Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/19867
DOI URL: http://dx.doi.org/10.21474/IJAR01/19867

RESEARCH ARTICLE

A NEW DLP-BASED AUTHENTICATION ALGORITHM FOR PUBLIC KEY CRYPTOSYSTEMS

Jincy Pauly, Saju M.I., Antony John E.F. and Renjith Varghese
The Department of Mathematics, St. Thomas College (Autonomous) Thrissur 680001, Kerala, India, Affiliated to University of Calicut, Malappuram 673635, Kerala, India.

Manuscript Info

Manuscript History
Received: 08 September 2024
Final Accepted: 17 October 2024
Published: November 2024

Key words:-
Discrete Logarithm Problem, Integrity, Authenticity, Automorphism

Abstract

Authentication is essential to secure communication because it guarantees that communications come from authentic sources and are not altered while being transmitted. An efficient authentication algorithm based on the DLP (Discrete Logarithm Problem) is presented in this study. By ensuring the integrity and authenticity of messages, this algorithm enhances current encryption techniques to offer a better security.

Introduction:-

In the contemporary world, data security is vital. Someone is watching every word that is said. Therefore, it is quite difficult to make clandestine contact. Here's where encryption comes into play. There are a lot of cryptosystems available right now. A superior communication method that offers greater data protection is the "public key cryptosystem" (PKC). The DLP, the knapsack problem, and the integer factorization problem are among the difficult mathematical problems that PKC typically uses. The initial public key systems were ElGamal [1] and RSA [2]. While Diffie Hellman's ElGamal and its underlying key agreement protocol [3] are based on the DLP, RSA is based on the integer factorization problem. There are numerous updated versions of ElGamal and RSA available [4–7]. There are many variations in the ElGamal system. The ElGamal cryptosystem operates on abelian groups of integers as an asymmetric cryptosystem. Using the DLP's difficulty on a finite extension field, Saju et al. [8] developed a PKC that is more secure than ElGamal. Mahalobious [9] investigated how automorphism and DLP affected ElGamal's security.

A key component of secure communication is authentication, which guarantees that messages come from reliable sources and are not altered while being transmitted. The DLP serves as the foundation for an effective authentication algorithm that we present in this research. By enhancing current encryption techniques, this algorithm ensures the integrity and validity of messages, offering a complete security solution.By focusing just on the authentication component, which was inspired by Luu Hong Dung et al. [10], the proposed method enables seamless integration with the encryption technique [11]. This modular approach makes use of the established security of DLP-based cryptographic primitives while guaranteeing compatibility with current systems.The suggested approach uses cryptographic signatures based on the DLP's computational difficulty and functions in the context of finite fields. It successfully thwarts known-plaintext attacks, ciphertext-only attacks, and secret key attacks, protecting the integrity and authenticity of messages in situations with limited resources.

Key Formation Procedure

Several domain/system parameters are used to determine the end-user's private/public key. These parameters include:

Corresponding Author:-Jincy Pauly
Address:-The Department of Mathematics, St. Thomas College (Autonomous) Thrissur 680001, Kerala, India, Affiliated to University of Calicut, Malappuram 673635, Kerala, India.

- The prime number p
-f(x) – an n^{th}degree primitive polynomial over $\mathbb{F}_p$, satisfy: $q = p^n$. Here, to ensure the security of the scheme, select pand nsufficiently large
- An element $a \in \mathbb{F}_q^*$

A randomly chosen automorphism from $< \sigma >$, where $< \sigma >$ is cyclic group of frobeniusautomorphism on $\mathbb{F}_q$ [12], serves as the private key, and the Key generation method (Algorithm 1.1)creates the matching public key using the private key and domain/system parameters in the manner described below:

Algorithm 1.1:

```
input: $p, q, a$
output: $\phi(), \phi(a)$
[1]. Pick a secret key$\phi \in < \sigma >$
[2]. Utilizing the following formula, find the public key:$\phi(a)$
```

Note:
– p, q, a: The parameters of the system
– $\phi(), \phi(a)$: the private key, the public key of the end-user in the system.

Now the senders public key will be $\phi_s(a)$, and that of receiver's will be $\phi_r(a)$: if ϕ_s be the sender's (encryptor) private key and $\phi_r$be the receiver's (decryptor) private key.

Encryption

The encryption technique uses the plaintext P, the sender's private key $\phi_s()$, the receiver's public key $\phi_r(a)$, and system parameters as input in the schemes built using the approach suggested here. The ciphertext$C$ and the component R are the algorithm's output. Here, both the sender and the recipient use component R for verification purposes.

Algorithm 1.2, the encryption algorithm, is explained in pseudocode as follows:

Algorithm 1.2:

```
input: $a, p, q, \phi_s(), \phi_r(a), P$.
output: $(R, C)$.
[1]. Determine the value of Seusing the formula: $S_e = \phi_s(\phi_r(a))$
[2]. Utilizing the function$F_1()$: determine the value of R:
        $R = F_1(P, S_e)$
[3]. Use the encryption function $E_k()$with the symmetric key k, discussed in {cite}, to encrypt the plaintext P.
        $C = E_k(P)$
[4]. Send the recipient the ciphertext$(R, C)$.
```

Note:
– P: the plaintext.
– (R, C): the ciphertext corresponding to P.

Attention:
– $F_1()$:The function should be designed in such a way that even with P known, computing S_e is challenging.

Decryption

Inputs for the Decryption-Authentication method include the ciphertext$C$, the sender's public key $\phi_s(a)$, the receiver's private key $\phi_r()$, and system parameters. The plaintext M is the result of the algorithm. Additionally, in the schemes built using the suggested approach, M is additionally verified with respect to the message's origin and data integrity.

Here is a pseudocode description of the Decryption – Authentication algorithm (Algorithm 1.3):

Algorithm 1.3:

```
input: $p, q, a, \phi_r(), \phi_s(a), (R, C)$.
output: $M$

[1]. Evaluate the value of $S_d$according to:
        $S_d = \phi_r(\phi_s(a))$
```

[3]. To decode C, use the symmetric key k and the decryption method $\mathrm{D_k}()$.

$$\mathrm{M} = \mathrm{D}_k(\mathrm{C})$$

[4]. Determine the value of V by the function $\mathrm{F_1}()$:

$$\mathrm{V} = \mathrm{F_1}(\mathrm{M}, \mathrm{S_d})$$

[5]. Verify that if $\mathrm{V} = \mathrm{R}$, then $\mathrm{M} = \mathrm{P}$, the sender's identity and integrity have been verified.

Attention:
– $\mathrm{F_1}()$: The function should be designed in such a way that even with M known, computing $\mathrm{S_d}$ is challenging.

Proof Of Validity

Here, it must be demonstrated that the message following decryption is identical to the message before to encryption: M = P and condition V = R will be met if the received and sent ciphertexts are identical. Consequently, the receiver can be certain of the origin and integrity of the received message after decoding if the criterion V = R is met.

It must be demonstrated that if the sent and received ciphertexts are identical, the message following decryption is the same as the message before to encryption: $\mathrm{M} = \mathrm{P}$ and condition $\mathrm{V} = \mathrm{R}$ will be met. In this way, the receiver can be guaranteed of the message's integrity and origin after decoding if the criterion $\mathrm{V} = \mathrm{R}$ is met.

Indeed, we have:

$$\mathrm{S_d} = \phi_\mathrm{r}(\phi_\mathrm{s}(\mathrm{a})) = \phi_\mathrm{s}(\phi_\mathrm{r}(\mathrm{a})) = \mathrm{S_e}$$

So:
Therefore, we have the first proof:

$$\mathrm{M} = \mathrm{D_K}(\mathrm{C}) = \mathrm{D_K}(\mathrm{E_K}(\mathrm{P})) = \mathrm{P}$$

Then, we have the second proof:

$$\mathrm{V} = \mathrm{F_1}(\mathrm{M}, \mathrm{S_d}) = \mathrm{F_1}(\mathrm{P}, \mathrm{S_e}) = \mathrm{R}$$

Security

The suggested schemes' security is assessed according to how well they withstand the following common attacks:
- Secret Key Attack: To be able to compute the secret key of the end-user in the system, the attacker needs to solve the discrete logarithm problem on the finite field $\mathrm{F_p}$. Currently, no polynomial time algorithm has been published for this difficult problem.
- Ciphertext-only Attack: The analysis in [11] has shown that direct attack on the functtions$\mathrm{E_k}(), \mathrm{D_k}()$ is not viable when only ciphertext is available.
- Known-plaintext attack: Calculating kmakes no sense in this scenario, because this keyis only utilized once. However, the attacker can still find $\mathrm{S_e}$or $\mathrm{S_d}$to calculate kfor later encryption sessions. The attacker can rely on known $\mathrm{R}, \mathrm{P}$and Kto calculate $\mathrm{S_e}$and $\mathrm{S_d}$from:

$$\mathrm{R} = \mathrm{F_1}(\mathrm{P}, \mathrm{S_e})$$

However, if theselect the functions $\mathrm{F_1}()$as MD5 hash [13,14] or SHA 256 [15,16] hash functionthe attacker will not be able to achieve his goal.

Conclusion:-

Authentication is a crucial element of secure communication, ensuring that communications originate from trustworthy sources and are not tampered with during transmission. This study propose an efficient authentication algorithm based on the Discrete Logarithm Problem (DLP), which offers a comprehensive security solution by improving on existing encryption approaches and guaranteeing the validity and integrity of messages.

Utilizing cryptographic signatures generated from the computational hardness of the DLP, the suggested algorithm functions within the confines of finite fields. It successfully defends against known-plaintext, ciphertext-only, and secret key attacks, preserving the integrity and authenticity of messages in settings with limited resources.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The first author extends her deepest gratitude to the Department of Science & Technology, Government of India for financial support under ‘WISE Fellowship for Ph.D’ programme to carry out this work.

References:-

1. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory. 31, 469–472 (1985)
2. Rivest, D.R.: RSA (cryptosystem). Arithmetic Algorithms and Applications. 19 (1977)
3. Diffie, W.: Diffie-Hellman Key Exchange, (1976)
4. Panda, P.K., Chattopadhyay, S.: A hybrid security algorithm for RSA cryptosystem. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). pp. 1–6. IEEE (2017)
5. Ivy, B.P.U., Mandiwa, P., Kumar, M.: A modified RSA cryptosystem based on ‘n’prime numbers. International Journal of Engineering And Computer Science. 1, 63–66 (2012)
6. Takagi, T.: Fast RSA-type cryptosystem modulo pkq. In: Advances in Cryptology—CRYPTO’98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings 18. pp. 318–326. Springer (1998)
7. Aikins-Bekoe, S., Hayfron-Acquah, J.B.: Elliptic curve diffie-hellman (ECDH) analogy for secured wireless sensor networks. International Journal of Computer Applications. 176, 1–8 (2020)
8. Saju M.I., Renjith Varghese and E.F. Antony John.: A design of public key Cryptosystem in an algebraic extension field over a finite field using the difficulty of solving DLP. Malaya Journal of Matematik (MJM). Volume 8, 459–463 (2020). https://doi.org/10.26637/MJM0802/0022
9. Mahalanobis, A.: Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups. Florida Atlantic University. (2005)
10. Dung, L. H., Thai, N. V., Thanh, N. K., & Van Hiep, P. (2023). A method for constructing public-key block cipher schemes based on discrete logarithm problem. Journal of Military Science and Technology, (CSCE7), 15-26.
11. Jincy Pauly, Saju M I, Renjith Varghese, Antony John E F. Design of Public Key Cryptosystem Based on the Underlying Mathematical Complexity, manuscript under review in Journal of Interdisciplinary Mathematics (JIM), 2024.
12. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1996)
13. Ah Kioon, M. C., Wang, Z. S., & Deb Das, S. (2013). Security analysis of MD5 algorithm in password storage. Applied Mechanics and Materials, 347, 2706-2711.
14. Turner, S., & Chen, L. (2011). Updated security considerations for the MD5 message-digest and the HMAC-MD5 algorithms (No. rfc6151).
15. Gilbert, H., &Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In International workshop on selected areas in cryptography (pp. 175-193). Berlin, Heidelberg: Springer Berlin Heidelberg.
16. Handschub, H., & Gilbert, H. (2002). Evaluation report security level of cryptography–sha-256. Journal of Womens Health.