

Original Article

Multiple Digital Signature Integration in the University Data Backup Archive using Enhanced DLP-based Security Framework

Aris J. Ordonez

IT Department, Bicol University College of Science, Legazpi City, Philippines.

Corresponding Author : ajordonez@bicol-u.edu.ph

Received: 27 February 2026

Revised: 17 August 2026

Accepted: 21 August 2026

Published: 30 September 2026

Abstract - The dependency of universities on information systems has emphasized the need for a secure archival mechanism for institutional data. This study covers the implementation of a repository for database backup of Bicol University using a multiple digital signatory framework using Enhanced Discrete Logarithm Problem (DLP). The method consolidates five security managers of Bicol University, each maintaining their own digital signatures. The backup activity covers hashing of the database files using SHA-512 and encrypts the result using an Enhanced DLP-based Cryptosystem to generate a consolidated digital signature. The verification process requires the participation of, but is not limited to, five (5) security managers to ensure integrity, authenticity, and non-repudiation of the backup file and the stored security stamp. The evaluation conducted showed consistent and validated generation of digital signatures and security stamps, reliable detection of file tampering, and integration of collaborative authorization of security managers, which establishes distributed accountability and operational trust. Further analysis of the algorithm showed no established patterns between the plaintext and ciphertext, manifesting a high level of security. The sensitivity test using the Avalanche Effect exposed no patterns between the ciphertext and the plaintext and key, manifesting encryption strength. This was further validated by the use of the Strict Avalanche Criterion (SAC), which also showed a higher level of security. However, complexity analysis disclosed that higher computing resources are necessary to effectively implement the system. Nonetheless, the study confirmed that the enhanced DLP-based multiple digital signature framework is cryptographically secured and provides a practical and scalable approach for securing institutional data.

Keywords - Cryptography, Cybersecurity, Digital signature, SHA-512, Enhanced DLP, Multi-party authorization.

1. Introduction

Universities nowadays are relying heavily on centralized information systems to provide stakeholder services, academic activities, administrative support, and financial monitoring and operations. These systems normally generate mission-critical information that is significant for operational efficiency, accountability, policy compliance, and archiving. At Bicol University, the central database system served as the core repository of student records, personnel information, process documentation, transaction support, report generation, and research documentation. As part of its governance policy, a regular backup of the school's database is stored in the university's digital archive. Normally, backup procedures are required for availability and disaster recovery; however, these backups do not guarantee authenticity, integrity, and non-repudiation all the time. Consequently, unauthorized alterations, insider threats, or unintentional corruption may remain undetected until the data are verified during needed restoration or regular auditing.

Typical security frameworks such as access control, standing encryption, and transport layer data protection can provide confidentiality to standard operations; however, this offers limited assurance against tampering on stored data. Stored backup files may still be altered by users with privileged access, some malware, or compromised administrators without leaving tracks of alterations. This may be addressed by security stamps, by allowing verifiers to mathematically check the integrity of the backup file. This implementation, however, relies on single signing control, compromising trust, and there is a potential single point of failure. In organizations where accountability is important, a unilateral control provision does not reflect governance policies that require collaborative security and auditability.

In Bicol University, information systems support most of its major institutional transactions. This includes the admission system, enrolment system, registration system, student information management system, faculty and employee records system, financial transactions system,



procurement transaction system, service monitoring and response system, employees' financial claims management system, human resource management system, research and extension outputs system, budget management system, property management system, and other information systems relevant to university operations. The data generated and processed by these systems also form part of the information that the university server platform manages, maintains, holds, and protects.

As part of its mandate, the ICT Office is responsible for regularly conducting database backup activities to safeguard against system failures, data corruption, and other incidents that may result in data loss. These backup procedures ensure the availability and recoverability of critical data, thereby supporting business continuity and minimizing the risk of permanent data loss.

However, these database backups, particularly those generated in the form of database dumps or text-based backup files, are inherently vulnerable to unauthorized access, alteration, and possible compromise. These files are considered high-risk because they are complete, highly portable, often weakly protected, and represent an exact copy of the live database. Any person who gains access to the backup file may be able to open, edit, delete, insert, or modify records before restoration if there is a need for one. Once exported outside the Database Management System, these backup files no longer benefit from the system's built-in security controls, such as role-based access control, audit trails, transaction logging, input validation, and real-time monitoring.

In view of these risks, there is a need to implement a well-established security protocol that goes beyond conventional protection against hacking and unauthorized access. A reliable verification scheme should be integrated into the database backup process to ensure the authenticity, integrity, and non-repudiation of backup files. This protection mechanism must not be unilaterally controlled by a single authority to ensure checks and balances. With the existing established encryption algorithms that rely heavily on parallel or sequential encryption to allow multiple keys to secure the process, a modification is necessary to allow the integration of multiple private keys that are simultaneously injected into the process to secure important information. This will help guarantee that the backup data remains complete, unaltered, verifiable, and trustworthy with multiple levels of security before it is used for system recovery or restoration.

To address this identified gap, this study proposed a Digital Signature Scheme in the University Data Archive using an Enhanced Discrete Logarithm Problem (DLP)-based Security Framework. The method distributes control among, but is not limited, five designated security managers: the ICT Director, Data Privacy and Protection Officer, University IT

Officer, Network Administrator, and System Administrator (additional actors may be introduced). Each personnel possess a private key serving as a digital signature, forming a collaborative cryptographic control rather than a unilateral security administration, expanding the security level to another layer. Before the process of archiving, the generated database backup is hashed using SHA-512 to produce a fixed-length message digest representing the exact state of the file. The generated message digest is then encrypted using the enhanced DLP-based security algorithm, with the combined participation of all five security managers. The resulting encrypted hash now serves as the digital signature and is stored alongside the original generated backup file.

The verification process requires the participation of all the identified security managers, implementing a multiple authentication protocol. To verify the authenticity of the database backup, the file is re-hashed, and the stored digital signature then undergoes decryption using the five private keys to recover the original hash value. The matching decrypted signature and the message digest of the original file confirm the integrity, authenticity, and non-repudiation of the process, whereas any discrepancy indicates compromised files. By enforcing collective verification, the system eliminates the monopoly of validation and shows strengthened institutional accountability.

To ensure the reliability of the integrated cryptographic algorithm before its implementation, and to further analyse its level of security, this study also tested its accuracy using manually pre-computed test data; its level of security was tested by using Avalanche Effect's sensitivity test, utilizing Confusion and Diffusion Test and with reference to Strict Avalanche Criterion (SAC) for a higher level of security quality. The performance of the algorithm is further analysed through the standard Time and Space Complexity Analysis, which is focused on analysing its performance on required iterations (Time Complexity) and resource requirements (Space Complexity).

Overall, this research aimed to design, evaluate, and integrate a security framework that utilizes a distributed digital signature using enhanced DLP-based cryptography with multiple signatories in the system. The study runs parallel to a governance security model where cryptographic frameworks reflect organizational responsibility, transforming the backup process from passive preservation into verifiable, tamper-evident secured backup.

2. Review of Related Works

The transformation to digitalization of educational institutions has transformed universities into data-driven environments where centralized automated transactions manage academic, financial, and administrative records. Consequently, information has become a critical digital asset

requiring strong integrity and authenticity assurance. Some conventional protection mechanisms, such as password-controlled policies and encryption-based methods, normally prevent unauthorized access but do not ensure verifiable proof that backup files remain unaltered over time. Schneier emphasized that security frameworks must ensure not only confidentiality but also integrity and accountability to establish trust in digital processes [1]. Similarly, Stallings stated that data backups require cryptographic verification frameworks because storage redundancy alone cannot detect silent corruption or malicious modification [2]. In relation to this, several cryptographic hash algorithms were considered by this study as possible solutions to the need to secure university information.

Computer Science theory and concepts consider cryptographic hash algorithms as one of the bases for integrity verification methods. An example of this is the SHA-512 hash function. The algorithm is a part of the SHA-2 family, which was standardized by NIST. The algorithm generates a fixed-length hash code that uniquely represents the file's content and structure [3]. Due to its avalanche behavior and collision resistance feature, even a single-bit change in the original file produces a completely different hash value (avalanche effect). In the research conducted by Wang and Yu, the process showed that strong hash functions are significant for digital forensics and file authentication because they allow reliable detection of even minimal digital data tampering [4]. However, hash functions alone cannot identify who authorized or verified a file, thus necessitating the use of digital signatures as an expansion to serve this purpose.

By extending Digital signatures through hashing, identity is bound to data verification. This was manifested in the works of Rivest, Shamir, and Adleman, who introduced public-key cryptography that enabled authentication through asymmetric key pairs [5]. On the other hand, ElGamal implemented a signature and encryption scheme based on the Discrete Logarithm Problem (DLP) [6]. These methods successfully ensured authenticity, integrity, and non-repudiation in the process, which became widely adopted in secure communications and electronic governance systems of established organizations [7]. Menezes et al. have also emphasized a similar concept that transforms a hash value into a legally attributable proof of authorship using a digital signature [8]. These concepts gave light on the possibility of utilizing several methods to introduce a more appropriate and better fit to the needs identified in this study.

Despite their effectiveness, most typical digital signature frameworks operate under the control of a single signatory, which requires only one private key to authorize the security stamp and verification. In most organizations, the responsibility for data protection is distributed among multiple security officials. A single-signatory framework in this situation introduces risk. A compromised credential may

falsely validate an altered file without checks and balances. A collaborative authorization using multiple handshake cryptography may solve this problem. In the research work of Desmedt and Frankel, they introduced shared cryptographic control requiring multiple participants to generate a valid signature [9]. Shamir's secret sharing scheme also demonstrated that cryptographic trust can be distributed across several entities [10]. These, however, were done in a parallel or sequential manner. Signatures are tendered separately, all at the same time or in a series. Synchronous signing using a collaborative framework has not yet been introduced.

In the case of the Digital Signature Threshold Signature Scheme (TSS), which also uses multi-signature, the process involves reconstruction of a shared secret. The method creates exposure during reconstruction and increases complexity. To overcome this, Bellare and Neven proposed a multi-signature construction avoiding key reconstruction of the TSS but requires multiple independent signatures attached to the same message [11]. While the method is secure, this approach increases storage consumption and verification processing cost, making it inefficient for large archival repositories such as university database backups. Furthermore, most frameworks rely on sequential or parallel signing rather than simultaneous collaborative authorization.

Studies conducted about database security showed that database archives remain vulnerable even when encrypted. Behl and Behl, in their study, reported that backup files are typically targeted because they contain complete datasets in a single container [12]. Studies conducted on some developed higher-education information systems applications revealed that insider threats are typically the source of major risk due to their privileged administrative access and vested trust [13]. This is why this study considered multi-party approval mechanisms to provide stronger governance control than administrator-centric models.

To further explore this concept, similar published studies that used encryption as a method of protecting database backups of server platforms were reviewed. One of these is the study of Aydin, which demonstrated the use of Transparent Data Encryption (TDE) and AES-256-based backup encryption to protect MS SQL Server backups from unauthorized restoration [14]. Although the method successfully prevented unauthorized access to the backup files using encryption, the process consumed higher CPU usage and disk activity during restoration. This is because the method encrypts the whole backup file and requires decryption before its restoration. Another drawback is that only a single key was used during the encryption process, which does not expand the access control to multiple authorities. The need to have a security procedure that does not alter the database dump through encryption could be a better option, and this could be further enhanced by involving more actors in the security procedure for an expanded security

level. The study leaves opportunities for further research on dump-file integrity, intrusion detection, key compromise, and secure recovery procedures.

Another study examined the advantages and disadvantages of encrypting database backups as a method of securing information. In the study of Boicea et. al., another process layer was added to the method before conducting the backup operation. The content of the database was encrypted first before export in the form of a database dump [15]. The method improved the security protection of the database, but increased the required processes significantly during the actual use of the database file. The database file was protected while it was in the form of a database dump; however, decryption is required when it is restored and needs to be accessed by the application, and encryption is necessary before the dump operation. Another drawback to this process is that multiple authorities cannot manage the operations due to the limitations brought by the encryption algorithms used.

With due consideration to these solutions, where trade-offs were observed in attaining security, the need to have a backup process that does not require encryption of backup dumps for protection or the need to encrypt the data first before backup operations, must be considered. This is not to mention that these existing technologies only allow a single authority to manage the encryption key that is required for database restoration.

To find a way to fill this research gap, several algorithms were explored in this activity. The Discrete Logarithm Problem (DLP) remains one of the most trusted mathematical foundations in cryptography due to its computational complexity and is considered a Hard Problem in mathematics [16]. ElGamal Cryptosystem, on the other hand, is a DLP-based algorithm and a known Digital Signature variant and a widely used protocol because of its mathematical reversibility feature and public verifiability [6]. However, this classical DLP-based protocol supports only a one-sender-one-receiver framework. Some research in collaborative authentication has explored adapting DLP-based cryptography into multiple signatory handshake workflows, but most of the common implementations rely on separate signature integration (Sequential/Parallel) rather than unified cryptographic protection [17].

Some of the latest and state-of-the-art secure archival systems highlight a verifiable storage framework as part of their security mechanism. This method was tested in Ateniese et al., which introduced provable data repository techniques that ensured stored files remain intact and verifiable even without retrieving full contents [18]. Similar works by Juels and Kaliski also proposed proofs of retrievability for long-term archival verification for data storage systems [19]. Although effective for cloud storage, these methods do not incorporate institutional accountability through identifiable

signatories. Digital signatures are a critical component of auditability in organizational governance. The need to preserve digital objects in a way that their persistence is guaranteed by persistent verification metadata, as well as the stored object, was identified by Kahn and Wilensky [20], and similarly, ISO's information security standards advocate for accountability and multi-custodian participation in protecting data [21], which multi-signature validation supports by limiting unilateral authorization.

A published study about Federated Digital Systems claimed that an authentication process that involves multiple authorities can provide a basis for assessing the trustworthiness of digital identities. In this study, Gomi [22] proposed an authentication model where assertions disseminated using multiple authorities are joined to evaluate user identity. This supports the use of multi-actor verification as a means of strengthening assurance in online transactions, particularly where responsibility for authentication is distributed among several trusted entities.

Although the existing literature provides examples of applications of multi-signature and threshold cryptosystems, there is still a need for a unified cryptographic transformation that uses multiple keys to create a single signature that is verifiable by all parties involved in a transaction, without having to reveal each party's secret, without having to generate additional signatures, and without requiring the use of sequential signing processes. In addition, current methods have the disadvantage of imposing additional computational burdens, necessitating the reconstruction of individual secrets, and/or do not directly support repository archival.

Thus, in consideration of the identified gap above, there exists a need for a cryptographic mechanism that is capable of combining multiple private keys into a single verification process for institutional backup repositories. The method would allow the development of a digital signature system with multiple signatories that could be the security foundation of database backups as a verifier for the integrity of the database dump without the need to directly protect the file through encryption.

3. Methodology

Design-and-development and descriptive research methodology were used for the development, deployment, and evaluation of a secure university data repository archive based upon a multi-party digital signature mechanism using the Enhanced Discrete Logarithm Problem (DLP) cryptographic algorithm. Part of this methodology was to assess the mathematical hardness of the Enhanced DLP-based algorithm, previously determined in other studies, to evaluate its potential as an operational institutional security control for protecting backups of critical data, and to implement it in a fully working system in production. This research was carried out within the

framework of the Interconnected BU Systems (iBU), the central university information system that generates a full database backup of all institutional records twice each day and stores the backup at the end of each month. As such, the backup file constitutes the official recovery image of all institutional records, and thus has to be adequately protected, accountable, and traceable. The security process was designed to require distributed responsibility among five designated security officers who would be responsible for securing and validating the archived data; specifically, the ICT Director, the Data Privacy and Protection Officer, the University IT Officer, the Network Administrator, and the System Administrator. Each officer had access to an independent private cryptographic key, and the system required a collaborative trust model in which no single officer would have authority to individually secure or verify archived data.

The repository system followed a three-layered operational structure consisting of the data layer, security processing layer, and verification layer. In the data layer, the centralized database server created a full backup of all institutional records and transmitted the full backup to the repository server. In the security processing layer, the full backup underwent hashing and digital signing operations to ensure that the data would be authentic and secure. In the verification layer, all security officers were required to participate in verifying the authenticity of the full backup file before any authentication confirmation of the file could take place.

Before being placed into archival storage, the backup file was first processed using the SHA-512 [3] cryptographic hashing algorithm to create a fixed-length message digest that represented the exact binary footprint of the file. This message digest was referred to as the reference integrity value. The resulting message digest was then encrypted using the Enhanced DLP-based algorithm that integrated the private keys of the five designated security officers. The Enhanced DLP-based algorithm produced a consolidated encrypted output through multiple simultaneous cryptographic handshakes, producing a unified digital signature that represented the institutional security seal confirming the authenticity, integrity, and non-repudiation of the backup file. The repository stored both the original backup file and the generated digital signature.

To verify the security of the backup file, all five security officers were required to participate, thereby enforcing institutional accountability. When verifying the security of the backup file, the repository server performed the following steps: first, the repository server hashed the archived file using SHA-512 to produce a new message digest. Second, the repository server decrypted the stored digital signature using the private keys of the five security officers through the enhanced DLP multi-party decryption process. Third, the repository server compared the newly generated hash to the

original hash recovered from the stored digital signature. If the two hashes matched, the repository server confirmed that the file was valid and had not been altered. However, if the two hashes did not match, the repository server confirmed that the file had been compromised or tampered with.

The prototype system was developed using Python-based cryptographic modules for implementing enhanced DLP operations and secure hashing functions, and included a web-based administrative interface that enabled controlled authorization participation. The repository was installed in a secure institutional network and required that all designated officers authenticate their participation during verification procedures.

The evaluation of the system focused on the effectiveness of the system's implementation and the strength of its cryptographic security. The system was evaluated on several factors, including: the successful generation of digital signatures immediately after the creation of a backup file, the ability to enforce mandatory multi-party participation during verification procedures, the correct identification of altered and unaltered files, and the ability to prevent a single user from validating the file. Simulations were conducted to test whether the system could detect when a stored backup file had been intentionally modified to assess the reliability of the verification mechanisms.

The workflow consisted of creating the monthly database backup, hashing the backup using SHA-512, encrypting the hash using the Enhanced DLP multi-party keys, storing the file and signature in the repository, requiring five-party authorization for verification, re-computing the hash and decrypting the signature, and comparing both values to determine whether the file was valid and intact.

Further testing covers the test of the algorithm's accuracy using actual test data, which were manually computed to ensure correct results. The same input data were fed to the system to compare the output with the manually computed result to determine its accuracy level. Performance analyses were also conducted using Time and Space Complexity Analysis [23] to look into the algorithm's time requirement in terms of required iterations, and space requirements in terms of needed resources.

To test the level of security, Pearson Correlation [24] and Avalanche Effect using the Confusion and Diffusion Test [25] were conducted. The Pearson Correlation test tests the independence of the output in relation to the input to disregard the possibility of the existence of patterns. Avalanche effect was also conducted for the same purpose as part of a sensitivity test up to the bit level of the input and output data. Security Analysis using Strict Avalanche Criterion (SAC) [26] was also commissioned in order to elevate the evaluation to a higher standard.

The Strict Avalanche Criterion was applied to both the Confusion Test and Diffusion Test as part of the Sensitivity Tests. Through these methodologies, a collaborative cryptographic custody model was established that relied on institutional data archives being collectively validated rather than relying on a single administrator, which provided increased trust, accountability, and security for the preservation of critical university records.

3.1. System Architecture Diagram Description

The proposed university data repository framework is implemented using a three-layer protocol that integrates secure backup storage with a multi-signatory verification scheme using the Enhanced DLP multiple-handshake algorithm. The first layer, the Data Layer, consists of the process involving the database server that generates the regular database backup file and transmits it to the repository server (Figure 1).

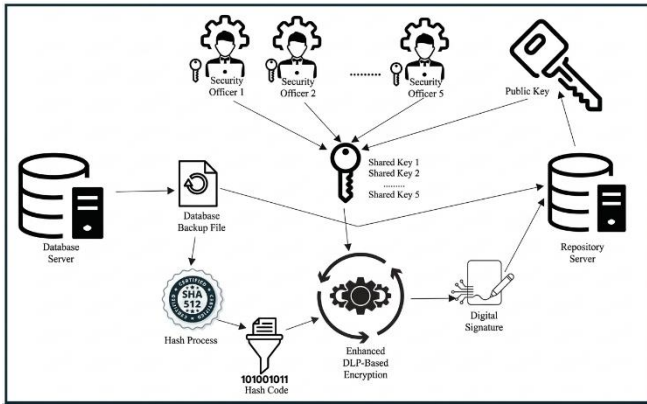


Fig. 1 Database archiving process with digital signature integration

The next layer, the Security Processing Layer, is responsible for all cryptographic operations involving the enhanced DLP-based Framework: the backup file is hashed using the SHA-512 hashing process, producing a unique message digest (hash code), which is then encrypted via the enhanced DLP-based protocol incorporating the private keys of the five designated security officers. The consolidated output forms a single digital signature (Security Stamp) that is stored alongside the original backup file in the storage (Figure 1).

The last layer, the Verification Layer, manages the integrity validation process. Verification requires the participation of all five security officers to decrypt the Security Stamp, recompute the file's SHA-512 hash from the original backup file, and compare it against the decrypted Security Stamp. This layered framework utilizes a distributed accountability method ensuring that no single officer can independently authorize or validate backup files to provide integrity, authenticity, and non-repudiation of institutional data in the backup system (Figure 2).

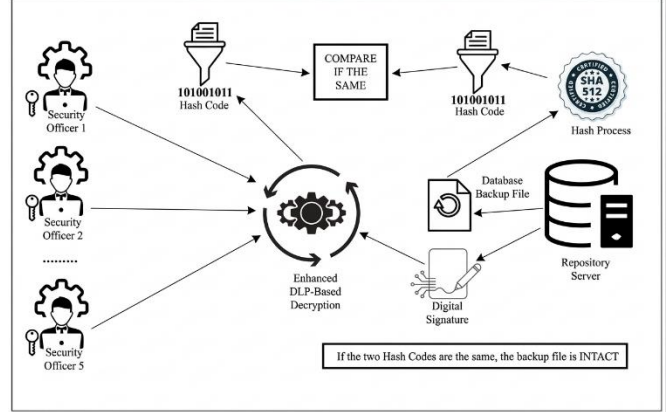


Fig. 2 Database file backup verification process

3.2. Enhanced DLP-based Algorithm Workflow

The Enhanced Discrete Logarithm Problem (Enhanced-DLP)-based algorithm serves as the controlling mechanism for integrating the different digital signatures into the university database backup archive. Instead of treating the digital signature as a simple cryptographic protective process, the system implements it as a controlled multi-authority security procedure. The algorithm covers three major processes—key generation, multiple signatory encryption, and collective decryption/verification process—ensuring that integrity, authenticity, and non-repudiation are achieved through coordinated participation of all designated security officers. During the key-generation phase (Figure 3), each of the five security managers independently generates a private–public key pair derived from common DLP parameters (P, g), where P is a large prime and g is a primitive root modulo p . The private keys S (Figure 4) remain exclusively kept in the possession of their respective officers, while the public keys are registered within the system's verification service. All keys are mathematically related to the same DLP domain but remain independent from each other and are stored separately. This creates a distributed trust environment in which no single entity can dominate the signing process on its own without others knowing it. The collection of public keys ($P, g, K_{\{1,2,3,4,5\}}$) forms the verification structure, while the private keys collectively become the approval authority of the archive (Figure 4).

Key Generation Phase

1. Prime Number P is set by the server (Preferably very large Prime Number)
2. Generator g is selected from the Cyclic Group
 $Cyclic\ Group = \{0 \leq g \leq P\}$
3. Shared Key b is generated from the Server's Private Key a (a remains confidential, only b is shared) using the formula $b = g^a \mod P$
4. The Public Keys $\{g, P, b\}$ are shared to the Signatories
5. The Private Key a by the Receiver is not disclosed and kept private in the possession of the receiver

Fig. 3 Enhanced DLP-based key generation algorithm

Encryption Phase

1. The different signatories create their own individual Private Keys which will serve as their digital signatures
 $\{S_1, S_2, S_3, S_4, S_5\}$ (can be expanded to more than 5 signatories)
 Shared keys $\{K_1, K_2, K_3, K_4, K_5\}$ are then generated from the Private Keys (signatures) of the signatories using the formula
 $K_{(1,2,3,4,5)} = g^{S_{(1,2,3,4,5)}} \bmod P$
2. Plaintext Message m is then encrypted using the formula:

$$C = \frac{m \cdot b^{S_2} \cdot b^{S_4}}{b^{S_1} \cdot b^{S_3} \cdot b^{S_5}} \bmod P$$

3. The generated ciphertext is shared with the target recipient together with its decryption key
 $C = \text{Ciphertext}$
 $K_{(1,2,3,4,5)} = \text{Shared Key for Decryption}$

Note: The algorithm is not limited to five (5) signatories only. It can be expanded to more than five following the pattern indicated in the formula.

Fig. 4 Enhanced DLP encryption algorithm (Signing phase)

Decryption Phase

1. The Decryption phase processes the Ciphertext C using the Shared Decryption Key $K_{(1,2,3,4,5)}$ using the formula below:
- $$m = \frac{K_1^a \cdot K_3^a \cdot K_5^a}{K_2^a \cdot K_4^a} \bmod P$$
2. The Plaintext m is derived by decrypting the Ciphertext C using the shared Keys $K_{(1,2,3,4,5)}$ and the Receiver's Private Key a .

Note: The algorithm is not limited to five (5) signatories only. It can be expanded to more than five following the pattern indicated in the formula.

Fig. 5 Enhanced DLP decryption algorithm (Verification stage)

During the signing stage (Figure 1), the database backup file is processed using SHA-512 hashing to produce a fixed-length message digest (Hash Code).

The Enhanced-DLP algorithm then collaboratively applies a multi-private-key encryption procedure simultaneously to this digest.

All the security managers transform the hash using their consolidated private keys to produce a cryptographic signature, which will serve as the Security Stamp of the backup file.

This process binds their consolidated identity through the cryptographic system to each other and to the encrypted hash code that eventually becomes the Backup File's Security Stamp. The resulting value constitutes the final digital signature (Security Stamp), representing a consolidated cryptographic approval derived from all private keys rather than a single signer. The signature is stored together with the backup file in the file repository system. The original data remains unencrypted for efficient storage and retrieval.

Digital Signature Creation Code
 # m is the hash code created by SHA512
 # P is the Prime Modulo, b is the shared key
 # S is an array of the signatures
 # Key generation Phase is outside this function
 # Python Code

```
def CreateDigitalSignature(m,P,b,S):
    Ciphertext = [] #digital signature string
    x = len(m) #length of hash code
    y = len(S) #number of security managers assigned
    for i in range(0,x):
        cipher21 = m[i]
        cipher22 = 1
        cipher21Counter = 1
        while cipher21Counter < y:
            cipher21 = cipher21*b**S[cipher21Counter]
            cipher21Counter += 1
        tempCiph = (cipher21*modinv(cipher22,P)) % P
        Ciphertext.append(tempCiph)
    return Ciphertext
```

Fig. 6 Digital signature creation algorithm

Digital Signature Verification Code
 # K is the Shared Decryption Key
 # Cipher is the Encrypted Hash (Digital Signature)
 # a is the private key of the server
 # P is the Prime Modulo
 # Python Code

```
def DecryptDigitalSignature(Key, Cipher, a, P):
    hash512 = []
    x = len(Cipher) #length of the ciphertext
    y = len(Key) #number of Security Managers
    for i in range(0,x):
        newMsg1 = Cipher[i]
        newMsg1Count = 0
        while newMsg1Count < y:
            newMsg1 = (newMsg1*K[newMsg1Count]**a) % P
            newMsg1Count += 1
        newMsg2 = 1
        newMsg2Count = 1
        while newMsg2Count < y:
            newMsg2 = (newMsg2*Key[newMsg2Count]**a) % P
            newMsg2Count += 1
        hash512.append((newMsg1*modinv(newMsg2,P)) % P)
    return hash512
```

Fig. 7 Digital signature verification algorithm

The Verification Process is conducted (Figure 2) through a method that involves the designated Security Managers and collectively executes the decryption process using the Enhanced DLP-based Protocol. When a backup file is accessed for validation, the system initially extracts the SHA-512 hash of the stored backup file. The saved Security Stamp is then decrypted using the corresponding private keys of the five Security Managers. The Enhanced-DLP verification equation (Figure 4) requires the successful contribution of each registered public-private key combination; failure of any component results in verification rejection. Once the Security Stamp is validated, the recovered digest (Decrypted Security Stamp) is compared to the extracted hash of the Backup File. Matching values confirm that the backup file remains

unchanged and that all authorized Security Managers participated in the verification process. A resulting mismatch indicates compromise or incomplete authorization. Through these stages, the Enhanced-DLP algorithm functions not only as a cryptographic method but also as a central security verification mechanism. The Key Generation Phase distributes authority among authorized security managers, while multiple private-key encryption enforces collaborative signing, and collective decryption establishes accountable conformed verification. This digital verification framework, therefore, becomes a mathematically provable record of institutional authority over the archived database backup file.

3.3. Enhanced DLP-based Algorithm Complexity Analysis

The Enhanced DLP-Based Algorithm utilizes three essential functions that are significant for the effective execution of the algorithm. These are the Extended Euclidean algorithm, the Modular Inverse Algorithm, and the Prime Number Test Algorithm [23]. Time Complexity analysis for the Encryption Algorithm indicates that it executes at most n^2 iterations, which is Quadratic (1).

$$f(n)=2n^2+8n+n \log n+8 \text{ or } O(n^2) \quad (1)$$

Space Complexity, on the other hand, showed that the computational formula of the algorithm with respect to the resources used is n^2

$$f(n) = n^2+3n+9 \text{ or } O(n^2) \quad (2)$$

which is also Quadratic (2).

The Decryption Algorithm's registered iterations (Time Complexity) can be represented by the function

$$f(n) = 4n^2+4n+n \log n+4 \text{ or } O(n^2) \quad (3)$$

Which is Quadratic (3), while its resource utilization (Space Complexity) is at n^2

$$f(n) = n^2 + 3n + 9 \text{ or } O(n^2) \quad (4)$$

Which is a Quadratic Complexity (4).

Generally, the Enhanced DLP-based Cryptographic Algorithm is based on complexity analysis, which is both quadratic in its Time and Space Utilization, thus requiring faster machines to effectively and efficiently utilize. Although ideally, quadratic complexity may not be the best for algorithms in terms of speed, this will not be the case for security algorithms. Security Algorithms do not have to be fast. They need to be accurate, reliable, and hard to break regardless of their performance speed. This study, however, also presented some major drawbacks of the algorithm to serve as an opportunity for future researchers who may try to improve the system.

3.4. Enhanced DLP-based Algorithm Security Analysis

The further testing of the Enhanced DLP-based algorithm demonstrated 100% processing accuracy across 1,000 samples. The process involved actual code deployment and used test data with pre-determined, manually computed output that was compared with the results produced by the system. This, however, only proves the accuracy of the process, an essential factor for testing, but it lacks analysis on how secure the process was.

To further test the method along security, Pearson Correlation was used to determine the existence of patterns between the plaintext and ciphertext during the encryption process using statistical analysis. This process is necessary as part of the initial security assessment. Established patterns between input and output are normally a significant sign of encryption defects. Powerful pattern searching algorithms for cracking encryption methods could exploit this vulnerability to break the encryption process. Pearson Correlation could check if there is no linear relationship between the plaintext and ciphertext, which is a good sign of a high level of security. Two numerical variables (inputs and outputs) with no linear relationship are normally a sign of strong encryption security.

In the case of the Enhanced DLP-based Algorithm, the security analysis using Pearson Correlation using 500 samples revealed an r value of 0.054631131 (closer to zero than +1), which showed no to very minimal pattern between the plaintext and ciphertext, which means that the algorithm is cryptographically secured from pattern searching algorithms.

$$r = \frac{\sum(x-\bar{x})(y-\bar{y})}{\sqrt{\sum(x-\bar{x})^2 \sum(y-\bar{y})^2}} \quad (5)$$

Using Pearson's Correlation Formula (5), the observed data, input (plaintext) and output (ciphertext), x and y respectively, are computed to get the correlation coefficient r , which is between +1 and -1. A near +1 value is a perfect positive relationship, which means that the output y moves in the same direction as input x when changes are introduced (Table 1), while a near -1 value means that the output y moves in the opposite direction of input x when changes are introduced. Both (+1 and -1), however, showed patterns between the input and output, which is a matter of security concern and may be taken advantage of by pattern searching algorithms. A value near zero (very minimal to 0) indicates that there are no established patterns between input (x) and output (y), and is a good indicator of security for a cryptographic algorithm.

Table 1. Interpretation of correlation coefficient value

Value of Correlation Coefficient r	Meaning
+1	Perfect Positive Relationship
0	No Linear Relationship
-1	Perfect Negative Relationship

A standard and better way of testing the security level of a cryptographic algorithm is by using the Avalanche Effect Sensitivity Test. The process is done by inducing minimal change in the input (plaintext) and observing the changes triggered by the input in the output (ciphertext). In cryptography, this is normally done by changing one bit in the plaintext and expecting to change more than 50% of the bits in the ciphertext as a basis for the security of the process.

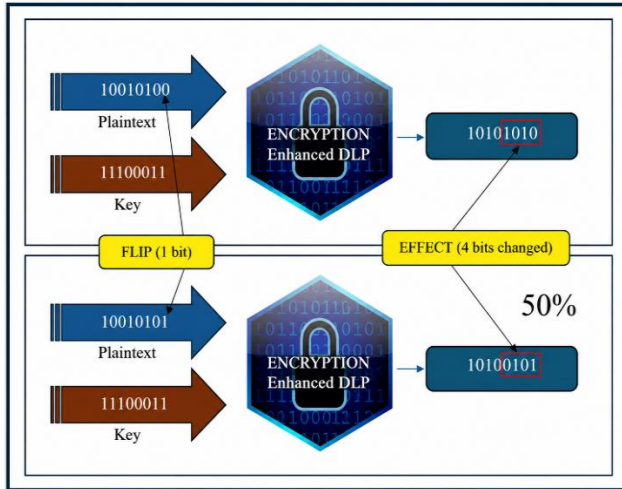


Fig. 8 Illustration of diffusion test process flow

Diffusion Test, as shown in Figure 8, is an application of the Avalanche Effect test that tests the test of independence between the plaintext and ciphertext. The effect on the ciphertext is observed by flipping a bit in the plaintext and checking how many bit flips happened in the ciphertext as a result of the single bit change in the plaintext after the cryptographic process.

The cryptographic process is deemed secure if the average percentage of observations is more than 50% for all the test cases. The illustration in Figure 8 demonstrates the process, showing a comparison between the initial stage and the situation after the bit flip.

Confusion test, as shown in Figure 9, is also an application of the Avalanche Effect tests, but the observation is done between the Encryption Key and the Ciphertext. The bit flip is done in the Encryption key, and the observation is done on its effect on the ciphertext.

The same case with the Diffusion test; the process is deemed secure if the average percentage of observation is more than 50% for all the test cases. The Diffusion and Confusion Tests are both anchored on the concept of the Avalanche Effect.

However, the observation is only focused on the average effect on the output for the bit flip triggers in the input. If the average change for all test cases is more than 50%, the method

is deemed secure. This is regardless of whether some of the test cases fall below 50%, as long as the mean of the results is more than 50%.

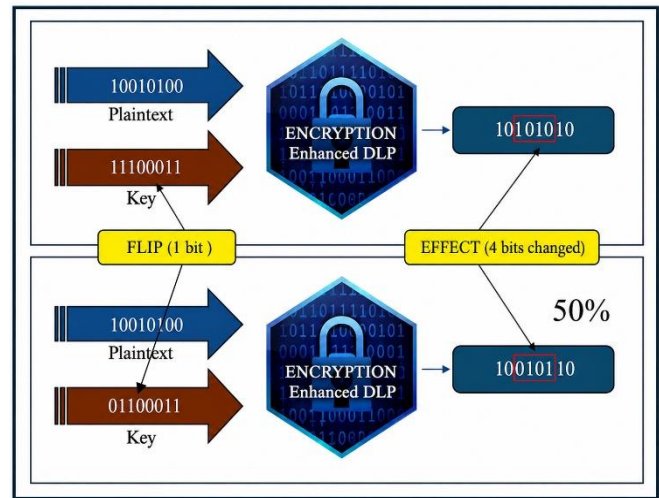


Fig. 9 Illustration of the confusion test process flow

The Strict Avalanche Criterion is an extension of the Avalanche Effect, but requires that the 50% threshold be observed for all instances of bit change. This means that every bit flip must produce at least a 50% change in the output to qualify for this security criterion.

This security analysis is merely an extension of the Avalanche effect and may be applied for both Diffusion and Confusion Tests to elevate the level of security analysis. This study utilized the Strict Avalanche Criterion (SAC) for deeper security analysis.

The security evaluation using tests of independence (Pearson Correlation) and sensitivity tests (Diffusion and Confusion Tests) showed no observable encryption or decryption patterns in the process. For the Pearson Correlation Test's r value of 0.054631131, nearing 0 rather than +1 or -1, the test showed that the ciphertext does not show or very minimal dependence on the plaintext.

This means that the Enhanced DLP-based algorithm is deemed safe from being broken by pattern searching algorithms (Cryptanalysis), which rely heavily on established patterns between inputs and outputs. The performed confusion test in the algorithm produced a value of 54%, while the diffusion test yielded 54.925% of avalanche effect, both indicating a high level of security in the process (Table 2).

The Strict Avalanche Criterion (SAC) further recorded avalanche effects of 54.8% for all cases, with no cases falling below 50%, exceeding the minimum 50% threshold, thus confirming the security of the process. Overall, the results proved that the Enhanced DLP-based algorithm is reliable and cryptographically secure.

Table 2. Result of security analysis

Type of Test	Result	Findings
Accuracy Test	100% Accurate (1,000 Sample Tests)	Accurate
Pearson Correlation Test of Independence between the Plaintext and Ciphertext	$r = 0.054631131$	Secure
Confusion Test (Sensitivity Test)	54% Average (Above the 50% Threshold)	Secure
Diffusion Test (Sensitivity Test)	54.925% Average (Above the 50% Threshold)	Secure
Strict Avalanche Criterion (All Samples)	54.8% Average with no case falling below 50% (Above the 50% Threshold)	Very Secure

4. Discussion of Findings

The developed data backup security protocol was implemented in the university's central server system environment to provide protection to the regular database backup using a multiple digital signature framework, which is based on the developed Enhanced DLP-based multiple handshake algorithm. The implementation demonstrated that the process successfully integrated the cryptographic method into the institutional archiving process without disrupting the in-place backup generation process. The backup file, after its storage, was automatically processed by the security system, where the SHA-512 hashing procedure generated a consistent message digest representing a reliable digital fingerprint of the file. The hash was then encrypted using the five independent private keys of the designated security managers, producing a consolidated digital signature attached to the stored backup archive serving as its Security Stamp.

During actual operation, it was observed that the system consistently produced a valid digital signature for every generated backup file. The signing process follows the established protocol that requires the participation of the five security managers. The method ensures that the archive could not be sealed unilaterally by a single administrator. This proved the presence of distributed accountability in the process, which was the primary objective of this study. The signing process introduced minimal processing setbacks and was completed within an acceptable time in relation to the target backup file size. This proves that the enhanced security framework is applicable for institutional implementation, especially in academic institutions. Verification testing showed the reliability of the collaborative authentication protocol. When the verification process was initiated, the system required the mandatory participation of all five

security managers before proceeding with the verification of the stored Security Stamp. The decrypted Security Stamp was successfully reconstructed only when all private keys were present, confirming that the system prevents partial authorization and unilateral validation. The recomputed SHA-512 hash of the archived backup file consistently matched the recovered original hash from the decrypted Security Stamp when no modification of any form was performed in the file, indicating preserved integrity and authenticity of the stored database backup.

To prove this point, tampering simulations were performed by deliberately modifying portions of the copy of an archived database backup file (Table 3). In every altered case, the recomputed hash of the backup file did not match the decrypted Security Stamp, and the system correctly flagged the file as compromised, demonstrating reliable detection of alteration, thus satisfying the integrity-verification requirement. On the other hand, unaltered files were consistently identified as intact by the process. Insignificant actions and alterations-such as renaming or merely opening the file without introducing changes-did not trigger any irregularity flags as a result. Furthermore, the inability of any single Security Manager to execute the process single-handedly established operational security, as successful validation required the collective participation and approval of all authorized security managers.

Observations in the workplace showed that the Enhanced DLP-based framework strengthened trust in the archival process among system administrators and data custodians. The requirement of multiple signatories as part of the process created a check-and-balance mechanism in the system, prevents unilateral approval of sensitive institutional data, and reduces insider threat risks alike. Unlike traditional single-key digital signatures security protocols, the implemented approach ensured that responsibility for data protection was shared, documented, and verifiable.

The Enhanced DLP-Based Multiple Signature Protocol operates through three essential supporting algorithms: the Extended Euclidean Algorithm, Modular Inverse Algorithm, and Prime Number Test Algorithm, which are significant for the key generation phase, encryption phase, and decryption phase. The Complexity analysis conducted on the algorithm using Big O notation showed that both the encryption and decryption processes of the Enhanced DLP-based algorithm exhibit quadratic time and space complexity n^2 . This indicates that the algorithm requires sufficient computational resources for efficient and faster operation, especially in large-scale deployment and implementations. This raises concerns about its processing speed. The quadratic complexity for both Time and Space of the algorithm could be a major concern when the data count increases. Further studies may be conducted in this area to further improve the performance of the algorithm.

Table 3. Tampering simulation result

Test Case	Interventions and Results		
	Modification Introduced in the Database Backup	Hash Match?	Result
October 2025 Backup	No Modification	Yes	File Intact
Tamper 1	Add one Character	No	Compromised
Tamper 2	Metadata Timestamp Edited	No	Compromised
Tamper 3	Added a single space in the Text Field	No	Compromised
Tamper 4	Modified Student Grade	No	Compromised
Tamper 5	Random Byte Corruption	No	Compromised
November 2025 Backup	No Modification	Yes	File Intact
Tamper 6	Opened the File. No changes made	Yes	File Intact
Tamper 7	Random Byte Corruption	No	Compromised
Tamper 8	Deleted a Space	No	Compromised
Tamper 9	Swap Values between two records	No	Compromised
Tamper 10	Remove a space at the beginning of a text record and insert a space at the end.	No	Compromised
December 2025 Backup	No Modification	Yes	File Intact
Tamper 11	Renamed a file	Yes	File intact but under a different name
Tamper 12	Deleted a Record	No	Compromised
Tamper 13	Added a Field	No	Compromised
Tamper 14	Renamed a Field	No	Compromised
Tamper 15	Change Field Type	No	Compromised

The accuracy evaluation test that demonstrated a 100% processing accuracy as observed among 1,000 tested samples is proof of the functional reliability of the algorithm. This means that the system is fit for production based on its capability to deliver the required output.

The Test of Independence using Pearson Correlation revealed no observable encryption or decryption patterns between the Key/Message and the Ciphertext. Further testing using the Confusion test, which produced a value of 54% and the Diffusion test that yielded a value of 54.925%, is a reflection of a high level of cryptographic security. The Strict Avalanche Criterion (SAC) also recorded 54.8% avalanche effects for all test cases, which is above the minimum 50% threshold and further confirms this.

To summarize all, the Enhanced DLP-Based Algorithm is computationally accurate, highly reliable, and cryptographically secure, making it applicable for secure digital data protection deployments and implementations. The test results further confirm that the Enhanced DLP-based multi-handshake mechanism can be integrated into a real institutional data backup repository environment with an associated security framework, effectively guaranteeing authenticity, integrity, and non-repudiation of database backups while maintaining practical usability. Interestingly, instead of improving the mathematical security of DLP itself, the study showed the practical advantage of extending the

algorithm into a collaborative authorization framework through a multi-signatory scheme, which is proven to be appropriate for organizational data governance, thereby achieving its primary objective of establishing a secure, accountable, and trustworthy archival verification process for critical university records.

5. Conclusion and Further Works

5.1. Conclusion

This study covered the implementation of a secure university data backup security framework that utilizes a multiple digital signature scheme that is patterned on the Enhanced Discrete Logarithm Problem (DLP) multiple handshake security algorithm. The approach was designed to protect the regular database backup of the university that is stored in a central repository system. The process secures the files regularly by enforcing collaborative authorization among five designated security managers, each possessing an independent private cryptographic key serving as their digital signature that is used in verifying the integrity, authenticity, and non-repudiation features of the file. Before its storage, the backup file is hashed first using the SHA-512 algorithm, and the resulting message digest is encrypted using the enhanced DLP process to generate a unified digital signature attached to the archived file.

The test results showed that the system can be successfully integrated into the institutional backup workflow

and was able to enhance the existing operations. The repository site consistently produced verifiable digital signatures, required complete multi-party participation during validation, and reliably detected any unauthorized modification of saved archived files. The verification mechanism confirmed integrity and authenticity when files remained unchanged and correctly identified tampered files during simulation tests. Furthermore, the requirement for all security officers to participate in verification established operational non-repudiation and prevented unilateral approval of institutional records.

Security Analysis confirms the security of the Enhanced DLP-based Algorithm through the test of randomness and the sensitivity test. However, complexity analysis uncovers a possible drawback in the system, especially in its performance. High-speed computing resources are necessary to effectively implement the system. Comparing the Enhanced DLP-based Cryptosystem to the state-of-the-art security protocols, this method was able to accomplish what the other methods failed to accomplish. The security method's applicability is not defined by its level of security or complexity but by its ability to provide what the users need. Existing security methods can provide broad options in executing security protocols, but failed to provide the requirement of a simultaneous process of digital signing. The options that they provide can be done by sequential or parallel methods, but never do it all at the same time. The design of the encryption algorithm that they use limits their ability to execute this kind of method. This study enhanced the existing DLP-based algorithm to allow the execution of tendering digital signatures all at the same time, thus paving the way for another option of a security protocol.

Overall, the study still confirms that extending the typical DLP-based cryptographic process into a multi-signatory framework improves organizational trust and accountability in data management and preservation. The research also demonstrated the value of applying enhanced cryptography to institutional governance and highlighted the value of distributed responsibility among multiple custodians. The implemented repository security model provides a practical approach for protecting mission-critical university information and ensuring a reliable data recovery method.

5.2. Further Works

In consideration of the results of this study, it is recommended that future research focus on the major drawback uncovered during the performance analysis, which revealed that the algorithm quadratically expands as the data increases; thus, there is a need for high-speed computing resources to effectively use the framework. Research along these lines is recommended for alternative possibilities. The result of this study may also be expanded to propose a framework that extends in several directions. The system may

be enhanced by introducing threshold authorization or allowing a configurable number of additional officers to participate in the archiving process and emergency recovery scenarios without compromising accountability. Integration of Hardware Security Modules (HSM) or smart card-based key storage in the process can further protect private keys from being compromised. Additional automation may also be implemented through scheduled verification routines that periodically validate archived backups to detect silent corruption. The architecture may also be extended to support archival of distributed databases or multi-site data backup replication, enabling trusted sharing of verified academic records across distributed university systems. Performance optimization for large-scale datasets and incremental backup structures may likewise be explored to improve scalability. Finally, the framework can be adapted for other institutional applications such as research data preservation, legal document archiving, and government records management, where collective authorization and verifiable integrity are critical operational requirements.

Data Protection and Regulatory Compliance

This study was conducted in compliance with internationally accepted ethical principles for information systems, research activities, and recognized information security standards. The proposed framework follows the principles of privacy by design and security by design, integrating SHA-512 hashing with an Enhanced DLP-based multiple digital signature mechanism to ensure the integrity, authenticity, and non-repudiation of institutional database backup archives.

The conducted system evaluation was performed using authorized and controlled information without involving human subject experimentation or the collection of personally identifiable information. The implementation is consistent with the principles of ISO/IEC 27001, ISO/IEC 27002, and the NIST Cybersecurity Framework, incorporating cryptographic controls, distributed authorization, secure key management, and auditability to support secure institutional data governance.

Acknowledgments

The author expresses his sincere gratitude to the personnel and staff of the Bicol University ICT Office (BU-ICTO) for their technical support and assistance throughout the conduct of this study. Appreciation is likewise extended to the Bicol University Research & Development Management Division (RDMD) under the Office of the Vice President for Research, Development, and Extension (OVPRDE) for facilitating the research process. The author also acknowledges the Bicol University College of Science for providing the resources and encouragement that contributed to the successful completion of this work.

References

- [1] Bruce Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, 2015. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017. [[Google Scholar](#)] [[Publisher Link](#)]
- [3] FIPS 180-4, “Secure Hash Standard (SHS),” National Institute of Standards and Technology (NIST), 2015. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Xiaoyun Wang, and Hongbo Yu, “How to Break MD5 and Other Hash Functions,” *Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, vol. 3494, pp. 19-35, 2005. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] R.L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] T. Elgamal, “A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Whitfield Diffie, and M. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, 1st ed., CRC Press, 1997. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Yvo Desmedt, “Threshold Cryptosystems,” *Advances in Cryptology - AUSCRYPT '92: Workshop on the Theory and Application of Cryptographic Techniques*, Gold Coast, Queensland, Australia, vol. 718, pp 1-14, 2005. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Adi Shamir, “How to Share a Secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [11] Mihir Bellare, and Gregory Neven, “Multi-Signatures in the Plain Public-Key Model and A General Forking Lemma,” *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, United States, pp. 390-399, 2006. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [12] P.W. Singer, and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know®*, Oxford Academic, 2014. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Eric Cole, and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*, Syngress Publishing, 2006. [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Zühre Aydın Yenioğlu, “Backup Encryption and Encrypted Backup Operation Performance in SQL Server,” *International Journal of Pure and Applied Sciences*, vol. 8, no. 2, pp. 380-385, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Alexandru Boicea et al., “Comparative Study Over the Encryption and Non-Encryption of the MySQL Database,” *International Business Information Management Association*, Seville, Spain, pp. 18-23, 2016. [[Google Scholar](#)]
- [16] Douglas Robert Stinson, and Maura Paterson, *Cryptography: Theory and Practice*, 4th ed., CRC Press, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Colin Boyd, Anish Mathuria, and Douglas Stebila, *Protocols for Authentication and Key Establishment*, 2nd ed., Springer Berlin, Heidelberg, pp. 1-521, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] Giuseppe Ateniese et al., “Provable Data Possession at Untrusted Stores,” *Proceedings of the 14th ACM conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, United States, pp. 598-609, 2007. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Ari Juels, and Burton S. Kaliski, “Pors: Proofs of Retrievability for Large Files,” *Proceedings of the 14th ACM conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, United States, pp. 584-597, 2007. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] Robert Kahn, and Robert Wilensky, “A Framework for Distributed Digital Object Services,” *International Journal on Digital Libraries*, vol. 6, no. 2, pp. 115-123, 2006. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [21] ISO/IEC 27001:2022, *Information Security Management Systems-Requirements*, 3rd ed., International Organization for Standardization, 2022. [[Publisher Link](#)]
- [22] Hidehito Gomi, “Authentication Trust Metric and Assessment for Federated Identity Management Systems,” *IEICE Transactions on Information and Systems*, vol. E95-D, no. 1, pp. 29-37, 2012. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Thomas H. Cormen et al., *Introduction to Algorithms*, 4th ed., MIT Press, 2022. [[Google Scholar](#)] [[Publisher Link](#)]

- [24] Karl Pearson, "Note on Regression and Inheritance in the Case of Two Parents," *Proceedings of the Royal Society of London*, vol. 58, pp. 240-242, 1895. [[Google Scholar](#)] [[Publisher Link](#)]
- [25] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] A.F. Webster, and S.E. Tavares, "On the Design of S-Boxes," *Advances in Cryptology-CRYPTO '85 Proceedings*, Springer, Berlin, Heidelberg, vol. 218, pp. 523-534, 2000. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]