Digital signature algorithm based on ElGamal, Diffie-Hellman protocol and the number π

Rolando Flores-Carapia , Víctor Manuel Silva-García , Marlon David González-Ramírez * , Miguel Gabriel Villarreal-Cervantes

Posted Date: 27 December 2023

doi: 10.20944/preprints202312.2075.v1

Keywords: Digital Signature Algorithm, ElGamal, Diffie-Hellman protocol, π number, S-box

Article

Digital Signature Algorithm Based on ElGamal, Diffie-Hellman Protocol and the Number π

Rolando Flores-Carapia †, Víctor Manuel Silva-García, Marlon David González-Ramírez †,* and Miguel Gabriel Villarreal-Cervantes †

Centro de Innovación y Desarrollo Tecnológico en Cómputo, Instituto Politécnico Nacional, 07738, Ciudad de México, México; rfloresca@ipn.mx; vsilvag@ipn.mx; dgonzalezr@ipn.mx; mvillarrealc@ipn.mx

* Correspondence: dgonzalezr@ipn.mx

† These authors contributed equally to this work.

Abstract: This research proposes an algorithm to sign messages using the ElGamal asymmetric cryptosystem, called: Digital signature algorithm based on ElGamal, Diffie-Hellman protocol and the number π (DSAπ). This proposal has a high level of security like the DSA standard, in addition, execution times are reduced in relation to it. The Diffie-Hellman protocol and the number π were used in the construction of the digital signature algorithm in conjunction with the Hash-Sha-512 function. Some experiments are presented to provide evidence that the bits on the right side of the decimal point of π appear randomly, such as: a color image was constructed of a string of consecutive bits chosen at random, of the number π. Subsequently, parameters such as: entropy, correlation, discrete Fourier transform, goodness-of-fit test χ^2 were evaluated. It is mentioned that an S-box 8×8 is involved in the signature. The sensitivity of the signature was measured, that is, when small changes are made to the sender's private key, or small changes to the message. Finally, an image was constructed using the signatures of random texts, and subsequently the randomness of its pixels was obtained, to verify that there is no relationship between the different signatures.

Keywords: Digital signature algorithm; ElGamal; Diffie-Hellman protocol; π number; S-box

1. Introduction

This research proposes an algorithm to digitally sign sensitive messages, using the ElGamal cryptosystem called Digital signature algorithm based on ElGamal, Diffie-Hellman protocol and the number π (DSAπ). It is mentioned that using the Diffie-Hellman protocol it is possible to construct a common key, both for the sender and the recipient: [1] performed an authentication between communication devices using an identifier based on ElGamal, the elliptic curve and the signature digital, which as a result, reduced computational complexity and facilitates key management; Similarly, [2] proposed a hybrid algorithm integrating Diffie-Hellman algorithm and Delta Encoding technique (Newton Forward and Backward Interpolation); [3] highlights the advantages of key management with Diffie Hellman algorithms, where an image encryption algorithm with seed-generated keys was proposed. Several systems have been developed with different approaches to sign messages in order to verify the authentication of these [4,5]. Furthermore, taking into account that any written message can be converted into an image, with the DSAπ algorithm it is possible to sign messages that can be color images or 256 gray levels. As evidence that the bits appearing on the right side of the decimal point of the number π are random, evaluations are performed on the pixels of an image obtained using the bits on the right side of the decimal point of this number. The parameters used in this work to evaluate randomness are the following: entropy, correlation coefficient or simply correlation, goodness-of-fit test χ^2 and discrete Fourier transform [6–8]. As a substantial part of the encryption process, the proposed algorithm applies an S-box 8×8, in order to ensure the randomness of the signature [9].

There are some developments that use the digital signature and ElGamal algorithm: [10] performed a generic Robot Operating System (ROS) style attack that violates unforgeability in the

 doi:10.20944/preprints202312.2075.v1

parallel environment; [11–13] developed algorithms based on the digital signature and ElGamal, they only mention some attacks that can intervene, without applying any of these, such as the discrete logarithm problem, when a cryptosystem is used, in a nutshell, they do not mention the procedures that try to know the value of the private key when the public key is known. In DSAπ the randomness of the signature is evaluated according to the following parameters: correlation coefficient, entropy, discrete Fourier transform, and the goodness-of-fit test; However, in other research, sometimes entropy is used, on occasions the correlation coefficient is used, and not often none of them [14–17]. It is important to note that two characteristics that make the proposal of this research different from others are the following: the number π and a substitution box (S-box 8$\times$ 8) [18,19].

The content of this work is presented below: Section I presents the state of the art, citing some related articles; Section II shows the models used in DSAπ; Section III presents the proposed developments; Section IV shows a digital signature of the proposed model with particular values, with the intention of illustrating it. Section V, the experiments are visualized and results are shown. The analysis of results is carried out in Section VI, and finally, in Section VII the conclusions are presented.

2. Mathematical elements used in DSAπ

This section shows a theoretical description of the elements used in this work, including the ElGamal and Diffie-Hellman algorithms.

2.1. ElGamal model and Diffie-Hellman Protocol

The ElGamal model is a digital signature scheme based on the complexity of the discrete logarithm calculation and Eq. (1) shows this model. Where p is a prime number of size 2^{2048} approximately. This cryptosystem is based on the set of residues Z_p.

$$y \equiv \alpha^x \mod p \tag{1}$$

In this work p is generated as the Eq. (2), where q_1, q_2 are primes of approximately the same size, and both are around values of 2^{1024}; furthermore, n is the smallest pair, such that it makes p prime. To verify that this number is prime, the Miller-Rabbin algorithm is used [20,21].

$$p = n(q_1 \times q_2) + 1 \tag{2}$$

The reason for expressing the prime p in this way is due to the calculation of the primitive α, given the precision of finding the prime factors of $p-1$ [22] and, n is not greater than a four-digit number, when p is approximately 2^{2048}. In addition, the following elements are also involved in the parameters p and α: two private keys and two public keys; such that, a pair of them are from the sender and the other from the recipient. The sender is named A and the recipient is named B, hence the private and public keys of the sender are: a_A, $\beta_A = \alpha^{a_A} \mod p$; and those of the recipient: a_B, $\beta_B = \alpha^{a_B} \mod p$.

The Diffie-Hellman protocol applied to the ElGamal cryptosystem generates a common key for A and B. In the case of A, proceed as follows as in Eq. (3); and for B as in Eq. (4).

$$\beta = (\beta_B)^{a_A} \mod p \tag{3}$$

$$\beta = (\beta_A)^{a_B} \mod p. \tag{4}$$

Below, in order to illustrate the point, an example is shown with particular values that are not safe in a real implementation:

Example. Consider that $q_1 = 101$ and $q_2 = 107$. For this particular case $p = 18(97)(101) + 1$, the result is $p = 176347$. Now, it is not complicated to show that $\alpha = 113$ is a generating element, because it complies with the following: $113^{(p-1)/q} \mod p \neq 1$, taking into account that q can be 2, 3, 97 or 101. In this case, the private key of A is $a_A = 5824$, and the private key of B is $a_B = 10521$. Then, the sender's

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

public key is, β_A = 94565, and the recipient's public key is, β_B = 26724. With this information, the joint key would be: $\beta = \beta_B^{a_A} \mod p = \beta_A^{a_B} \mod p = 124046$.

2.2. Hash Sha-512 Algorithm

Taking into account that the digital signature uses the output string of some Hash Sha function, and that in this case it is 512 bits; the shortest string length allowed is 224 bits [23]. To verify the integrity of the message, this tool is used [24]. Another important aspect that should be noted is that the Sha - 512 algorithm defines a function that is not one to one [25]. This property means that, when the 512-bit output string is known, it is very difficult to find the message; This problem is known as "Preimage", and the attack consists of the following: in a sample of 2^{256} messages the collision probability has at most a probability of 0.5. [26].

2.3. Digital Signature Algorithm (DSA)

In this subsection, the algorithm that is currently used to sign with the ElGamal cryptosystem is presented, this procedure is known as: Digital Signature Algorithm – DSA [27].

As mentioned above, the sender and recipient are denoted as: A, B. Additionally, the following parameters are public: two primes p, q such that q divides $p-1$. Also, the generating element α, and the public keys of the communicating people β_A and β_B.

β_A and β_B are defined as Eq. (5) and Eq. (6), respectively. Taking into account that a_A, a_B are the private keys of A and B. The prime p is defined in Eq. (7), where n is even and q_1, q_2 are primes of approximately the same size. Then, the prime q involved in this process can be q_1 or q_2.

$$\beta_A = \alpha^{a_A} \mod p \tag{5}$$
$$\beta_B = \alpha^{a_B} \mod p \tag{6}$$
$$p = n(q_1 \times q_2) + 1 \tag{7}$$

On the other hand, sender A wants to send a message X to recipient B, and sign it. From here, A, B choose the secure communication scheme of their preference, in such a way that B decrypts it according to the chosen scheme, for example PKI [28]. However, to verify the authentication and integrity of the message, A signs it, according to the following procedure:

1. An integer $1 < k < q-1$ is chosen at random.
2. The calculation of two parameters is carried out in Eq. (8) and Eq. (9).

$$\gamma = [\alpha^k \mod p] \mod q \tag{8}$$
$$\delta = (\text{ Sha } 3 - 224(X) + a_A \times \gamma) \times k^{-1} \mod q \tag{9}$$

In this calculation γ or δ can be zero, if so, another value of k is chosen. Additionally, it is important to note that A signs with his private key. Hence, the signature of A is shown in Eq. (10).

$$Sig_k(X, k) = (\gamma, \delta) \tag{10}$$

With the above, B performs the measurements shown in Eqs. (11) and (12). In this case, B received the encrypted message X, according to the chosen communication scheme, and subsequently decrypted it.

$$e_1 = (\text{ Sha3} - 224(X))\delta^{-1} \mod q \tag{11}$$
$$e_2 = \gamma\delta^{-1} \mod q \tag{12}$$

To verify that A signed the recipient B proceed as follows: the signature is true $\Leftrightarrow [\alpha^{e_1}\beta_A^{e_2} \mod p] \mod q = \gamma$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

It is noted that B uses the public key A in this verification. On the other hand, it is mentioned that there are variants of this algorithm; such as, for example, the Schnorr signature scheme [29].

2.4. π Number

DSAπ uses the number π, some comments are made below: it is a transcendent number, which implies that it is a more complex number than the irrational ones [30]; In this sense, evidence is presented related to the randomness with which the bits appear to the right of the decimal point. In the Results Section, several Tables are shown that point in the direction of the randomness that the bit strings have to the right of the decimal point of π; the S-box 8×8 is obtained from a string of bits to the right of the decimal point, which is the result of the product of an integer and π. Later it is seen that by expressing a positive integer with a factorial basis it is possible to construct a permutation. Likewise, a S-box $8 \times$ is a permutation of 256 elements [31].

2.5. Entropy

In the Results Section, randomness measurements are made when blocks of signatures are concatenated. The above is in order to support the fact that there is no relationship between the different signatures obtained through the proposed procedure. In this sense, an image of 512×512 pixels is constructed, with signature blocks using the Hash Sha-512 algorithm.

The information entropy will be useful to evaluate the randomness, which is represented in Eq. (13) [32].

$$H(x) = -\sum_{x \varepsilon X} P(x) log_2 P(x) \tag{13}$$

In practice, the image information is considered to be random if the entropy has values close to 8 [33].

2.6. Correlation Coefficient

Another useful parameter to evaluate the randomness of the information constructed with blocks of signatures is the correlation coefficient, or simply the correlation. Considering that an image of 512 $\times$ 512 pixels is generated, the evaluation of the randomness of the information in it is carried out in three directions: horizontal, vertical and diagonal [34].

The calculation of the correlation is carried out according to the following procedure: n pixels are chosen at random from the image formed with the digital signature blocks; Then, to calculate the correlation, the pixels adjacent to the randomly chosen n are considered, in the horizontal, vertical and diagonal directions. Furthermore, each randomly chosen pixel has a value ranging from 0 to 255, which is called x. In this sense, the adjacent pixel also has 256 levels, which range from 0 to 255. Adjacent pixels are denoted as y_d, where the subscript d represents the direction. The Eq. (14) evaluates the correlation. When the correlation in the three directions is close to zero, the information in the image is said to be random [35].

$$r_{d;x,y} = \frac{\frac{1}{n}(\sum_{i=1}^{n}(x_{i,d} - \overline{x}_d)(y_{i,d} - \overline{y}_d))}{\sqrt{(\frac{1}{n}\sum_{i=1}^{n}(x_{i,d} - \overline{x}_d)^2(\frac{1}{n}\sum_{i=1}^{n}(y_{i,d} - \overline{y}_d)^2))}} \tag{14}$$

To obtain the variables, $\overline{x}_d, \overline{y}_d$ that appear in Eq. (14), these are defined in Eqs. (15) and (16).

$$\overline{x}_d = \frac{1}{n}\sum_{i=1}^{n} x_{i,d} \tag{15}$$

$$\overline{y}_d = \frac{1}{n}\sum_{i=1}^{n} y_{i,d} \tag{16}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

2.7. Discrete Fourier Transform

This research proposes using the Discrete Fourier Transform (DFT) to measure the randomness of the pixels of an image that is constructed with blocks of signatures, which are generated randomly. In fact, this parameter tests for no repetitive bit strings. This instrument is a statistical hypothesis test: where the null hypothesis assumes that the information is random [36].

Below are the elements involved in this process, one of them is the test statistic, this variable is defined in Eq. (20).

The decision parameter is expressed in Eq. (21). In this same sense M_0 in (17) is a constant and l in (18) is a bound. It is important to mention that m is the length of the bit string being evaluated.

$$M_0 = \frac{(0.95) \times m}{0.05} \tag{17}$$

$$l = \sqrt{\mathrm{Ln}\frac{1}{0.05}(m)} \tag{18}$$

To calculate the functions g_j that are expressed in Eq.(19), the variable y_k = -1, 1; and the constant $i = \sqrt{-1}$; Likewise, $j = 1, 2 \ldots \frac{m}{2} - 1$, considering that m is even, since the pixels are built with Bytes. Relative to M_1 of Eq. (20), it is noted that it starts with the value zero; that is, $M_1 = 0$. Subsequently, the calculation of $\| g_j \|$ is carried out for all j, and the result of each one is compared with l. If it is less, 1 is added to M_1, otherwise, the variable M_1 remains with the same value.

$$g_j = \sum_{k=1}^{m} y_k e^{\frac{2\pi(i)(k-1)j}{m}} \tag{19}$$

When the calculations of the $\| g_j \|$ for all j are completed, the final value of M_1 is obtained, it follows that it is possible to calculate the statistic e using Eq. (20), taking into account that, in statistical hypothesis tests there is a region of rejection, and therefore one of acceptance. In this sense, the variable $P - value$ expressed in Eq. (21) is taken as the decision parameter; That is, if the value of $P - value$ is less than 0.01, then the randomness hypothesis is rejected, otherwise it is accepted [37]. It is clarified that, in this research, the level of significance is 0.01.

$$s = \frac{M_1 - M_0}{\sqrt{\frac{m(0.95)(0.05)}{4}}} \tag{20}$$

$$P - value = \mathrm{erfc}\frac{|\, s \,|}{\sqrt{2}} \tag{21}$$

The erfc function is calculated according to Eq.(22); taking into account that $\Phi(x)$ is the cumulative function of the standard normal.

$$\mathrm{erfc}\frac{|\, s \,|}{\sqrt{2}} = 2(1 - \Phi(|\, s \,|)) \tag{22}$$

2.8. Goodness-of-Fit test

The procedure to calculate the goodnes-of-fit test parameter is also a statistical hypothesis test [38]. In this sense, this parameter assesses how much the distribution of information adjusts to one that is uniform, which will determine that the information is random, although it is clarified that it is possible to construct a theoretical distribution which is not random, but is adjusts to a uniform distribution; However, in practice it is considered that if the information fits a uniform distribution, it is said to be random; In addition, the randomness of the information is evaluated with other parameters.

There is a null hypothesis and another alternative. In fact, the null hypothesis considers that the distribution of bits conforms to a uniform distribution; but, when the evidence says otherwise, then it is rejected. Every hypothesis test has a statistic; In fact, it is the instrument with which information is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

evaluated; Furthermore, this, together with the level of significance, defines a region of acceptance and rejection. The statistic used in this research is defined by Eq. (23); taking into account that the variable has a distribution χ^2 with $m-1$ degrees of freedom [39]. It is clarified that the variables o_i, exp correspond to the observed and expected value. Using the central limit theorem the statistic χ^2 approximates a normal distribution. In fact, the mean μ has a value of 255, and the standard deviation, σ, has a value of approximately 22.5 [40]; Also, it is taken into account that the information is graphed in a histogram of 256 possible levels. Furthermore, the significance level proposed in this work is $\alpha = 0.01$. Based on this information, the rule for making a decision is as follows: if the value of the statistic, χ^2, according to the information is less than or equal to 308; that is, $\chi^2 \leq 308$, then the null hypothesis is accepted. Otherwise it is rejected.

$$\chi^2 = \sum_{i=1}^{m} \frac{(o_i - \exp)^2}{\exp} \tag{23}$$

3. Presentation of new Elements

In this section some contributions are presented, such as the algorithm to generate permutations, as well as the digital signature proposal using the ElGamal cryptosystem.

3.1. The Permutaions Algorithm

Below is an algorithm to generate permutations. In Eq. (24) the set Z_n is defined with $n \geqq 2$.

$$Z_n = \{n \varepsilon N \mid 0 \leq n < n!\} \tag{24}$$

Also, $\forall\ n \varepsilon N$, this can be expressed on a factorial basis as shown in Eq. (25).

$$n = D_0(n-1)! + D_1(n-2)! + \ldots D_{n-2}(1)! + D_{n-1}(0)! \tag{25}$$

According to the Euclid division algorithm the coefficients D_i in Eq. (25) are unique [41]. In fact, later when the algorithm is built it will be seen that the constant 0!, $D_{n-1} = 0$. Furthermore, the constants D_i satisfy the inequality of Eq. (26).

$$0 \leq D_i < (n-i) \text{ with } 0 \leq i \leq (n-2) \tag{26}$$

With the constants D_i of Eq. (25) the algorithm to generate a permutation is described below:

1. An increasing array is constructed as follows: $Z[0] = 0$, $Z[1] = 1 \ldots\ Z[n-1] = n-1$.
2. The constant D_0 is taken, and according to Eq. (26), this constant satisfies $0 \leq D_0 < n$. Therefore, $Z[D_0]$ is an element of the array generated in I. Hence, in this research it is proposed to eliminate $Z[D_0]$ from the array, and replace it with the last element of the array generated in I; that is, by $Z[n-1]$. As can be seen, only two operations were carried out. In the first, an element is removed from the array, and in the second, its place is replaced by the last element of the array from step 1. It is mentioned that when $Z[D_0]$ is the last element of the array from the previous step, in this case 1; then, its place is occupied by the immediately preceding one; that is, in this case it would be $Z[n-2]$.
3. In this step we take D_1, and in the same way as before, $Z[D_1]$ is an element of the array that resulted in 2, because $0 \leq D_1 < n-1$. From here, $Z[D_1]$ is removed from the array in step 2, and its position is replaced by the last element of the array. In case $Z[D_1]$ is the last element of the array, then its position is taken by the immediately preceding element.
4. If its continue removing elements from the array, it reach the following scenario; $Z[D_{n-2}]$ and $Z[D_{n-1}]$, where $Z[D_{n-1}] = s$ with $0 \leq s < n$. In this sense, $D_{n-1} = 0$ because it is the only element left to eliminate, in other words, it has position zero.

Regarding the complexity of this algorithm, it can be noted that it is $O(n)$, because in each step only one elimination and substitution is performed, leaving the other elements of the array unchanged.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

The following example is proposed to demonstrate the aforementioned process:

Example. It has the following arrangement: $Z_n = \{0, 1, 2, 3, 4, 5\}$; that is, $n = 6$. The above leads to having 720 permutations; that is, from permutation 0 to 719. It is considered that $n = 491$. From here, in Eq. (27) n is expressed on a factorial basis, and then, in Table 1 the expansion is done to obtain the permutation 4, 0, 1, 2, 3, 5 of the arrangement Z_n.

$$491 = 4(5)! + 0(4)! + 1(3)! + 2(2)! + 1(1)! + 0(0)! \tag{27}$$

Table 1. Permutation of seven elements.

	$D_0 = 4$	$D_1 = 0$	$D_2 = 1$	$D_3 = 2$	$D_4 = 1$	$D_5 = 0$
0	0	0✓	5	5	5	5✓
1	1	1	1✓	3	3✓	
2	2	2	2	2✓		
3	3	3	3			
4	4✓	5				
5	5					

In this work the constants D_i are chosen randomly, that is, a number is not given and subsequently expressed on a factorial basis, since this process consumes time, and in this research one of the objectives is the reduction of time. Additionally, this tool will be used later to generate an S-box 8×8 of 256 elements. Then, since the constants D_i are chosen randomly, it follows that the permutation is also randomly chosen, which implies that the S-box will be dynamic.

To conclude the Section, it is mentioned that this algorithm generates a bijective function [41].

3.2. Digital Signature procedure proposed

Below is a description of the digital signature proposal that uses the ElGamal cryptosystem. But first, it is described how to obtain a permutation on an array of 256 elements.Where S - box 8×8 is a permutation of 256 elements; ranges from 00 to ff in hexadecimal base [42].

First, the product indicated in Eq. (30) is made. The variables involved in this expression are defined in the following subsection. In order to add insertion, it is proposed to take blocks of 1 Byte after the decimal point, starting from bit 2048. Each Byte has an associated integer that goes from 0 to 255. In this sense, the integer associated with the first Byte as d_0, to the second as d_1, and so on until Byte d_{254}. The constants D_i of the Eq. (25) are obtained as follows: $D_i = d_i \mod 256 - i$ with $i = 0, 1, \cdots 254$.

With this information, and according to the algorithm developed in the previous Subsection, it is possible to build a permutation on an array of 256 elements, and consequently the S-box with the expected characteristics.

3.3. Diffie-Hellman protocol and π number for the Digital Signature Algorithm

This proposal begins with some general comments on this scheme. It is based on the fact that the sender is called A, and the recipient is called B. Also, the module of the model is a prime $p \cong 2^{2048}$, which was generated as indicated in Section II. Furthermore, a primitive $1 < \alpha < p - 1$; that is, an integer that can generate all the elements of the set Z_p^* [43]. A has a private key $1 < a_A < p - 1$, and a public key $\beta_A = \alpha^{a_A} \mod p$. In the same way, B has a private key a_B and a public key $\beta_B = \alpha^{a_B} \mod p$.

With this information, A performs the following steps to sign a message X.

1. Randomly generate an integer k that satisfies $1 < k < p - 1$.
2. Using your private key you obtain the variable γ according to Eq.(28).

$$\gamma = k \times (\beta_B^{a_A}) \mod p \tag{28}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

Additionally, perform the calculation indicated in Eq.(29).

$$h = \text{SHA-512}(X) \tag{29}$$

Taking the integer associated with the string h of 512 bits, the operations of Eq. (30).

$$h \times k \times \pi \mapsto C \tag{30}$$

In this case, C represents a 2048-bit string, which is obtained in the following way: from the product $h \times \gamma \times \pi$ 2048 bits are taken after the decimal point. Using the algorithm described at the beginning of this section and taking the Bytes to the right of the decimal point and after bit 2048, it is possible to obtain a permutation on an array of 256 elements, which defines an $S - box$ with the agreed attributes . This box is named S.

3. Once the string C and the box S are generated, the parameter δ is obtained according to Eq. (31).

$$\delta = S(C) \tag{31}$$

The operation $S(C)$ is a substitution procedure, in this sense, The C string of 2048 bits is divided into blocks of one byte, and to perform the substitution it proceed in the same way as the Advanced Encryption Standard AES [44].

4. In this research it is proposed that the digital signature be expressed according to Eq.(32).

$$Sig(X, k) = (\gamma, \delta) \tag{32}$$

Once A sent (γ, δ), then B proceeds as follows: To confirm the authentication and integrity of message X, B uses the public key of A and carries out the calculation indicated in Eq. (33).

$$k = \gamma \times [(\beta_A)^{a_B}]^{-1} \tag{33}$$

5. Also, perform the calculation $h = \text{SHA} - 512(X)$. With the above measurements, B can obtain C by performing the operation of Eq. (30), and subsequently generate S. Then, it can be calculated at $\delta^{'}$. It is written differently, because it is not necessarily equal to δ.
6. To conclude this part, B verifies if $\delta = \delta^{'}$, if so, it confirms that the message was sent by A; Furthermore, it was not altered. Otherwise, the signature is rejected.

4. Particular values for model of signature proposed

This section illustrates the model developed with particular values, that is, the ElGamal cryptosystem as well as, at γ, the $S - box$ and the parameter δ with specific quantities. Also, in particular, the image of peppers with 512 × 512 pixels is used as message X. The latter, to calculate $h = SHA - 512(X)$. In this sense, Figure 1 shows the image of peppers.

1. The model used is $y \equiv \alpha^x \bmod p$, where the module p and the primitive α, which intervene in the signing process and are written in hexadecimal base; furthermore, $p = nq_1q_2 + 1$, with q_1q_2 being prime and n being even. The particular values of these variables are written below:

   q_1 = c90ecc40f41b8e2a0858037f4de90d2e15a6121ce9b151fb4e0d51c0de8a9666ea882eba
   9d233fa3abadf70a098be5e5a00eb1005bd8c3519301ffb272988665148d3d7239670cd33d60
   599b41160608ab5497a5d17c149d3e35f8e7f15aef0696e8c48a37e8e2ba73bcf0a267886ff2

   57f7f75b2603455a2418d69c4651d00f

   q_2 = ee5b8b66666ff516440a0501edb330ca85b09bd8e231e588a65050a93aeb664c6334cd057
   362004f76619adc2bc3dfa5d25bc76f8e5a5eb999431e6b1720512b9e78a2b47d9694c0b403a

   146d24541011ca6a4840acbe26ecda9a6ff8ac674ab6df1127c77221e9f32654e31d30a4cf70

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

442b6bfb0d4dedb99126be6ffc6eab1

$n = 62$

p = 47a9c62c3021e4dbd0e8ee548d5e1b2dc6a1c4f5bb0345f720ba54f2256a9befb394d7b15 5fa27bfe1701aa3f61732f852c51deebd0b20bfc098266348d5cdff871e3d4a6b623a3a40c3a44

95d13b699771c4c9d036ef1cce70c746d618ad2000520ffe9db5764e74e2344befe45688d4a4ff 14219e346de9911f398aa6c86438e38ab0ffcfe56160fb060f361e0c06335c458a516a6bd6a0e4 2677593be5b0d663905152c4ffb9d0cbc7552904a7c13453008950343bd204d41ed3d47cd4b f4fa03956208dfe0c5f1d9fa8275073ca63f20df1de1bbedec281f890956a2355 e8517a334e9c1 e8c8aea862d3b5965e1c6c22ef7efe212154c979e9fbdfc7e7445f

α = 1bc36c7fd8704a7d008f320070dc9c2a2cd51047d7d48401816693f6d f3c83f6a99d7 2bf3d8555f192dcbe33aaabad164070b905b92a8d2bbc8f2c72eab5bb61fa1e549 3c21c7fd1

dd8c2e50f06072b4c31bf0e3ca3e07574c361d6b9eec474229ae024fb3fcf3f040f937eef2e638

3e644189be811aaf8e7175111ce364a24c960e7273514b7772fffaa39d7074465e53a76ec78ac

3270a938295fcf51b5dc962240658513aaab0c383005dbf7ae530c5fcd4c7420e0301bb4d89b

0e3de8f61f6c844155c81aed618c6dd7e4be4d2277376e6b93c4001a717b2376911f14a017ca f3d6f8da8adabeeed578d0fa3a4bd1b7b74adbe82b2327936f352b60248ce

The particular values of private and public keys, both for the sender and for the recipient, as well as the common key, β, are presented below:

a_A = c3ef3be7248d72be5de8d531ff2b5aaa1c5c6caf2d7fade94302fd3eb923f53e0e9fa67a1 5fa19a842af51ddb4a6d897fe633c9c5c908cfeca68df86fe58cdcc08300cc05ea38c0020cb8d6

d19a465a7688d97122cca67a978fcd71d1cc709c96a0213d389753cfa8a99d212a648e1a3aa1 8bf86036ebbe10eeed469a950163c74572d00e1fdb9fbbc08531b3486ec9d0c46f25c9543cf

5eb4d31d2071adaf339a6ee586e938c0e3762a4492029ffbd536a98d77a3f63b740f7aea002b 0f6844818863da1f7f14ae896ed735502fb18b2f77818ceba6e6d4be952dc9bb37e6b6fce38e

a1f7f174ee8004590ea1a22600a0e2a8a584d9f40273c2e73d82e5284a

β_A = 4067213f39fd257d30ac2a17470628c0beb1dc53c806ce4632e026e4350299cc7f484072 af98a7f88e67cbee75ea7721c09a728508dd7626438ad5d49c7716f6f6d5d397cec0c7b98f229 48cec6b251e198ea11c48690320d8faa22cc20ee21fc76eb50ed84f226d13536fecb7d85520d4 e78eb36ded395ca07d3ef85c906e8a592042e948fcfdc3c7d78d79e8bccb577c9c00796c47421 215bd9c0fb8b03a41e4901e652642b2d63e0885c2c161e9da36c10d363f848ec2d973a5dc155 e9129c73adb1411920a72f3653c23845558805a9d404e7116a8be0bbbad58c2837520a5b4220 e16d27aa628a1ec3f191363db1db54380d87480b2ee48bc1580c06a26a2

a_B = c4b942d9c75e950495fa22f46b196ecc45fb5332fa4b4b23ffff999144af53c80f08ea89c639 1677d8da4258938cb48dbf085ca2bbbb9899725c4ee9dc4e47ce7c1e80b0e1f2825cd97540eb 8bac8a907fe02eb404a93c44b065bc47489fb10ede073e0e838d910f4375ea95fd462f14bd8e 7872a3acf19da600f26c9a62ac0aa6371c633234648814db059be90be459c991d526aa044766 51352ee84059f8983acfcc92936dcacfe2264d1c0763e7a05397292c22e1025df53a4ef69542

ab68bc4aec1073cf47a6e42cad7aeff27ad81fa94c5afabcd543068f43fd25de8248237a335784

d829354d541ac289cb23cf9166b78a6c648d29bd09703d50edbf4a

β_B = 25df467d93e9ad760aadaeabf23be2bb6fd579707964433ed719bac3878cab157ee2b05 f5209475ce133ceab202f8cbae552f62852bda4031f1603cc082134a111fcf3a8867e2c5ab884b 9da0b6a9fe1bc9ece7410467421e03cde66d5a2de2840c8896c1eb63d0230c17ac46af284e1d1 5de080004fa87b7cd816c5c09d44295e385eca13f00659a1532de359a7d7716032db3998b5ad b0b529f36a6d5c65f8c831e555f17de40f841203574598652568a399f159327fc1da17a75b2d

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

fa087c9ec69bcd09efe897f4acf41c8c6fc93ecbfd7ad60c7344e8451c8dbdad5b51544ed769
d525a678383dc27706ee2cd788a34d8955d18cfd640b5af8c4091093f99

β = 154b4820e5d1480d15f78ae71061a2699c9bce5883f22b70083ccadcc15b03592ab89461
740860487fb8c8b49c785f1b68a2884b007283921a0531dc79f5e212bc27fd0500855c32942f
d759bb491f024133ee6928fca8116a686900004177fa04b4ae2ddc7b50449abcf17c421b8ea3
0f671736771d25794bdfde42f2cedd0d2378942150023a2d1cc949793ec7ee2172277bedc4a2
7cf50c9352bc3b1a5120dfd55a3778604cac6f1b52350909d62d9e2e263c81b5b3a96f7cf52e
fbaf738776138b454fd32d3fe6fa501ad84ae2f70a2b6c97caee23446feede85dd58a5f3a62b
7c965cc78e6e551d34d50eddfc9f756e9704345edf4bf15c6e9b03f320b1f2

2. In relation to the variables k and h that were used in this development, they are shown below, as well as the box that was generated with these values is presented in the Table 2.

k = 0053f7811cbc41ddd8ee8d01888a31508b6f5b07b0838ca4c4b347856c3705ce351a6b90
e9f9be27240a96e22660d1e9e96cca5b75c6cbb6732dbf7c00cc2b12c4be5fea42d4e8e47095
48f18a86e8f922aa4dfe7c4c8a8118fbf5248fd51d90a208fb988f95669ea757cc351c441f081f
f10cf92a5b728d9ae31186809a82d1b7bf66a23985e2ddae184ab745e21b9dc7092f54e93c2b
60e1af3baa3b63015cecaaca0fa7ea02286fa0ea7f6da8874003bbdd1620385d85d5269b9728
7843ba28934de8410e6f08d1b8d394fade0a7bb9cd3f473795af825f105856b022f073534118
357037d104bc262efe56cc4bd3d3087df1979dcae066349bee3aa7b00e56

h = 0c91b4b65321c770d0e892391636893f757bcf982364ae934991c546ec1d920b387d61f52
d087ca87205ecbb980cae454bcf223191ce506b542e680d5483d2f6

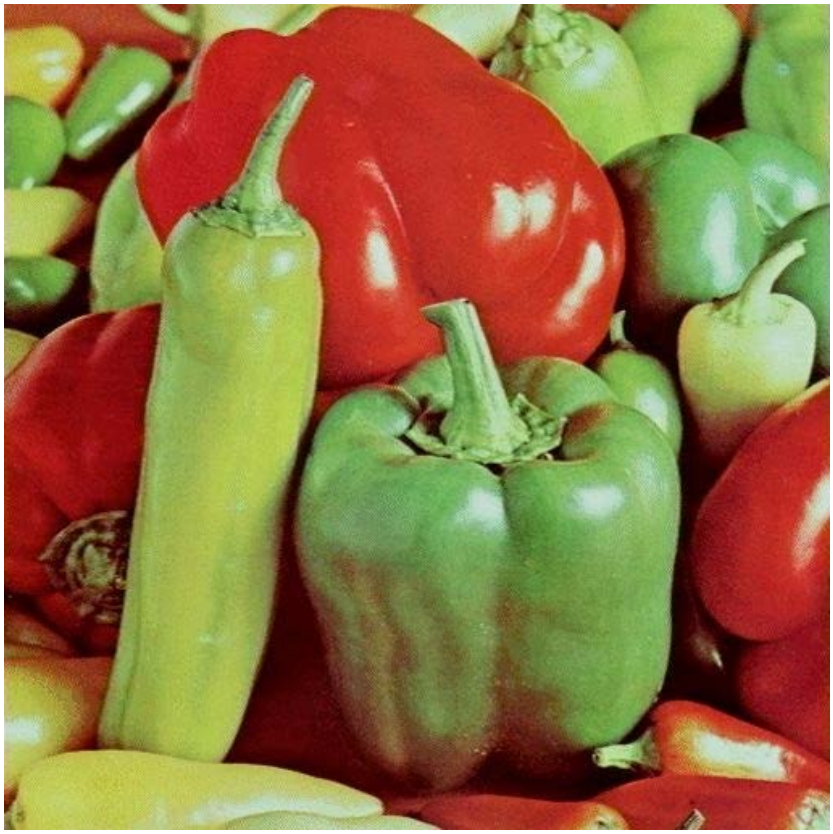

Figure 1. Peppers image of 512 × 512 pixeles size.

3. Finally, the values of the parameters are described, *Gamma* and *Delta*, which represent the signing of the sender, that is, $F(Gamma, Delta)$. In addition, the information of the π number was obtained from some important works [45,46].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

γ = 1d95637beae8d5e86c5c9d16b1cc6087cfd7ed7a9addda50f2cd7cea7dcddbbc1d6e8f1
747584383177ddfd8aa87e8ea4d2ae6047e5b7f5f7cfe344a87a47d21550e4d99f8697237f2d
1e14d432b2cf50252048ffaad2c9d634b8bed1ff369a25122edff9d099095e4c3600004b3be9
5fdc728f878b0b62ed46ab4d595109ea2a465c67aefb42a2d885f17e82af6460e59f28c61efb
362ea32e7e6c821a5dd5d15816953cf22ca0084d30147969faa28a1c483c29026e7a269f7054
e845c3ad70cc087ca61827c06088be618fb82775659b177108986f91e9753521d50f205d1f93
de1a222f11398d693ebd6dcf71741ec6a2b84bdbc185d69918a5ab89219a2d4

δ = 21c7b8510dac23a98bfcedccc90102e20983e26dc8d713da2e4f1266403df05a31e4ac3
bee8e6ee7244945f3c0fc74907b3a15ac5ee40feeec7ac3cbbb033ddd123fd6b896c34638b70
f050700adc7cc10639a314f118d598e071d68753ac1766a7f34cf5505eb6712346648d95018a
b2978602f1ec7dccea7e52c6f791895892e41b18d8efb32b3dae46ac2f2b8258aa222be42359
c803fe929b0d388ad741dfdf79034b36f17cb31298f2b8ce87f955220bda00f536cdd9e3407c
8bf61fd4cad3c0c8a220b4a6fd1649dae2a5d80ce87ee095724549ef86bf689d52a2e085d961
913ff056f5f7bb69dd490508c954c3148765c9272870de1e4c8e7d31830b3

Table 2. The S-Box 8 × 8 taking into account the particular values of k and h.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
80	00	21	6e	89	c2	4a	5d	f4	0a	1f	01	f6	9a	1e	0b
ad	09	f8	69	42	9c	e0	20	48	2c	25	de	cf	fc	19	7e
e5	ef	4c	1b	44	77	d2	46	82	73	93	24	f1	8a	02	03
84	d4	fa	64	60	95	79	08	27	c1	51	0e	e7	ac	6c	07
86	5c	54	2d	f0	6f	16	7d	39	dd	04	ec	52	45	b5	bd
df	fd	b2	49	30	e4	17	3b	62	29	9d	cd	cb	ae	56	b7
14	ab	26	d1	6d	a4	5a	db	36	0f	94	f7	53	e9	d3	05
eb	c9	61	c7	34	b9	63	cc	8d	9b	a1	f3	18	67	0c	e1
75	22	74	81	3e	aa	dc	c5	06	d0	e6	b8	58	31	4d	90
97	4f	6a	b0	ea	68	72	fe	c6	c4	1d	55	a6	10	a5	ff
28	fb	ca	96	47	7f	4e	43	b6	f2	33	d5	23	7b	41	c0
e3	1c	85	76	be	83	a7	b1	92	59	f5	ee	66	ed	8b	b3
0d	e2	3f	e8	40	87	99	37	bb	8f	2f	5f	70	d7	5b	88
15	13	c3	c8	da	a9	a8	2a	65	8c	af	f9	32	d8	12	1a
4b	6b	a2	11	57	bc	2e	78	2b	ba	d6	a3	98	bf	7a	9e
50	7c	a0	d9	35	9f	3d	3c	3a	ce	38	71	b4	8e	91	5e

Hexadecimal values.

5. Experiments and Results

This section presents the results of the experiments related to the digital signature and the number π, as well as the results of some experiments with π.

5.1. Π *number*

It is stated that the probability of the value of a bit of the right side of the decimal point, either 0 or 1, is 0.5. That is, if a position on the right side of the decimal point of the π point is randomly chosen, the probability that the value of the bit in said position is zero or one is 0.5. Therefore, the Table 3 is shown as evidence of this characteristic.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

Table 3. Estimation of the probability of a bit $P(X_I)$ to the right of the Decimal Point of Pi.

Chain length 2^n	Percentage of zeros	Percentage of ones
$n = 3$	75.000000 %	25.000000 %
$n = 6$	57.812500 %	42.187500 %
$n = 9$	54.687500 %	45.312500 %
$n = 12$	51.318359 %	48.681640 %
$n = 15$	49.935913 %	50.064086 %
$n = 18$	50.069427 %	49.930572 %
$n = 21$	49.978303 %	50.021696 %
$n = 24$	49.978560 %	50.021439 %
$n = 27$	50.003378 %	49.996621 %
$n = 30$	49.999330 %	50.000669 %
$n = 33$	50.000011 %	49.999988 %
$n = 39$	49.999981 %	50.000018 %

In this work the following experiment is carried out: from the bits chain on the right side of the decimal point of π, a block of consecutive bytes is randomly taken, so that they form an image of 512 $\times$ 512 pixels. Figure 2, which shows us a color image of this π block, is built.

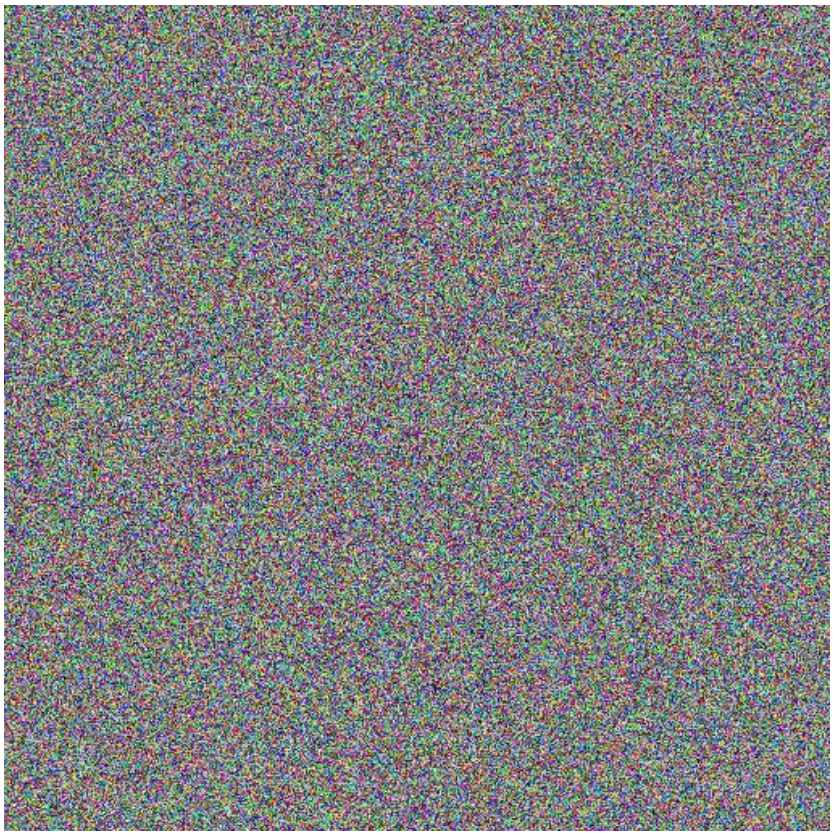

Figure 2. Image of π built with a block of 512 $\times$ 512 pixels chosen at random

In the Table 4 the values of the entropy of each basic color are shown.

Table 4. Information entropy of Figure 2.

Color	Red	Green	Blue
Entropy	7.99928	7.99935	7.99925

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

5.2. An Image Construccion Using Signatures Blocks

In this part, the following experiment is carried out: different values of K are chosen at random and, consequently, different parameters γ, δ are obtained. With these blocks of 2048 bits a color image of size 512×512 pixels is generated. To show that the information contained in the image is randomly, the following measurements are carried out: entropy, correlation coefficient in the directions: horizontal, vertical and diagonal [47]. Also, the discreet transform of Fourier and Goodness-of-Fit Test is used according to the χ^2 distribution. First, Figure 3 is shown, which was built with blocks of 2048 bits using the parameters γ, δ.

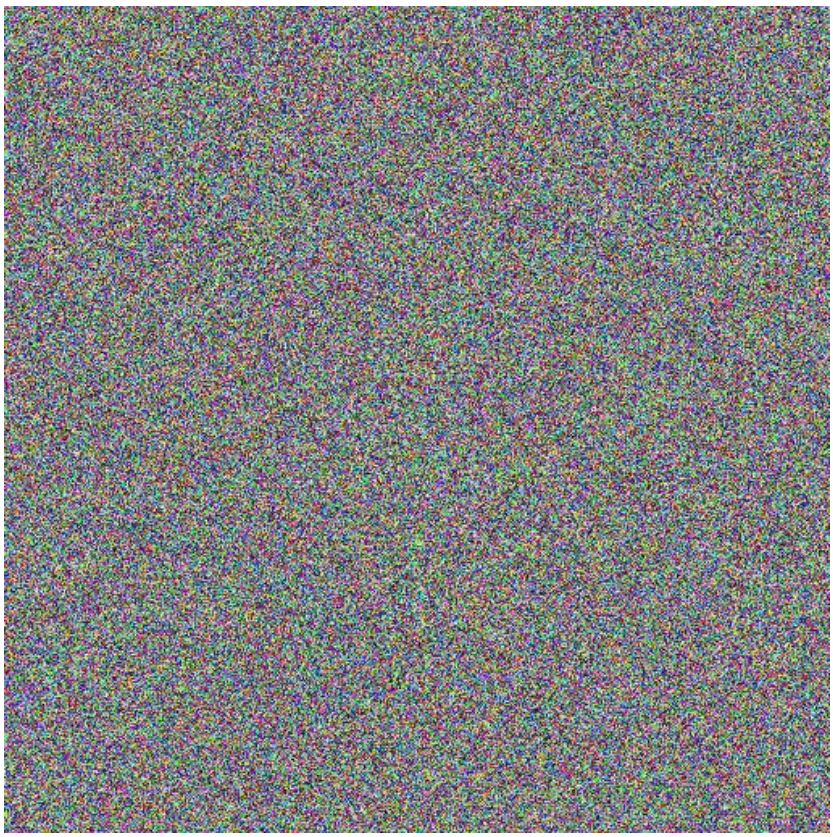

Figure 3. Image of 512×512 pixels, built with blocks of 2048 bits using γ, δ. These parameters are obtained randomly generating different values of K.

Values related to entropy and correlation coefficient, these are presented in the Tables 5 and 6.

Table 5. Information entropy of Figure 3.

Color	Red	Green	Blue
Entropy	7.99922	7.99928	7.99937

Table 6. Correlation coefficient of Figure 3.

Correlation	Red	Green	Blue
Horizontal	0.00140	0.00501	0.00150
Vertical	0.00608	0.00895	−0.00145
Diagonal	−0.00907	−0.00150	0.00917

The values of the parameter measurements: discreet transformed from Fourier and Goodness-of-Fit Test, these are shown in the Tables 7 and 8.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

Table 7. Discrete Fourier Transform of Figure 3 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
DFT	0.52272/✓	0.67178/✓	0.35863/✓

Table 8. Goodness-of-fit test applied to Figure 3 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
χ^2 **test**	0.07/✓	0.08/✓	0.11/✓

5.3. Sensitivity to changing plain text

The results related to changes in the plain text message are shown, in order to provide evidence of the integrity of the signature. DSAπ uses Lena's image, Figure 4, as a message, and subsequently a Byte in the image is modified. Then, the γ, δ associated with each change are evaluated and, in the same way as in the previous subsection, an image is generated with the 2048-bit blocks. This is presented in Figure 5.

Figure 4. Image of π built with a block of 512 $\times$ 512 pixels chosen at random.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

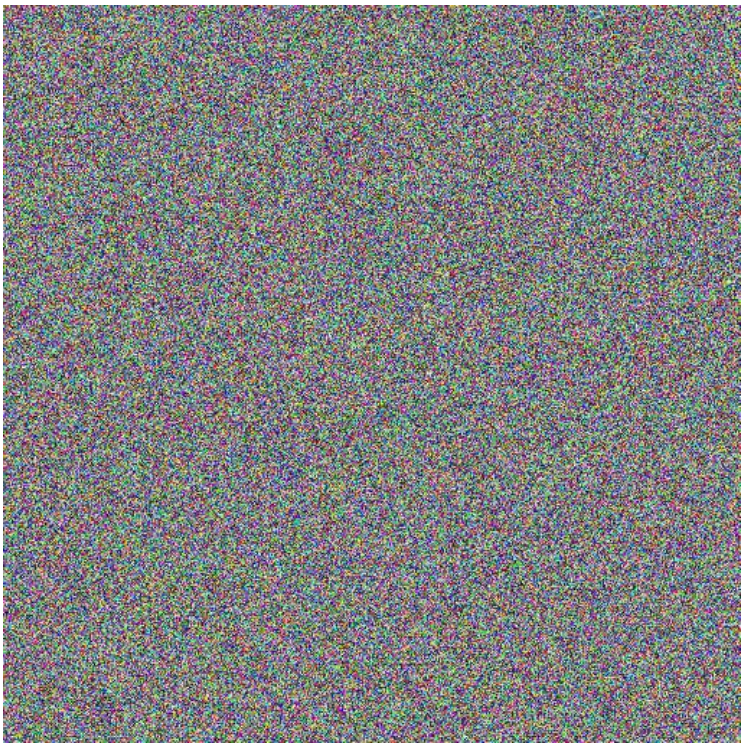

Figure 5. Image of 512 × 512 pixels, built with blocks of 2048 bits using γ, δ: These parameters are obtained by randomly generating different values of k.

Tables 9, 10, 11 and 12 describe the results of the entropy, correlation coefficient, DFT and goodness-of-fit test with the intention of showing the bits of the image. In this order of ideas, Tables 9 and 10 present the results of the entropy and the correlation coefficient.

Table 9. Information entropy of Figure 5.

Color	Red	Green	Blue
Entropy	7.99934	7.99930	7.99926

Table 10. Correlation coefficient of Figure 5.

Correlation	Red	Green	Blue
Horizontal	0.00130	−0.00418	−0.00477
Vertical	0.00023	0.00061	0.00337
Diagonal	0.00341	0.00104	−0.00278

In this same sense, Tables 11 and 12 present the evaluations of the DTF parameters and goodness-of-fit test of Figure 5.

Table 11. Discrete Fourier Transform of Figure 5 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
DFT	0.49/✓	0.09/✓	0.29/✓

Table 12. Goodness-of-fit test applied to Figure 5 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
χ^2 **test**	0.79/✓	0.55/✓	0.31/✓

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

5.4. Sensitivity to changes in the sender's private key

For the purpose of providing evidence related to sender authentication, the following experiment is then carried out: random changes are made to the sender's private key, and subsequently an image, RGB, of 512×512 pixels is constructed. Afterwards, the following measurements are carried out on the generated image: entropy, correlation coefficient, discrete Fourier transform and goodness-of-fit test. In a nutshell, the aim is to show that the image information constructed in this way is randomly distributed. Which would mean that there is no relationship between the different signatures that are obtained when the sender's private key is modified. Figure 6 presents the color image that was obtained as mentioned above.

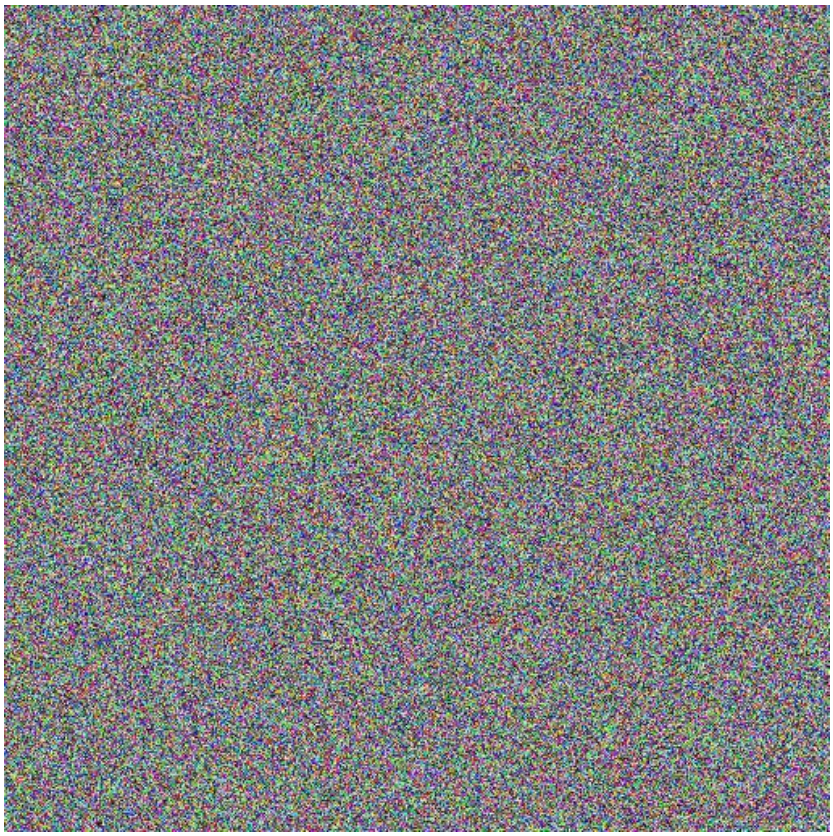

Figure 6. Image of 512×512 pixels, built with blocks of 2048 bits using γ, δ. These parameters are obtained by randomly modifying the sender's private key.

Regarding the entropy and the correlation coefficient in the three directions of Figure 6, these are shown in Tables 13 and 14.

Table 13. Information entropy of Figure 6.

Color	Red	Green	Blue
Entropy	7.99927	7.99927	7.99922

Table 14. Correlation coefficient of Figure 6.

Correlation	Red	Green	Blue
Horizontal	−0.00321	−0.00090	−0.00293
Vertical	−0.00203	0.00138	0.00157
Diagonal	0.00068	−0.00543	0.00340

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2075.v1

The resulting values of the discrete Fourier transform parameters and goodness-of-fit-tes are presented in Tables 15 and 16.

Table 15. Discrete Fourier Transform of Figure 6 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
DFT	0.43/✓	0.68/✓	0.57/✓

Table 16. Goodness-of-fit test applied to Figure 6 information (✓ Accepted, x rejected), with significance level $\alpha = 0.01$.

Color	Red	Green	Blue
χ^2 **test**	0.37/✓	0.33/✓	0.11/✓

6. Analysis of Results

First, an analysis of the security of the digital signature scheme proposed in DSAπ is carried out. If the attacker knows the sender's private key, a_A, it is possible to know what the message is and sign it. The above leads to the problem of the discrete logarithm; that is, having knowledge of the sender's public key, β_A, find out what is the value of a_A. In this regard, some research addresses this point, which they call *Generic Attacks* for the ElGamal cryptosystem [48,49]. These have a complexity of $O(\sqrt{p})$. Taking into account that $p \cong 2^{2048}$ these types of attacks cannot be carried out, at least, currently [50]. There is another type of attack called Pohlig-Hellman, which has the same complexity as the generic ones; that is, $O(\sqrt{p})$ [51]. It is mentioned that, when the Diffie-Hellman protocol is used, there is a risk of the *Man in the middle* attack [52]. To avoid this, it is advisable to use public key exchange and cryptographic techniques in the cloud, where authentication methods are used.

Comparing the complexity of the DSAπ algorithm with respect to the DSA standard, it is supported that the signature algorithm proposed in this research consumes less time, based on the following arguments: In both schemes Hash-Sha calculations, exponentiations and modular multiplications are performed, but there are two important differences: multiplicative inverse in DSA, and the substitution box in DSAπ. In this sense, the clarification is made that the calculations of β and β^{-1} in DSAπ are carried out in advance, because the sender and recipient know their public keys; Furthermore, this calculation is carried out once, since β is fixed. However, in the case of DSA the calculation of the multiplicative inverse of k is performed in each communication. On the other hand, if the k string is considered to have l bits, the complexity of calculating the multiplicative inverse is $O(l^3)$ [24]. Also, it should be considered that if γ or δ are equal to zero, another k must be chosen and the calculations performed again. Regarding the calculation of the box, it has a complexity of $O(n)$.

Considering that the proposed scheme uses the number π, evidence is presented that the bits on the right side of the decimal point of π appear randomly, as shown in Figure 2 and in Table 4. Which implies that there is no pattern given to the signature. In fact, Figure 3 is constructed with the signatures obtained when the value of k is varied and kept fixed to the message and the private key; Afterwards, randomness measurements are made and it is observed in Table 5 that the information in the image is randomly distributed.

It is important to show evidence that the signature is an authentication instrument. Figures 4 and 5, in addition, the Tables from 6 to 13 show that any change in the message or the sender's private key gives a random change in the signature, so an attacker faces the problem of knowing the sender's private key, that is, the discrete logarithm problem [53].

7. Conclusions

In this research work, a novel way of signing documents was developed based on the ElGamal cryptosystem, which competes with the DSA that is currently in use [24]. The above, because it is faster

and also, its security at this time cannot be violated. Also, it is noted that the parameters γ and δ of the proposed algorithm are always different from zero, which does not happen with the DSA algorithm, which can sometimes be zero and, when this is the case, the calculations must begin. again. On the other hand, evidence is presented that the DSAπ scheme is an instrument that verifies integrity and authentication, since, if changes are made to the message or the sender's private key, the signatures are different.

Measurements will be carried out according to the following parameters: entropy, correlation coefficient, discrete Fourier transform and goodness-of-fit test, in order to verify the randomness of the signature, that is, that there are no patterns in the information, which which certifies the authentication and integrity of the message. The well-known number π was used due to the randomness of its bits on the right side of the decimal point. Finally, in future work a scheme that includes post-quantum algorithms will be proposed [54].

Author Contributions: Conceptualization, methodology, formal analysis, investigation, visualization, writing—review and editing, data curation, software, validation, writing—original draft preparation Flores-Carapia, R; Silva-García, V.M; González-Ramírez, M.D.; Villarreal-Cervantes, M.G.; resources, supervision, project administration, funding acquisition,Flores-Carapia, R.

Funding: This work was funded in part by the financial support program of the Comisión de Operación y Fomento de Actividades Académicas (COFAA), the Instituto Politécnico Nacional (IPN) and the Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONACHYT).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon request.

Acknowledgments: The authors would like to thank the Instituto Politécnico Nacional of México (Secretaría Académica, Comisión de Operación y Fomento de Actividades Académicas COFAA, SIP, and CIDETEC), and the CONACHYT (SNI) for their support in the development of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DSAπ Digital Signature Algorithm based on ElGamal, Diffie-Hellman protocol and the number π
DSA Digital Signature Algorithm
S-box Substitution box
DFT Discrete Fourier Transform

References

1. KUMAR, Vivek, e.a. Enhanced pairing-free identity-based broadcast authentication protocol in WSN using ElGamal ECC. *Security and Privacy* **2023**, *6*, e278.
2. Dawson, J.K.; Ayawli, B.B.K.; Agyemang, S.; Baah, P.; Akyeramfo-Sam, S. Ensuring Cloud Data Security Using the Soldier Ant Algorithm. *Journal of Advances in Information Technology* **2023**, *14*.
3. Abusukhon, A.; Anwar, M.N.; Mohammad, Z.; Alghannam, B. A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm. *Journal of Discrete Mathematical Sciences and Cryptography* **2019**, *22*, 65–81.
4. Wang, L.; Yuan, Y.; Ding, Y.e.a. Analysis and Design of Identity Authentication for IoT Devices in the Blockchain Using Hashing and Digital Signature Algorithms. *International Journal of Distributed Sensor Networks* **2023**, *2023*.
5. Schoenmakers, B.; Segers, T. Secure Groups for Threshold Cryptography and Number-Theoretic Multiparty Computation. *Cryptography* **2023**, *7*, 56.
6. Parida, P.; Pradhan, C.; Gao, X.Z.; Roy, D.S.; Barik, R.K. Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access* **2021**, *9*, 76191–76204.

7. Qin, Y.; Zhang, B. Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal. *Applied Sciences* **2023**, *13*, 8117.
8. Badawy, M. Security Evaluation of Different Hashing Functions with RSA for Digital Signature. *IJCI. International Journal of Computers and Information* **2023**, *10*, 99–116.
9. Shafique, Arslan, e.a. Chaos and Cellular Automata-Based Substitution Box and Its Application in Cryptography. *Mathematics* **2023**, *11*, 2322.
10. Akhmetzyanova, L.; Alekseev, E.K.; Babueva, A.A.; Smyshlyaev, S.V. On the (im) possibility of secure ElGamal blind signatures. *Mathematical issues of cryptography* **2023**, *14*, 25–42.
11. Singh, A.K.; Roy, M.K.; Karforma, S.; Mukhopadhyay, S. IMPLEMENTATION OF E-BANKING TRANSACTION SYSTEM USING ELGAMAL DS. *Journal of Data Acquisition and Processing* **2023**, *38*, 1883.
12. Mehibel, N.; HAMADOUCHE, M. Efficient and secure digital signature algorithm (DSA). *Emirates Journal for Engineering Research* **2023**, *28*, 3.
13. Adeniyi, E.A.; Falola, P.B.; Maashi, M.S.; Aljebreen, M.; Bharany, S. Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information* **2022**, *13*, 442.
14. Abdallah, H.A.; ElKamchouchi, D.H. Signing and verifying encrypted medical images using double random phase encryption. *Entropy* **2022**, *24*, 538.
15. Jasra, B.; Moon, A.H. Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system. *Expert Systems with Applications* **2022**, *206*, 117861.
16. Qin, Y.; Zhang, B. Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal. *Applied Sciences* **2023**, *13*, 8117.
17. Yousif, S.F. Performance comparison between RSA and El-Gamal algorithms for Speech Data Encryption and decryption. *Diyala Journal of Engineering Sciences* **2023**, pp. 123–137.
18. Lubis, R.K.; Pardede, A.; Khair, H. Digital Signature Security Analysis By Applying The Elgamal Algorithm And The Idea Method. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)* **2023**, *3*, 373–382.
19. Saeed, H.; Elsisi, M.; Diab, T.O.; El Sobky, W.I.; Abdel-Wahed, M.; Mahmoud, A.K. Famous Digital Signatures Used In Smart Contracts. In Proceedings of the 2023 International Telecommunications Conference (ITC-Egypt). IEEE, 2023, pp. 649–656.
20. Ngendahimana, M.; Shen, W.; et al. RSA Cryptosystem Speed Security Enhancement (Hybrid and Parallel Domain Approach). *Crypto and Information Security* **2023**, *2*, 1–20.
21. Kokaras, M.; Foti, M. The cost of privacy on blockchain: A study on sealed-bid auctions. *Blockchain: Research and Applications* **2023**, p. 100133.
22. Panario, D.; Perin, L.P.; Stevens, B. Comparing balanced sequences obtained from ElGamal function to random balanced sequences. *Cryptography and Communications* **2023**, *15*, 675–707.
23. Liu, J. Digital signature and hash algorithms used in Bitcoin and Ethereum. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022). SPIE, 2023, Vol. 12636, pp. 1302–1321.
24. Stinson D., P.M. *Cryptography: theory and practice*; Taylor & Francis group, 2019.
25. Gallian, J. *Contemporary abstract algebra*; Chapman and HallCRC, 2021.
26. FIPS, P. 180-4 Secure Hash Standard (SHS). *FIPS, PUB* **2015**.
27. Baccouri, S.; Farhat, H.; Azzabi, T.; Attia, R. Lightweight authentication scheme based on Elliptic Curve El Gamal. *Journal of Information and Telecommunication* **2023**, pp. 1–31.
28. Shawky, M.A.; Jabbar, A.; Usman, M.; Imran, M.; Abbasi, Q.H.; Ansari, S.; Taha, A. Efficient Blockchain-Based Group Key Distribution for Secure Authentication in VANETs. *IEEE Networking Letters* **2023**, *5*, 64–68. https://doi.org/10.1109/LNET.2023.3234491.
29. Lei Wang, Y.Y.; Ding, Y. Analysis and Design of Identity Authentication for IoT Devices in the Blockchain Using Hashing and Digital Signature Algorithms. *International Journal of Distributed Sensor Networks* **2023**, *2023*.
30. Balasubramanian, K.; Davidson, E.R. Rational approximations to pie: transcendental π and Euler's Constant e. *Journal of Mathematical Chemistry* **2023**, pp. 1–6.
31. Garipcan, A.M.; Erdem, E. FPGA modeling of a novel fully-synthesizable and secure TRNG based on key-dependent s-box. *Digital Signal Processing* **2023**, *136*, 103969.
32. Shannon, C.E. A mathematical theory of communication. *The Bell System Technical Journal* **1948**, *27*, 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

33. Rana, S.; Mondal, M.R.H.; Kamruzzaman, J. RBFK cipher: a randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment. *Cybersecurity* **2023**, *6*, 3.
34. Wen, H.; Kang, S.; Wu, Z.; Lin, Y.; Huang, Y. Dynamic RNA Coding Color Image Cipher Based on Chain Feedback Structure. *Mathematics* **2023**, *11*, 3133.
35. Al-Mhadawi, M.M.; Albahrani, E.A.b.; Lafta, S.H. Efficient and secure chaotic PRNG for color image encryption. *Microprocessors and Microsystems* **2023**, *101*, 104911.
36. Heumann, C.; Schomaker, M.; Shalabh. Hypothesis testing. In *Introduction to Statistics and Data Analysis: With Exercises, Solutions and Applications in R*; Springer, 2023; pp. 219–265.
37. Ahakonye, L.A.C.; Nwakanma, C.I.; Lee, J.M.; Kim, D.S. SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet of Things* **2023**, *21*, 100676.
38. Luengo, E.A.; Olivares, B.A.; Villalba, L.J.G.; Hernandez-Castro, J. Further analysis of the statistical independence of the NIST SP 800-22 randomness tests. *Applied Mathematics and Computation* **2023**, *459*, 128222.
39. Lorenzo-Seva, U.; Ferrando, P.J. A simulation-based scaled test statistic for assessing model-data fit in least-squares unrestricted factor-analysis solutions. *Methodology* **2023**, *19*, 96–115.
40. Silva-García, V.M.; Flores-Carapia, R.; Cardona-López, M.A.; Villarreal-Cervantes, M.G. Generation of Boxes and Permutations Using a Bijective Function and the Lorenz Equations: An Application to Color Image Encryption. *Mathematics* **2023**, *11*, 599.
41. Ventre, A.G. Algorithms. In *Calculus and Linear Algebra: Fundamentals and Applications*; Springer, 2023; pp. 257–267.
42. Mahboob, A.; Siddique, I.; Asif, M.; Nadeem, M.; Saleem, A. Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption. *Multimedia Tools and Applications* **2023**, pp. 1–19.
43. Panario, D.; Perin, L.P.; Stevens, B. Comparing balanced sequences obtained from ElGamal function to random balanced sequences. *Cryptography and Communications* **2023**, *15*, 675–707.
44. Pujiono, I.P.; Rachmawanto, E.H.; Nugroho, D.A. The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images. *Journal of Applied Intelligent System* **2023**, *8*, 69–80.
45. Müller, H. The Physics of Transcendental Numbers. *Progress in Physics* **2019**, *15*, 148–155.
46. Balasubramanian, K.; Davidson, E.R. Rational approximations to pie: transcendental π and Euler's Constant e. *Journal of Mathematical Chemistry* **2023**, pp. 1–6.
47. Lai, Q.; Hu, G.; Erkan, U.; Toktas, A. A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Systems with Applications* **2023**, *213*, 118845.
48. Blazy, O.; Kakvi, S.A. Identity-Based Encryption in DDH Hard Groups. In Proceedings of the International Conference on Cryptology in Africa. Springer, 2022, pp. 81–102.
49. De Feo, L.; Delpech de Saint Guilhem, C.; Fouotsa, T.B.; Kutas, P.; Leroux, A.; Petit, C.; Silva, J.; Wesolowski, B. Séta: Supersingular encryption from torsion attacks. In Proceedings of the Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27. Springer, 2021, pp. 249–278.
50. Lalem, F.; Laouid, A.; Kara, M.; Al-Khalidi, M.; Eleyan, A. A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques. *Applied Sciences* **2023**, *13*, 5172.
51. Li, L.; Abd El-Latif, A.A.; Niu, X. Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. *Signal Processing* **2012**, *92*, 1069–1078.
52. Khader, A.S.; Lai, D. Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. In Proceedings of the 2015 22nd international conference on telecommunications (ICT). IEEE, 2015, pp. 204–208.
53. Ranasinghe, R.; Athukorala, P. A generalization of the ElGamal public-key cryptosystem. *Journal of Discrete Mathematical Sciences and Cryptography* **2022**, *25*, 2395–2403.
54. Yang, N.; Tian, Y.; Zhou, Z.; Zhang, Q. A provably secure collusion-resistant identity-based proxy re-encryption scheme based on NTRU. *Journal of Information Security and Applications* **2023**, *78*, 103604.