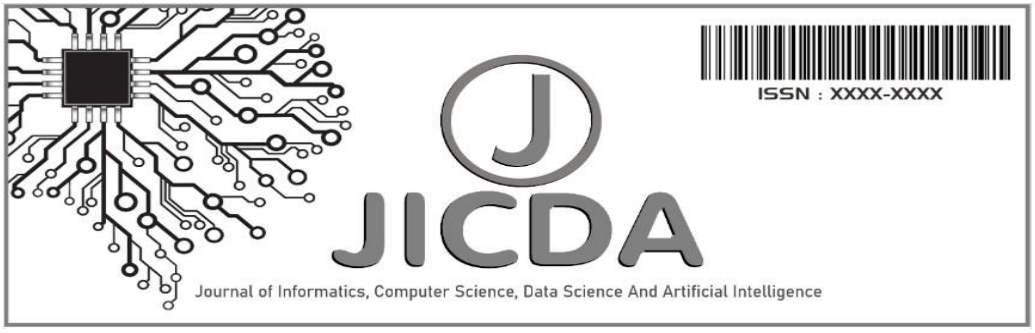
Journal of Informatics, Computer Science, Data Science And Arificial Intelligence
Volume 2 No. 2 June 2025, ISSN : 3031-9145



IMPELEMENTATION OF DSA ALGORITHM IN DIGITAL DOCUMENT SECURITY

Annisah Amalia[1], Mhd. Zulfansyuri Siambaton[2], Tasliyah Haramaini[3]
[1]Universitas Islam Sumatera Utara, annisaamaliah000@gmail.com
[2]Universitas Islam Sumatera Utara, zulfansyuri@ft.uisu.ac.id. [3]Universitas Islam Sumatera Utara, tasliyah@ft.uisu.ac.id

ARTICLE INFO

ARTICLE HISTORY:
Received : 27-05-2025
Revised : 04-06-2025
Accepted : 07-06-2025

Keywords:
Cryptography, Hash Function, Asymmetric Key, Digital Signature Algorithm, Secure Hash Algorithm-256

ABSTRACT

The Digital Signature Algorithm (DSA) is a cryptographic method used to ensure the integrity and authenticity of data by generating a unique digital signature for each document. In this study, the author examines the implementation steps of DSA, including the generation of public and private keys, as well as how digital signatures can be used to verify the sender's identity and prevent forgery. The implementation results indicate that the use of DSA significantly enhances the security of digital documents, providing strong protection against data tampering. These findings are expected to contribute to the development of more effective and reliable information security systems in the digital era.

INTRODUCTION

A signature is a form of personal identification, typically handwritten, used to authenticate documents or indicate approval. It is often a name or a distinctive symbol written by an individual. Legally, a signature plays a vital role in acknowledging or consenting to contracts, declarations, or other official documents

(Lapian et al., 2024).

A Digital Signature is a cryptographic mechanism used to ensure the authenticity and integrity of data in electronic transactions. It guarantees that the signed message or document originates from a valid (authentic) source and has not been altered since it was signed (integrity) (Ramdani et al., 2024).

To mitigate the risks of digital document tampering or forgery, robust document security mechanisms are essential. One of the most effective approaches is the implementation of digital signatures.

A digital signature is not a digitized version of a handwritten signature, but rather an encoded output generated through the Digital Signature Algorithm (DSA). The DSA utilizes a public key and a private key to create and verify the digital signature.

The main issue addressed in this study concerns security. The selection of DSA keys requires two large prime numbers for key generation. The security of DSA relies heavily on the confidentiality of the private key—if the private key is compromised, the digital signature can be forged. Furthermore, DSA employs a hash function to compute values, which plays a critical role in the overall efficiency of the system. The use of slower hash functions can negatively impact the speed of the signing and verification processes.

Technology is something we greatly rely on today, especially in our daily lives. This is because technology enables people to work more effectively and efficiently. One application of technology is the use of digital signatures on documents. Currently, many signing processes still rely on wet signatures, or what we refer to as manual signatures. Some individuals also use digital signatures by photographing their wet signature and inserting the image into the document to be signed.

Technology is something we greatly rely on today, especially in our daily lives. This is because technology enables people to work more effectively and efficiently. One application of technology is the use of digital signatures on documents. Currently, many signing processes still rely on wet signatures, or what we refer to as manual signatures. Some individuals also use digital signatures by photographing their wet signature and inserting the image into the document to be signed (Alwan & Qomariasih, 2024).

With the advancement of technology, documents are now produced not only in printed form but also in digital format. Digital documents offer advantages such as greater ease and efficiency of use; however, they are also more vulnerable to modification or forgery.

RESEARCH METHODS

Digital Signature Algorithm (DSA) Calculation

a. **Generate DSA Parameters**
Given:
p = 23
q = 11
Reason for using numbers such as p = 23 and q = 11:

1. They satisfy the mathematical requirements for DSA.
2. They are simple to use in this example calculation.

g = 4 using the formula:
$g = h^{(p-1)/q} \bmod p$
h = (p-1) / q = 22/11
h = 2
Then, p = 23, and h = 2,
$g = 2^2 \bmod 23 = 4$
g = 4

b. **Generate Private and Public Keys**
Private key = 3
Solution:
Public key $y = g^x \bmod p$
$= 4^3 \bmod 23$
y = 18

So, the public key of Annisa Amalia is y = 18, and the private key x = 3.

c. **Sign the Message**

1. Hash the message: H(m) = 9
2. Choose a random number k = 4 (where k is an integer between 1 and q – 1)
3. Calculate r:
   $r = (g^k \bmod p) \bmod q$
   $r = (4^4 \bmod 23) \bmod 11$
   r = 3
4. Calculate s:
   $s = (k^{-1} (H(m) + x.r)) \bmod q$
   $k^{-1} = 3$ (since $4.3 \bmod 11 = 1$)
   $s = (3.(9 + 3.3)) \bmod 11$
   $s = (3.(9 + 9)) \bmod 11$
   $= (3 .18) \bmod 11$

= 54 mod 11
s = 10

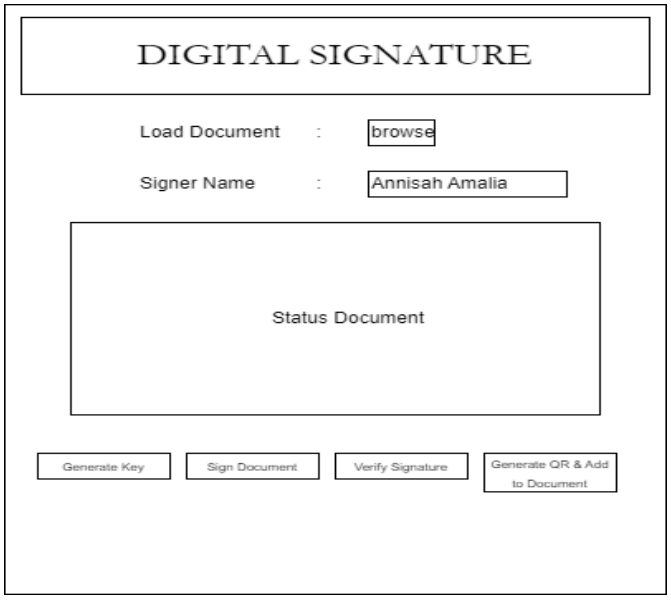
So, the digital signature for the "important document" is the pair (r, s) = (3, 10).

d. **Verify the Signature**
Signature: (r, s) = (3, 10)
Hash of the message: H(m) = 9
Public key y = 18

1. Calculate $w = s^{-1} \bmod q$:
   s = 10 mod q = 11
   w = 10 (since 10.10 mod 11 = 1)
2. Calculate u1 = (H(m).w) mod q and u2 = (r.w) mod q:
   u1 = (9.10) mod 11
   = 90 mod 11
   u1 = 2
   u2 = (3.10) mod 11
   = 30 mod 11
   u2 = 8
3. Calculate $v = ((g^{u1}. y^{u2}) \bmod p) \bmod q$:
   $v = ((4^{2} \cdot 18^{8}) \bmod 23) \bmod 11$
   $= (4^{2} \bmod 23) \bmod 11 = 16$
   $= 18^{8} \bmod 23 = 16$
   v = (16.16) mod 23
   = 256 mod 23
   v = 3

v = r, so the signature is valid because the (r, s) pair was indeed generated by the correct private key, and the signature matches the received message

Application Interface Design



is the interface design of the Digital Signature application. At the top of the interface, the application name "Digital Signature" is displayed. Next, there is a "Load Document" menu and a "Browse" button, which function to upload the document to be signed. Then, the "Signer Name" menu is available, which allows the signer's name to be entered into the document. The "Generate Key" menu is used to generate the private and public keys using the DSA (Digital Signature Algorithm). The "Sign Document" menu is used to sign the uploaded document with the private key. Next, the "Verify Document" menu is used to verify the signature on the document using the public key. Finally, the "Generate QR & Add to Document" menu allows the creation of a QR code and adds it to the document.

RESULTS AND DISCUSSION

This study successfully implemented the Digital Signature Algorithm (DSA) in a digital document security application equipped with digital signature and QR code-based verification features.

The testing results show that the DSA algorithm was effectively applied to:

- Generate private and public keys using prime number parameters ($p = 23$, $q = 11$) and generator $g = 4$.
- Create a digital signature in the form of a value pair $(r, s) = (3, 10)$ based on the hashed message.
- Verify the digital signature, which was confirmed as valid since the calculated v value matched r.

These computations indicate that the generated digital signature is valid, proving that the signing and verification processes function correctly according to DSA cryptographic principles.

The developed application also provides a feature for generating and embedding a QR code into the signed document. This feature serves to:

- Simplify the document validation process through quick and visual verification.
- Provide access to signer information and digital signature values through QR code scanning.

Thus, document authenticity verification can be performed efficiently by the recipient without requiring complex manual processes.

The use of DSA proved effective in:

- **Ensuring data integrity** – documents cannot be altered without affecting the signature.
- **Ensuring authentication** – only the holder of the private key can generate a valid signature.
- **Reducing the risk of forgery** – since forging the signature would require access to the confidential private key.

The efficiency of the DSA algorithm greatly depends on Hash function speed – SHA-256 is recommended for optimal security without compromising processing speed. Confidentiality of the private key – if the private key is exposed, the security of the digital signature is compromised. Nevertheless, the technical challenges encountered in implementing the DSA algorithm are minimal, as the algorithm is mathematically sound and easily integrable into modern digital systems.

CONCLUSION

From the research on the implementation of the Digital Signature Algorithm (DSA),

the following conclusion can be drawn:

1. Effectiveness of DSA in Digital Document Security: The implementation of the DSA algorithm is effective in maintaining the integrity of digital documents. By using a private key to create signatures abd a public key for signature verification, DSA ensures that document cannot be manipulated without detection.
2. Ease of Verification Process: The Digital Signature application utilizing the DSA algorithm is designed to facilitate the verification of document authenticity

through QR-Code scanning, allowing users to quickly and efficiently verify digital signatures.

3. Integration with Hash Algorithms: The DSA algorithm can be integrated with hash algorithms such as SHA-256 to enhance security in digital signatures. The use of a strong hash function helps ensure that the signed data remains intac and unaltered.

This conculusion summarizes the key findings of the research, emphasizing the effectiveness and practicality of implementing DSA in securing digital document.

REFERENCES

Alwan, D. A., & Qomariasih, N. (2024). Penerapan Tanda Tangan Digital dan Secure Coding berdasarkan OWASP pada Sistem E-Control Tugas Akhir. *Info Kripto*, *18*(2), 49–55. https://doi.org/10.56706/ik.v18i2.100

Lapian, R., Soeikromo, D., & Mamengko, R. S. (2024). Pengaturan Penggunaan Tanda Tangan Elektronik Menurut Uu No. 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Lex Privatum*, *13*(1).

Ramdani, M., Dzulfiqar, M. F., Abdallah, Z. A., Pahlevi, Z. R., & Rosyani, P. (2024). *Studi Perbandingan Teknik Thresholding Untuk Binarisasi Tanda*. *2*(2), 166–172.

Ajhari, Abdul Azzam, and Windarto Windarto. 2018. "Implementation of Affine Cipher and AES-128 Algorithms for Message Security and One-Time Password Account Registration in Android-Based Chatting Applications at Hang Tuah 1 High School Jakarta." Skanika 1(1): 323–34.

Alfani, Mhd Reza, Mhd Furqan, and Yusuf Ramadhan Nasution. 2024. "Text Data Security Using Digital Signature Algorithm (DSA) and Advanced Encryption Standard (AES)." Journal of Science and Social Research 4307(1): 301–6.

Alwan, Dhana Arvina, and Nurul Qomariasih. 2024. "Application of Digital Signatures and Secure Coding Based on OWASP in the E-Control Final Project System." Crypto Info 18(2): 49–55. doi: 10.56706/ik.v18i2.100.

Eritza, Afnita, Mukhlis Ramadhan, and Hafizah Hafizah. 2022. ―Application Digital Signature SHA Method and DSA Calculation Example." Journal Triguna Dharma Information System (JURSI TGD) 1(6):906. doi: 10.53513/jursi.v1i6.6002.