Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

COMPARATIVE ANALYSIS OF DIGITAL SIGNATURE ALGORITHMS (RSA, ELGAMAL)

Ergashev Isroilbek Abdirashid o‘g‘li
Chirchik State Pedagogical University
E-mail: isroilbek19960818@gmail.com.

Abstract
This paper deals with one of the most important tasks of cryptography - the electronic digital signature. Electronic digital signature (EDS) is needed to uniquely establish the author of any document. EDS is the analog of a common signature that authenticates any document or contract. In this paper we look at the advantages and disadvantages of the algorithms RSA, ElGamal.

Keywords: Encryption algorithms, electronic digital signature, RSA, ElGamal.

Introduction

АННОТАЦИЯ
В данной статье рассматривается одна из важнейших задач криптографии – электронная цифровая подпись. Электронно-цифровая подпись (ЭЦП) необходима для однозначного установления автора любого документа. ЭЦП — это аналог обычной подписи, которая удостоверяет подлинность любого документа или контракта. В данной статье мы рассмотрим преимущества и недостатки алгоритмов RSA, Эль-Гамаля.

Ключевые слова: алгоритмы шифрования, электронная цифровая подпись, RSA, Эль-Гамаль.

INTRODUCTION

Recently, information technology has entered our daily life: from important government projects to solving simple everyday problems. While new technologies offer endless opportunities and tremendous benefits, they also bring new challenges. One of them is the problem of protecting information from falling into the hands of unauthorized persons.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

There are many ways to protect information, but each of them can be reduced to one of two methods: intelligent protection of information from intruders and encryption of information.

This work is dedicated to one of the important functions of cryptography - electronic digital signature. Electronic digital signature (EDI) is necessary to uniquely establish the author of a document. ERI is an analogue of a simple signature that ensures the validity of a document or contract. Electronic digital signature enables: – Integrity control; – Protecting the document from changes (forgery); – Eliminating the possibility of denying authorship; – Proof of authorship of the document. These features of ERI are used to organize electronic document circulation with legal value.

METHOD

Electronic digital signature construction schemes.

There are several schemes for building a digital signature:

– Based on the symmetric encryption algorithm. This scheme assumes that the system has a third party - an arbitrator - who uses the trust of both parties. Document authoring consists of encryption with a private key and sending it to an arbitrator.

– Based on asymmetric encryption algorithm. Currently, such schemes of ERI are relatively widespread and widely used. In addition, there are other methods of digital signature that are modifications of the above schemes

When signing documents of sufficient size, ERI is placed not on the document itself, but on its hash. Given an input array of arbitrary length, a fixed-length bit string is called a hash.

Using hash functions provides the following possibilities:

– Reduces computational complexity;

– No compatibility issues;

– Ability to check data integrity.

Symmetrical scheme

Symmetric ERIs are less common than asymmetric ones, because after the emergence of the concept of digital signature, it was not possible to develop effective signature algorithms based on the symmetric ciphers known at that time.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

Asymmetric digital signature schemes are based on computationally difficult, unproven problems, and therefore it is impossible to say whether these schemes can be broken in the coming years. In addition, in order to increase cryptoresistance, it is necessary to increase the length of the keys, which sometimes leads to the need to rewrite the software of the asymmetric scheme, and sometimes to redesign the devices[2]. Symmetric schemes are based on widely studied block ciphers. Asymmetric scheme. ERI's asymmetric schemes belong to the type of public key cryptosystems. In digital signature schemes, signing is performed using a private key, and verification is performed using a public key.

The generally accepted digital signature scheme includes three processes: - Choosing a key pair. A private key is selected using a key selection algorithm, and then its corresponding public key is calculated; - Creating a signature. The given electronic document is signed using a private key; - Signature verification. Using the public key, the authenticity of the document and the signature are checked.

RESEARCH RESULTS

(Analysis of ERI's common algorithms)

Different mathematical schemes based on one-way functions are used in ERI algorithms to generate pairs of keys (closed and open). These schemes are divided into two groups. This division is based on certain complex problems: - the problem of calculating the factorial of large integers; - discrete logarithmization problem. RSA (derived from the initials of Rivest, Shamir and Adleman) The first and world-famous specific ERI system is the RSA system, whose mathematical scheme was developed in 1977 at the Massachusetts Institute of Technology. The reliability of the algorithm is based on the complexity of calculating the factorial of large numbers [4]. Algorithm for generating public and private keys of RSA.

Example	
Arbitrary prime numbers p and q are chosen	p=11, q=7
Multiply the numbers p and q.	n=77
The value of the Euler function in n is calculated	$\varphi(n) = 60$
An integer e that is prime to the value of $\varphi(n)$ is chosen. A prime number is usually chosen as e	e=7
A number d satisfying the following condition is chosen:: $de \equiv 1 (mod \varphi(n))$.	d=43
Q = (e,n) set will be announced.	(7,77)
Acts as a private key and is kept secret.	(43)

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

DISCUSSION OF RESULTS

Disadvantages of digital signature RSA - For the digital signature system RSA, it is necessary to check a large number of additional conditions that are difficult to perform in practice when calculating keys n modulo, e and d.

Non-fulfillment of any one of these conditions leads to the forgery of the digital signature by the person who discovered this deficiency[5,8,9]. - RSA is computationally expensive to ensure the cryptographic resistance of a digital signature to forgery (for example, at the level of the US National Encryption Standard (DES algorithm), i.e., to be 1018, the calculation of n, d and e is less than 2512 for each non-integers must be used), which is 20-30% more than the cost of creating a digital signature with the same level of cryptography using other algorithms. - Digital signature RSA is related to multiplicative attacks. In other words, the RSA digital signature algorithm allows an attacker to determine the signature by calculating the product of hashes of previously signed documents without knowing the private key d.

ElGamal (El-Gamal digital signature)

The ERI algorithm, which is easy to generate on personal computers and relatively more reliable, was developed in 1984 by Tahir El Gamal, an American of Arab origin, and named ElGamalSignatureAlgorithm (EGSA). The idea of EGSA is based on the practical impossibility of falsifying the ERI in the case of discrete logarithmization, which is more difficult to calculate than factoring a large integer. In addition, ElGamal was able to eliminate the flaw related to the forgery of ERI using some messages without knowing the private key of the RSA ERI algorithm [3]. ElGamal algorithm for generating public and private keys

1. Let's choose two prime numbers R and G,

$$G < P,\ G \in (10^{154}\ 2^{512}) \text{ and } P \in (10^{308}\ 2^{1024}).$$

These numbers are not kept confidential.

2. The sending party chooses such an integer x, $1< x (P-1)$ and follows:

$Y = G^{x} \pmod P$ The so-called public key parameter is used to verify the electronic signature is used. Here it is called the closed switch of the x-transmitter.

3. The transmitting side calculates its hash value for the given M-information:

$h(M) = m, \quad 1<m<(P-1)$

4. In the next step, the sender chooses such a number k, $1<k<(P-1)$ that

$EKUB(\kappa, P)=1$, $a = G^{\kappa} \pmod P$.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

5. From the x-secret key and using the extended Euclidean algorithm, the transmitting side determines the "b"-parameter from the following equation:

$$m = x*a + \kappa*b(\text{mod } (P-1)),$$

6. As a result, the resulting pair (a, b) in the hands of the transmitting party is considered as an electronic digital signature for the given M-information..

7. As follows, the triple (M, a, b) is transmitted to the other side through an open channel.

The second party extracts M-information from the triplet (M, a, b) and calculates its hash value $h(M) = m$.

8. The transmitting party takes the public key "Y" from the database of public keys on the server for users and calculates the following value: $Q = Y^a a^b \text{ (mod } P)$.

9. The receiving second party recognizes the transmitted M-data as valid and unaltered if and only if:

$$Q = G^m \text{ (mod } P)$$

if equality is appropriate.

Thus, it can be seen directly from the given algorithm that it is possible to sign an electronic document only with the closed key of the party transmitting information, and its verification can be carried out by a voluntary subscriber. The problem of finding a closed key for a given public key is equivalent to the problem of discrete logarithmization in a finite field with respect to large random numbers, and there is no effective algorithm for finding it today in mathematics [2-5].

SUMMARY

The El Gamal digital signature scheme has a number of advantages compared to the RSA digital signature scheme: 1) The number of integers involved in calculations in the digital signature algorithm with a specified tolerance level is 25% less, and this reduces the calculation by almost half. 2) when choosing a module p, it is enough to check that it is prime and that p-1 has a large number of prime multipliers. 3) The El Gamal scheme signature formation procedure does not allow calculating a digital signature using messages without knowing the private key (as in RSA). However, the El Gamal digital signature algorithm also has some disadvantages compared to the RSA digital signature scheme. In

Educator Insights: A Journal of Teaching Theory and Practice
Volume 01, Issue 12, December 2025
brightmindpublishing.com
ISSN (E): 3061-6964

particular, the length of the digital signature is 1.5 times longer, which requires more time to calculate [4].

REFERENCES

1. Talbot, John and Dominic Welsh. Complexity and Cryptography. Cambridge: Cambridge University Press, 2006.
2. Rothe, Jörg. Complexity Theory and Cryptology. Berlin: Springer, 2005.
3. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
5. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.
6. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004.
7. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO‘85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). – Pp. 396-402.
8. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Pp. 469-472.
9. Ergashev, I. A., & Hamdamov, A. H. (2021). KO ‘P TIPLI GALTON–VATSON JARAYONLARI UCHUN LIMIT TEOREMALAR. Academic research in educational sciences, 2(CSPI conference 3), 496-500.
10. Ergashev, I. (2022). QIZIQARLI GEOMETRIK MASALALARNI YECHISHDA KREATIV YONDASHUV. Models and methods in modern science, 1(13), 90-92.
11. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.
12. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.