography is not a new field of study. According to the history of cryptography, this method has been used since the Ancient Egyptian Age using hieroglyphs, Ancient Greek and Roman using scytale, historical records of the Arabs in the Arabic Origins of Cryptology book, kama sutra records in Ancient India, Renaissance Age in Europe, breaking the code of Queen Elizabeth I's assassination in England, until the German Government's use of the enigma machine during World War II. Cryptography is evolving at a rapid pace in the modern day (Munir, 2023).

In today's modern era, cryptography is growing very fast. This is evidenced by the total of cryptographic algorithms used. Some examples of cryptography algorithms in today's modern era: DES, 3DES, Diffie-Hellman, AES, Blowfish, IDEA, LOKI, FEAL, Lucifer, CAST, CRAB, SAFER, Twofish, Serpent, MARS, Camellia, 3 WAY, MMB, SkipJack, RC4, A5, SEAL, ECC, Cellular Automaton, RSA and so on. Each of these cryptography algorithms has its own advantages and disadvantages, so the selection of these algorithms should be relevant according to our needs.

Modern cryptography is not only limited to coding to keep messages secret. Modern cryptography also creates new sub-sciences. Some of these sub-sciences that are developing today, namely: steganography, One Time Pad (OTP), stream cipher, block cipher, public key, Elliptic Curve Cryptography (ECC), digital signature, hash function, Secure Socket Layer (SSL), digital watermarking and others. Many of these cryptography sub-sciences are applied in the ICT field. Nemati and Yang (2011) explain some examples of cryptography applications including in the fields of: networking, cyber space, email, web services, wireless communication, electronic e-commerce, emerging areas and others. In addition, Bruen and Forcinito (2005) also added their ideas about cryptography applications in the field of

e-government. Even in everyday life, without realizing it cryptography applications are all around us such as when using smart cards, transactions through ATM machines, cable TV payments, communication via cellular phones and others.

The implementation of cryptography in securing message delivery often causes a movement that can be detected by the interceptor. For this reason, a new technique is needed that can disguise the delivery of the message. The message masking technique is called steganography. Steganography is one of the techniques used in the scientific family of cryptology. Steganography utilizes a cover object to disguise the secret message so as to produce a stego object. Steganography applications not only use images as media, but can also be sound, text, files, binary or communication channels (Munir, 2023).

A grayscale image that is 1 pixel in size is equivalent to 1 byte. While 1 pixel of a Red Green Blue (RGB) colored image is equivalent to 3 bytes. Steganography takes advantage of the weakness of the visual senses to distinguish colors that are not significantly different. Radescu and Gliga (2004) recommend that a cover image should be a grayscale image because the change in value in a grayscale image during the encoding process is not too significant. Aditya Sahu and Monalisa Sahu (2020) provide several examples of steganography applications in disguising messages including in the fields of networking, streaming media, meteor burst communication, Audio Video (AV) synchronization, password protection, printer stego, healthcare stego, military communication, fingerprinting, digital imaging, media database and so on.

When it comes to data management, every user of Information, Communication and Technology (ICT) must be cautious. Over time, the amount of data used and managed will increase. This complicates the storage capacity available for data storage. Furthermore, the volume of data sent and received can have an impact on digital communication systems. As a result, the term "data compression techniques" is frequently used to

refer to a technique useful in the management and communication of digital information. Data compression techniques are processes that allow you to reduce the size of data without losing important information, which can save storage space, speed up data transfer, and improve the efficiency with which network resources are utilized. Various data compression techniques, including lossless and lossy compression methods, have been developed over the last few decades. Despite the numerous compression methods available, selecting the best method for a specific type of data and application remains a significant challenge.

In the context of this study, data compression methods are critical. When data is encrypted or secret messages are inserted into it, the data size increases, which can impede data transfer or raise suspicion. As a result, there is a need for in-depth research into how to integrate data compression methods with cryptography and steganography to achieve the best possible balance of security, privacy, and efficient use of storage space or bandwidth. This study will look into the development of data compression methods that can reduce the size of secret messages in order to overcome challenges in secure and efficient data observation in an increasingly complex digital era.

The use of technology has made it much easier for humans in electronic transactions. However, these electronic transactions are not always used in a positive way because there are also certain individuals who use them for crime. One crime that often occurs is the theft of personal data. To take action against the perpetrators of these cyber crimes, the government issued regulations regarding the protection of personal data. It is hoped that this regulation can increase the security of information from each individual or group. Every agency, both government and private, must have confidential information about their institutions. The government has classified information or documents in the government into 4 categories, namely top secret, secret, limited and ordinary. The categorization of classified documents gives permission to anyone who can access them.

Apart from this categorization, each agency must also carry out physical, administrative and logical protection.

Data Encryption Standard (DES) is a method in cryptography that uses an encryption algorithm through stages: Initial Permutation (IP), Enciphering and Inverse Initial Permutation (IP^{-1}). While the decryption algorithm is the inverse of the encryption algorithm. This cryptography method is included in algorithms that use symmetric keys and block ciphers. Briefly, this algorithm goes through a process that uses several types of tables, namely: ASCII, Initial Permutation (IP), Permuted Choice - (PC - 1), Wrapping, Permuted Choice - 2 (PC - 2), Expansion, Substitution Box (S - Box), Permutation Box (P - Box) and Inverse Initial Permutation (IP^{-1}). There are slight differences in DES encryption and decryption algorithms, namely in the wrapping stage, key sequence and input key for iteration. DES cryptography has evolved into Triple Data Encryption Standard (3DES).

The 3DES encryption method is not much different from its predecessor. The 3DES algorithm performs 3 times the encryption process using 2 key versions, namely the 3key version K_1, K_2, K_3 or the 2key version K_1, K_2, K_1. In the decryption algorithm, it is also not too significantly different because it uses a 3-time process that resembles encryption with a choice of 2 key versions. Until now, 3DES is still one of the options for securing information in several large institutions. The 3DES method is one that is still quite effective in keeping messages secret and efficient in memory usage. In the time it takes to check all possible keys every 50 billion per second, 3DES has a longer time of about 800 days compared to DES which only takes 400 days (Alanazi et al, 2010). This means that 3DES is more effective in securing keys than DES. In addition, Daniel Commey et al (2020) have also compared cryptography methods in the encryption breaking process with the results of the longest execution time. The study found that with the same memory size of about 5MB, the longest encryption breakdown time starts from 3DES, AES and Blowfish. This shows that 3DES is more efficient than AES and Blowfish.

Least Significant Bit (LSB) is a steganography method that utilizes changes in the last bit of a binary character. The reason why it has to use the last bit is because a binary character has a sharp change when changing its Most Significat Bit (MSB), or in other words changing the leading part of the binary character. Whereas if you change the last bit, it minimizes the sharp changes. Currently, LSB has been developed to examine how much message capacity can be accommodated, how much the size changes after encoding, how fast the algorithm is to decipher the stego object and others.

A ZIP compression is a compression format used to combine and compress files or folders in a single archive. It is crucial in securing and managing sensitive data, especially in the context of classified documents. ZIP compression reduce file size and provide additional security by using compression algorithms like Deflate. This allows for efficient storage of classified documents via email or limited storage. The ZIP compression also supports data encryption, making it ideal for protecting sensitive data. By applying a password to the ZIP archive, the data remains secure. Thus, ZIP files are a valuable tool for storing, transmitting, and securing classified documents (Zhang, 2005).

Several researchers have conducted experiments related to 3DES cryptography. Shawkat et al (2022) compares 3DES and 3kRSA encryption algorithms on eyeOS, highlighting 3kRSA's efficiency despite higher computation time and output bytes. Future work aims for physics-based encryption methods. Gupta et al (2019) presents paper that OTDES algorithm is used to securely store and retrieve documents in the cloud, reducing security risks in hybrid cloud systems by removing repeated documents and encrypting them. Christy Atika et al (2018) study on 3DES cryptography demonstrated its effectiveness in encrypting plain images, with an average time of 176,0633 seconds for 64 x 64 images. Research by Devi and Chamundeeswari (2018) compares DES, AES, and Anonymization 3DES (A3DES) cryptographic algorithms for securing big data in healthcare, finding A3DES superior. Agnihotri et al (2020) developed

a combined cryptography method, combining AES and 3DES encryption, providing double protection against brute force attacks on document archives. Rubik's Cube is used to reconfigure the 3DES Algorithm key, enhancing its security, speed, and resistance against brute force attacks (Saadi, 2022). The new method, which increases throughput and speed of encryption and decryption, outperforms the traditional method, resulting in lower battery consumption. The study proposes a modified DES algorithm, employing three keys for encryption, block size, and state tables, to improve its defense against attack and brute-force assaults, despite increasing the complexity of calculating keys (Alsuwaiedi and Rahma, 2023). This paper by Vuppala (2020) proposes a novel FORTIS algorithm to enhance the Key Schedule Algorithm, resulting in a secure Triple Data Encryption Standard. The algorithm uses a Comparator and versatile shifter to reduce PGE values and improve efficiency. The TDES methodology by Ramachandra (2022) is a proposed approach for secure big data storage in the cloud environment, particularly in healthcare applications. It involves data selection and encryption using 112 bits and 168 bits key strength. The methodology simplifies the process by increasing key sizes, protecting against attacks and data privacy. However, it requires higher network and CPU usage. Nurdin et al (2022) study successfully implemented 3DES cryptography for SMS messaging, demonstrating its effectiveness in sending and receiving encrypted messages on Android-based smartphones.

In addition to previous research on 3DES cryptography, the following will explain previous research using LSB steganography. Kumar and Swain's (2019) research improves Reversible Data Hiding (RDH) by implementing modified LSB matching and n-Rightmost Bit Replacement (n-RBR) and Modified Pixel Value Differencing, enhancing Embedding Capacity (EC) in LSB. LSB image steganography improves payload capacity by using dilated hybrid edge detection. This technique maintains stego image imperceptibility and indirectly increases secret message

payload capacity, according to Rosal's (2019) research, comparing results from previous studies. Rustad et al (2020) utilized an adaptive pattern of inverted LSB in digital image steganography to enhance imperceptibility, resulting in decreased Mean Square of Error and increased Peak Signal to Noise Ratio. Yanting Wang et al (2020) proposed a high-capacity adaptive steganography based on LSB and hamming code, addressing issues with decoding and detecting size differences or file damage. Their experiment assessed perceptual quality, mean square error, and peak to signal to noise ratio, enhancing secret message disguise. Mandal et al (2021) conducted research on high-capacity LSB steganography using n-LSB and eight-way Cover Value Difference (CVD). They tested embedding capacity, visual quality, security, and comparative analysis with state-of-the-art methods. The experiment produced a better Absolute Edge Change rate globally. The LSB approach by Faheem (2023) is utilized in image watermarking for security, enhancing the efficiency of the process by detecting suitable watermark locations at the pixel level. The Hufman Code LSB-based image steganography technique, tested against various attacks, effectively resists noise and trimming attacks (Rahman, 2023). It uses Hufman code, HSI color model, MLEA, Magic matrix, and LSB substitution to embed secret messages in cover images. Hacimurtazaoglu and Tutuncu (2022) presents a LSB-based pre-embedding video steganography using a rotating and shifting poly-pattern block matrix, aiming to balance robustness, imperceptibility, and payload while reducing computational time and addressing statistical attacks. The paper that propose by Lu et al (2021) is a modified LSB matching method using dual-image and likelihood recording strategy, enhancing image quality and effectiveness against steganalysis attacks. It is suitable for simple secret images and requires adaptability for future use. The proposed algorithm uses Knight's Tour Algorithm for image encryption and steganography, generating a lossless pattern embedded into a cover and shuffled to obtain a stego object, ensuring high data security and confidentiality (Shashikiran, 2021).

Based on a brief explanation and previous research that has been done, the researcher took the initiative to develop research entitled “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents”.

1.2 Problem Identification

Based on the above background, the problem identification that will be solved in the research can be determined as follows:

a. Triple Data Encryption Standard (3DES) - Cryptography design alone is not optimal in disguising existence of classified documents.
b. Least Significant Bit (LSB) - Steganography design alone is not optimal in protecting confidentiality of classified documents.
c. Transformation of all file types in classified documents into Zipped Information Package (ZIP) extension can facilitate cryptography, steganography and data compression techniques.

1.3 Research Scope and Limitations

This research is limited to several research scopes. This restriction is done so that the research does not deviate from the problem formulation that will be made. The following are the limitations of this research:

a. This research uses:
    1) Software. Windows 11 64-bit software, Python and VLC Media Player.
    2) Hardware. Lenovo 82H8 Laptop with 11th Gen Intel® Core™ i5-1135G7 @2,40GHz processor specifications and Memory of RAM 20,48GB.
b. This research is carried out through 3 stages of the method for program encryption and otherwise, namely: ZIP - Compression Method, Triple Data Encryption Standard (3DES) -

Cryptography, and Least Significant Bit (LSB) – Steganography.

c. Object of Triple Data Encryption Standard (3DES) Cryptography using .pdf file types and limited to data available at Ku Poltekad Kupus II Ditkuad. On other hand, Least Significant Bit (LSB) Steganography using image and video files.

1.4 Problem Formulation

Problem formulations that can be compiled based on the problem identification above are as follows:

a. What is the encryption program of “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents”?

b. What is the decryption program of “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents”?

c. What are the results of statistical analysis in the program “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents”?

1.5 Research Objectives

Purpose of this research is to be a solution to the problem formulation which includes:

a. Can present the encryption program “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped

Information Package (ZIP) Extended Classified Documents".

b. Can present the decryption program "Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents".

c. Can perform statistical analysis on the program "Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents".

1.6 Research Benefits

It's expected that research can provide the following benefits:

a. Theoretical Benefits
   1) Can protect the security and disguise the existence of classified documents with an optimal size.
   2) As a reference for other researchers to develop other research in the field of cryptology.

b. Practical Benefits
   1) For Unit Ku Poltekad Kupus II Ditkuad. Can increase security in sending classified documents.
   2) For Cyber Defense Engineering Study Program of the Republic of Indonesia Defense University. Can be a reference in learning in the Military Cryptography Technology (MCT) course.
   3) For Researchers. As a prerequisite for fulfilling obligations in graduation in the Cyber Defense Engineering Study Program of the Republic of Indonesia Defense University.