CAUCHY –Jurnal Matematika Murni dan Aplikasi
Volume 7(3) (2022), Pages 483-492
p-ISSN: 2086-0382; e-ISSN: 2477-3344

On the Application of Noiseless Steganography and Elliptic Curves Cryptography Digital Signature Algorithm Methods in Securing Text Messages

Juhari*, Mohamad Febry Andrean

Mathematics Study Program, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University Malang, Indonesia

Email: juhari@uin-malang.ac.id*

ABSTRACT

Elliptic curve cryptography includes symmetric key cryptography systems that base their security on mathematical problems of elliptic curves. There are several ways that can be used to define the elliptic curve equation that depends on the infinite field used, one of which is the infinite field prima (F_P where $p > 3$). Elliptic curve cryptography can be used for multiple protocol purposes, digital signatures, and encryption schemes. The purpose of this study is to determine the process of hiding encrypted messages using the Noiseless Steganography method as well as the generation of private keys and public keys and the process of verifying the validity of the Elliptic Curves Cryptography Digital Signature Algorithm (ECDSA). The result of this thesis is that a line graph is obtained that store or hides a message using the steganography method and a message authenticity from the process of key generation and verification of validity using the ECDSA method. By selecting three samples consisting of one test sample and two differentiating samples, a line graph, an MD5 hash value, and a value at the point are obtained $M(r, s)$ different. Successively obtained values $M(r, s)$ to message "Matematika 2018", "MATEMATIKA 2018", and "2018 matematika" are $M(94,67)$, $M(15,17)$, and $M(9,16)$. The discussion in this thesis only covers the elliptic curves on prime finite field. So, for the next thesis, the next researcher can do a discussion about the elliptic curve on the finite field (F_{2^m}) or the application of elliptic curve cryptography and other steganography methods.

Keywords: cryptography; steganography; algorithm; elliptic curve; digital signature

INTRODUCTION

The form of communication in this era has gone through several stages of development. This can be clearly seen from the way people use various digital devices as a means of communication. Thanks to digital communication devices, people can communicate remotely through voice, text, images, and video. Different types of messages sent only to

Submitted: December 20, 2021 Reviewed: March 07, 2022 Accepted: March 28, 2022
DOI: http://dx.doi.org/10.18860/ca.v7i3.14434

certain parties are confidential. Therefore, in sending a message or information, it is necessary to pay attention to its authenticity or authenticity so that the message you want to convey is received by the right person an algorithm is needed to maintain the authenticity of the message or information, namely Elliptic Curves Cryptography Digital Signature Algorithm [1], [2]. A cryptographic value that depends on the message body and the sender of the message is called a digital signature or digital signature. Digital signatures generate different signatures on each document. It is a digital signature taken from the document itself [3]. Basically, the use of digital signature functions the same as signatures in printed documents, namely as a process for authentication [4]. The use of a digital signature combines two cryptographic algorithms at once, namely the first one-way hash function algorithm that will produce a message digest, and the second algorithm is the public key algorithm used to encrypt the message digest.

A hash function is a function that accepts an arbitrary-length string input and then compresses it into a fixed-sized message digest [5]. One of the one-way hash functions used is MD5 (message digest 5) which is an improvement over MD4 [6]. Broadly speaking, md5 manufacturing has four steps, namely the addition of bits of the blocker, the addition of the original message length value, initialization of the MD buffer, and message processing [7]. The public key algorithm in its implementation uses a pair of keys that are a public key that can be deployed, and a private key known to the owner only. Elliptic Curve Cryptography (ECC) is cryptography that operates on elliptic curve domains. In the process of working on cryptographic algorithms, elliptic curves require mathematical concepts, namely abstract algebra including group theory, rings, and fields [8]. In addition to abstract algebraic concepts, there is a theory of numbers, especially in the modular concept of arithmetic. In the application of cryptography, one of them is the elliptic curve digital signature algorithm or elliptic Curve digital Signature algorithm which is based on the ElGamal Signature algorithm. The result of this algorithm is in the form of the authenticity of a message M.

The method for keeping a message confidential is not just by using cryptography [9]. Another technique that can be used besides cryptography is steganography [10]. Steganography can be viewed as a complement to cryptography because they complement each other. The security of a message can be improved by combining cryptography and steganography [11]. In general, the technique used is to encrypt messages first with cryptographic algorithms, then encrypted messages are hidden in other media (voice, text, video, and images) by steganography methods [12]. If the concealment of the message on conventional steganography can degrade the quality of the cover, then the concealment of the message on the Noiseless Steganography or NoStega methods does not cause damage. Some research on elliptic curve cryptography has been done by Annisa Hardiningsih HR, creation and verification of digital signatures using the MD5 hash function and the RSA algorithm cryptography on a document. The results show that each electronic document produces a different signature, even though it is signed by the same person and electronic documents that have not changed their contents result in the decryption value of the digital signature and message digest modulo n of the same value [13].

In previous studies has been discussed related elliptic curve cryptography and is given a simple example of the use of elliptic curve cryptography in the ElGamal encoding process to make it easier to understand [14]. The study only discussed the application of elliptic curve cryptography to the ElGamal encoding process only and was limited to finite fields F_p.

In previous studies discusses the level of security and performance of cryptographic algorithms Elliptic Curves Cryptography Digital Signature Algorithm (ECDSA) or algorithms Rivest-Shamir-Adleman (RSA) [15]. So that this research will be carried out a combination of cryptography and steganography methods without the need for a cover to hide the message. The steganography method used is Noiseless Steganography (NoStega) and the cryptographic method used is the Elliptic Curves Cryptography Digital Signature Algorithm (ECDSA).

METHOD

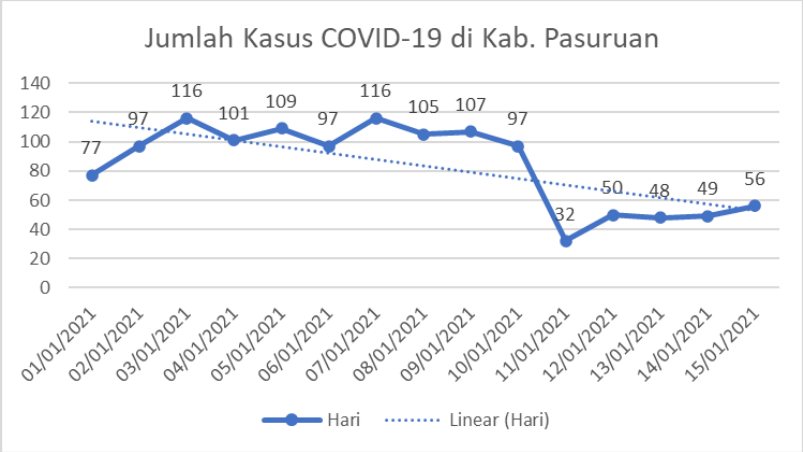
The stages of this study consist of five steps. The steps are as follows:

1. Represents message M into 8-bit ASCII code.
2. Perform a message concealment using the Steganography method.
3. Determining the equation of an elliptic curve on a primed finite field F_p.
4. Define elements of an ellipse group
   a. Calculating the modulo squared residual value p.
   b. Comparing it with the value of $y^2 = x^3 + ax + b(mod\ p)$.
   c. Specifying values $P(x, y)$ on an elliptic curve as a generator of the elliptic group.
   d. Determining a base point $B(x, y)$ selected from the ellipse group.
5. Determining the elliptic curve algorithm using the Elliptic Curves Cryptography Digital Signature Algorithm
   a. Performs the process of generating the public key and private key of the Elliptic Curves Cryptography Digital Signature Algorithm.
   b. Perform the signature generation process of elliptic curves cryptography digital signature algorithm.
   c. Verify the validity of the Elliptic Curves Cryptography Digital Signature Algorithm signature.

RESULTS AND DISCUSSION

Application of Steganography Method to a Message

Change a message M = " Matematika 2018" to a binary representation (each character is converted into an 8-bit ASCII code) to
01001101 01100001 01110100 01100101 01101101 01100001 01110100 01101001 01101011 01100001 00100000 00110010 00110000 00110001 00111000
Next, it will be converted back the above bit groups to decimal values 77 97 116 101 109 97 116 105 107 97 32 50 48 49 56 Then a graph will be made using the decimal value above, for example, the value states the number of COVID-19 cases in Pasuruan Regency.



Picture 1. Line Graph That Hides Messages "Matematika 2018"

Elliptic Curve Equation in Primed Finite Field F_p

For example, given $GF(97)$ and selected $a = 1$ and $b = 3$ with a and b fulfill $4(1)^3 + 27(3)^2 = 247 \not\equiv 0\ (mod\ 97)$, so that the elliptic curve equation is obtained [16]:

$$GF(97): y^2 = x^3 + x + 3$$

To determine the points in an elliptic curve $GF(97)$, using the method of searching the set of modulo quadratic residues. That is by looking for all elements of the modulo 97 quadratic residual set annotated with QR_{97}, using all the elements of the set $GF(97)$ as a $y$point that is then squared, and the result of the square of the y point is in modulo with 97, then the set is obtained $QR(97)$.

Modulo Prima Elliptic Group Elements $GF(97)$

Determined all points $P(x, y)$ on an elliptic curve $y^2 \equiv x^3 + x + 3\ (mod\ 97)$ by x and y equation side $GF(97)$. Then it is known the element inside $GF(97)$ is $\{0, 1, 2, \dots, 96\}$. Performed calculations for all points on the curve y^2 by substituting elements $GF(97)$ elliptic curve equation.

a. Find for modulo quadratic residues 97(QR_{97})

Table 1. Modulo Quadratic Residue 97

$y \in GF_{97}$	$y^2 (mod\ 97)$	QR_{97}
0	$y^2 (\text{mod } 97)$	0
1	$y^2 (\text{mod } 97)$	1
2	$y^2 (\text{mod } 97)$	4
3	$y^2 (\text{mod } 97)$	9
⋮	⋮	⋮
93	$y^2 (\text{mod } 97)$	16
94	$y^2 (\text{mod } 97)$	9
95	$y^2 (\text{mod } 97)$	4
96	$y^2 (\text{mod } 97)$	1

b. Determining the value of $y^2 \equiv x^3 + x + 3\ (mod\ 97)$

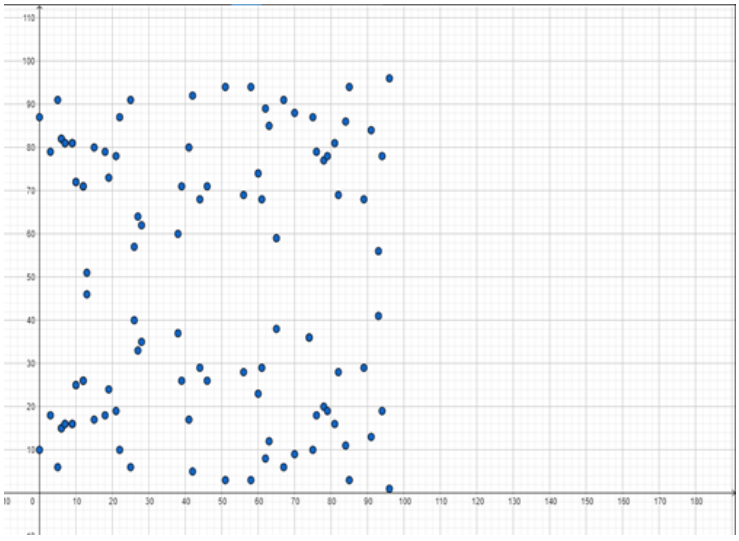
y^2 is the value of the predetermined elliptic curve equation in table 1. By substituting each value $x \in GF_{97}$ to equations $y^2 \equiv x^3 + x + 3\ (mod\ 97)$ then the results are obtained in Table 2.

Table 2. Value $y^2 \equiv x^3 + x + 3$ (mod 97)

$x \in GF_{97}$	y^2
0	3
1	5
2	13
⋮	⋮
94	70
95	90
96	1

c. Determining sequential pairs $(x, y) \subset E_{97}$

Based on table 2, for $x = 1$ obtained value $y^2 = 1^3 + 1 + 3\ (mod\ 97) = 5$. Once equalized against the modulo quadratic residual value of 97 in the table 2, apparently $y^2 = 5$ also found in QR_{97} hence for value $y_1 = 11$ and $y_2 = 18$. Then get a pair of dots $(x, y) = (1{,}11)$ dan $(x, y) = (1{,}18)$ which are the elements of the ellipse group $E_{97}(1{,}3)$.
Not all $x \in GF_{97}$ will generate a value y^2 of elements QR_{97}. For example, for $x = 0$ obtained value $y^2 = 0^3 + 0 + 3\ (mod\ 97) = 3$, While y^2 not contained on QR_{97}. So, for $x = 0$ no value y that filled.



Picture 2. Elliptic Curve Point $GF(97)$

So, the points contained on the elliptic curve are 96 points, if coupled with the O point in the infinity, then the points on the elliptic curve form a group with element $n = 97$.

Elliptical Group Generator $GF(97)$

Let's $P \in GF(97)$, then P called generator or generator of $GF(97)$ if each element $GF(97)$ can be written as a rank of P or $GF(97) = \{P^n | n \in GF(97)\}$ where $GF(97)$ is a prime number with elements in the galois field $\{0,1,2,\ldots,36\}$. In the previous discussion, 96 points have been obtained $P(x, y)$ so that the generator of the elliptic group $GF(97)$ can be searched by summing and doubling the points of the ellipse curve with the following formula:

a. Addition Elliptic Curve Point
   Let's $P(x_1, y_1) \in E(F_p)$, $Q(x_2, y_2) \in E(F_p)$, and $P \neq Q$, then $P + Q = (x_3, y_3)$ where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$
b. Doubling a point
   Let's $P = (x_1, y_1) \in E(F_p)$ then $P + P = 2P = (x_3, y_3)$ where $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = \frac{3x_1^2 + a}{2y_1}$

Of the 96 points of the curve that exist, it turns out that all of these points are generators of the elliptic group $GF(97)$.

Elliptic Curves Cryptography Digital Signature Algorithm

There are three digital signature elliptic curve algorithms used:

1. Generation of Public Key and Private Key Elliptic Curves Cryptography Digital Signature
   Known equations of elliptic curves over infinity fields $GF(p)$ that is $y^2 = x^3 + x + 3\ (mod\ 97)$. From the equation obtained pairs of points of the elliptical curve of 96 points and one infinite point which can be seen in the appendix in the table. For the generation of public and private keys a value is required P_A and P_B for each of the two sides.
   Sender generates its public and private keys as follows:
   a. Select an integer $x = 3$
   b. Count $P_A = x \cdot B$
      $P_A = 3 \cdot (0,10)$
      $P_A = 2(0,10) + (0,10)$
   By using the formula for doubling the points of the elliptic curve described earlier. The following will be shown the calculation process for the values of $2P$ and $3P$:

   a. Let's $P(x_1 = 0, y_1 = 10) \in GF(97)$, then $P + P = 2P = (x_3, y_3)$ where:
      $x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$
      $= \left(\frac{3 \cdot 0^2 + 1}{2 \cdot 10}\right)^2 - 2 \cdot 0 = \left(\frac{1}{20}\right)^2 - 0 = (1 \cdot 20^{-1})^2 - 0$
      $= (1 \cdot 34)^2 - 0 = 34^2 (mod 97) = 89$
      $y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$

$= \left(\frac{1}{20}\right)(0-89) - 10 = 34 \cdot (-89) - 10$
$= 34 \cdot 8 - 10 = 78 - 10 = 68\ (mod 97) = 68$
So $2P = (89,68)$

b. Let's
$P(x_1 = 0, y_1 = 10) \in GF(97), Q(x_2 = 89, y_2 = 68) \in GF(97)$, and $P \neq Q$, then $P + Q = (x_3, y_3)$ where:
$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$
$= \left(\frac{68-10}{89-0}\right)^2 - 0 - 89 = \left(\frac{58}{89}\right)^2 - 89$
$= (58 \cdot 89^{-1})^2 - 89 = (58 \cdot 12)^2 - 89$
$= 17^2 - 89 = 6(mod\ 97) = 6$
$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$
$= 17 \cdot (0-6) - 10 = 17 \cdot (-6) - 10$
$= (17 \cdot 91) - 10 = 82\ mod\ 97 = 82$

So $3P = (6,82)$
Then obtained value $P_A = (6,82)$. $P_A = (6,82)$ is the Sender public key and $x = 3$ the private key.

Recipient generates her private key and public key as follows:

a. Select any integer $y = 2$
b. Count $P_B = y \cdot B$
$P_B = 2 \cdot (0,10)$
By using the formula of doubling the points of the ellipse curve. Let's $P(x_1 = 0, y_1 = 10) \in GF(97)$, then $P + P = 2P = (x_3, y_3)$ where:
$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$
$= \left(\frac{3 \cdot 0^2 + 1}{2 \cdot 10}\right)^2 - 2 \cdot 0 = \left(\frac{1}{20}\right)^2 - 0 = (1 \cdot 20^{-1})^2 - 0$
$= (1 \cdot 34)^2 - 0 = 34^2(mod 97) = 89$
$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$
$= \left(\frac{1}{20}\right)(0-89) - 10 = 34 \cdot (-89) - 10$
$= 34 \cdot 8 - 10 = 78 - 10 = 68\ (mod 97) = 68$
Then obtained value $P_B = (89,68)$.

So, $P_B = (89,68)$ is Recipient's public key and $y = 2$ the private key.

2. Elliptic Curves Cryptography Digital Signature Generate Procedure
Sender generates a digital signature for a message M = "Matematika 2018" as follows:
a. Choose a random integer k, whose value lies in the hose $[1, p-1]$, will be selected $k = 10$

b. Count $k \cdot B = (x_1, y_1)$ and $r = x_1 \ mod \ p$. If $r = 0$ then back to the stage 1.
$k \cdot B = 10 \cdot (0,10)$
$= 5 \cdot (0,10) + 5 \cdot (0,10)$
$= (3,18) + (3,18)$
$= (94,19)$
So, $r = x_1 = 94 \ mod \ 97 = 94$
c. Count $k^{-1} mod \ p$
$k^{-1} \ mod \ p = 10^{-1} \ mod \ 97 = 68$
d. Calculate the hash value of M, that is $e = H(M)$.
With the message conveyed "Matematika 2018" then obtained
$e = a6bd3d71ecfd38391462dbedee65ba02$ (Hexadecimal)
$e = 221634437659671890243246613210809612 80$ (Decimal)
e. Count $s = k^{-1}(e + x \cdot r) mod \ p$. If $s = 0$, then repeat to the stage 1.
$s = 10^{-1}(22163443765967189024324661321080961280 2 + 3 \cdot 94) \ mod \ 97$
$s = 67$

Then obtained a message M be (94,67) from the generation of digital signatures.

3. *Elliptic Curves Cryptography Digital Signature* Verification Procedure Recipient will verify the digital signature (r, s) from Sender as follows:

a. Verify that r and s located inside the hose $[1, p - 1]$.
b. Retrieve the Sender public key, which is $3P_A$.
c. Recipient calculates the *Hash* value of M, that is $e = H(M)$.
$e = a6bd3d71ecfd38391462dbedee65ba02$ (Hexadecimal)
$e = 22163443765967189024324661321080961280 2$(Desimal)
d. Count $w = s^{-1} \ mod \ p$
$w = 67^{-1} \ mod \ 97 = 42$
e. Count $u_1 = e \cdot w \ mod \ p$ and $u_2 = r \cdot w \ mod \ p$
$u_1 = e \cdot w \ mod \ p$
$u_1 = (22163443765967189024324661321080961280 2 \cdot 42) mod \ 97$
$u_1 = 0$
Thus, the value of the value is obtained $u_1 = 0$
$u_2 = r \cdot w \ mod \ p$
$u_2 = 94 \cdot 42 \ mod \ 97 = 68$
Thus, the value of the value is obtained $u_2 = 68$
f. Count $(x_1, y_1) = u_1 \cdot B + u_2 \cdot P_A$
$(x_1, y_1) = u_1 \cdot B + u_2 \cdot P_A$
$(x_1, y_1) = 0 \cdot (0,10) + 68 \cdot (6,82)$
$(x_1, y_1) = 0 + (30(6,82) + 30(6,82) + 8(6,82))$
$(x_1, y_1) = 0 + \big((93,41) + (93,41) + (39,71)\big)$
$(x_1, y_1) = 0 + (26,57) + (39,71)$
$(x_1, y_1) = 0 + (94,19)$
$(x_1, y_1) = (94,19)$
g. Count $v = x_1 \ mod \ p$

$v = x_1 \ mod \ p$
$v = 94 \ mod \ 97 = 94$

From the calculation of the value v in the procedure of verifying the validity of obtaining the value $v = 94$. In the previous procedure obtained the value $r = 94$ on point $M(94,67)$. If, $v = r = 94$ then the valid signature or authenticity of a message received is correct.

CONCLUSION

The steganography method can be used to hide a secret message in another message as a *cover* so that the existence of the secret message cannot be detected. As well as the use of the *Elliptic Curves Digital Signature Algorithm* method on a message to identify or authenticate the authenticity of a message sent and received correctly from the real sender and recipient.

REFERENCES

[1] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2019.

[2] R. A. M. M.-K. Mojtaba Bisheh-Niasar, "Cryptographic accelerators for digital signature based on Ed25519," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 29, no. 7, pp. 1297-1305, 2021.

[3] P. Kitsos, N. Sklavos and O. Koufopavlou, "An Efficient Implementation Of The Digital Signature Algorithm," 2016.

[4] J. Tian, G. Xiong, Z. Li and G. Gou, "A Survey of Key Technologies for Constructing Network Covert Channel. Security and Communication Networks," pp. 1-20, 2020.

[5] L. K. A. C. M. &. L. C. Demir, "The pitfalls of hashing for privacy," *IEEE Communications Surveys & Tutorials,* vol. 20(1), pp. 551-565, 2017.

[6] Z. E. S. B. W. G. &. A. E. Rasjid, " A review of collisions in cryptographic hash function used in digital forensic tools," *Procedia computer science,* pp. 381-392, 2017.

[7] N. Hayati, A. Budiman and M. Sharif, "Implementasi Algoritma RC4A dan MD5 untuk Menjamin Confidentiality dan Integrity pada File Teks," vol. 1, p. 7, 2017.

[8] W. L. T. M. C. P. L. &. R. J. Castryck, "CSIDH: an efficient post-quantum commutative group action," pp. (pp. 395-427), 2018.

[9] P. G. A. K. T. M. C. &. Y. V. K. Dixit, "Traditional and hybrid encryption techniques: a survey. In Networking communication and data knowledge engineering," pp. (pp. 239-248), 2018.

[10] M. S. R. M. S. M. L. S. A. H. M. M. &. A. H. M. Taha, "Combination of steganography and cryptography: A Short Survey," vol. 518, 2019.

[11] H. T. S. &. H. H. T. ALRikabi, "Enhanced data security of communication system using combined encryption and steganography," vol. 145, p. 15(16), 2021.

[12] I. J. P. P. V. P. J. &. H. B. Kadhim, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing," vol. 335, pp. 299-326, 2019.

[13] H. A, "Implementasi Fungsi Hash MD5 dan Kriptografi Algoritma RSA Pada Pembuatan Tanda Tangan Digital," 2021.

[14] X. G. D. L. N. L. B. G. M. &. Q. C. Duan, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," no. IEEE Access, 2020.

[15] D. P. &. S. A. K. Timothy, "A hybrid cryptography algorithm for cloud computing security," *In 2017 International conference on microelectronic devices, circuits and systems (ICMDCS),* no. IEEE, pp. (pp. 1-5), 2017.

[16] W. Stallings, Criptography and Net Securitywork Principles and Practice, Pearson Education Limited, 2017.