CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1. Conclusion

With the fast grow in communication systems and computer networks to include all fields of daily life and used to transfer various types of data with different security levels; The researchers always develop the cryptographic systems to find more secure and confidential methods to ensure the integrity and confidentiality of transmitted data and withstand the attacks developed methods .

As discussed the cryptographic systems saw more developments and more modified algorithms, to improve cost, bandwidth or security attributes and among them the Signcryption algorithm which came to combine between the public cryptography algorithm and the signature algorisms in one step instead of the traditional approach, signature – then– encryption, with saving in communication overhead reach 40% and saving in computational cost 58%, in addition to achieve unforgeability, confidentiality, integrity and non – repudiation but lacks to achieve forward security and public variability. So, many modified signcryption algorithms came to get over the lacks of Zheng’s scheme .

Then introducing a new modified scheme “*Modified Elliptic Curve Signcryption*” this scheme based on ECDLP , in addition to achieve the functionality of the Signcryption schemes, unforgeability, confidentiality and non – repudiation it achieves forward security and encrypted message authentication or public verifiability, while others signcryption schemes lack in achieving forward security and public verifiability together in one scheme. But, reference [28] introduced modified scheme achieved the forward security and public verifiability of message but worsen the saving in communication overhead where the correct value of bandwidth saving is 20%, and increase the computational cost.

Also, the modified signcryption scheme uses a strong session key encryption depends on random choose value and the sender’s private key, plus, using the session key encryption to encrypt the message twice to increase the confidentiality and integrity of the message. The modified signcryption scheme enables the forward security so, if the adversary have the sender’s private key he must have the corresponding random chosen value to decrypt the message, and enables public variability or authenticate the encrypted message and also, check the recovered message. Although, the proposed signcryption scheme is slower than the Zheng’s signcryption scheme, it achieves saving in communication overhead reach 50% with respect to the traditional approach signature – then – encryption. And when applying the modified scheme on multiply recipients and compare it with Zheng’s signcryption for multi – recipients the new scheme achieves saving in communication overhead and computational cost higher than Zheng’s signcryption scheme.

6.2. Future work

As mentioned, IPSec mechanism is an open source mechanism can contain various of cryptographic algorithms, authentication protocols, and key management protocols to secure the sensitive transmitted data between two locations.

When applying the modified signcryption scheme on the IPSec mechanism (as mentioned in chapter 5), the transmitted data can be authenticated and encrypted in one step with less computational cost and saving in bandwidth reach 50% with respect to the traditional approach encryption – then – signature with keeping the public variability or authenticated encrypted message and in addition to increase the security of transmitted data. Also, the modified signcryption scheme is not restricted by a certain encryption algorithm while enable to use any symmetric key encryption and by this way can solve the problem of exchange the share secret key of symmetric algorithm between two peers and keep the easiness of hardware implementation of the encryption algorithms.

For the future work, if using the proposed application of applying the modified signcryption scheme on IPSec mechanism in its all cases; for authentication only, for encryption only, and for both encryption and authentication, can improve the security of computer networks and benefit with cost and bandwidth saving.

Also, I will work on enhancing the processing overhead and the computational cost of the new proposed modified signcryption scheme "*Modified Elliptic Curve Signcryption*".

REFERENCES

[1] Kartalopoulos, S. V., "Differentiating Data Security and Network Security", IEEE International Conference on Communications (ICC '08) , pp.1469-1473, 19-23 May 2008, At http://www.mediafire.com/?mtkawdjzzwj .

[2] Peter Gutmann, "Cryptography and Data Security", University of Auckland, Available at http://www.cs.auckland.ac.nz/~pgut001.

[3] Brian Morgan, CCIE No. 4865, Neil Lovering, CCIE No. 1772,"Implementing Secure Converged Area Network", July 2007.

[4] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, November 16, 2005

[5] Vijay K. Garg, "Wireless Communications and Networking ", Morgan Kaufmann , 2007, PP.449 - 461.

[6] Kenneth H. Rosen, "Elementary Number Theory and its Applications", 1984 by Bell Telephone Laboratories and Kenneth H. Rosen, Reprinted with corrections, June 1986.

[7] David A. SANTOS, "Number Theory for Mathematical Contests", August 13, 2005, http://www.4shared.com/office/2UCkUw9G/david_a_santos_-number_theory.html .

[8] Alirza Nemaney Pour, "Number Theory and Related Algorithms In Cryptography", September 2002, At http://www.freebookspot.es/Comments.aspx?Element_ID=467 .

[9] Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", 2004 Springer-Verlag New York, http://math.boisestate.edu/~liljanab/Cryptology2Spring2012/GuideToECC.pdf .

[10] Julio Lopez, Ricardo Dahab, "an Overview of Elliptic Curve Cryptography", Institute of Computing; State University of Campinas, Metadata Version 5 ,may 22, 2000, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.2771 .

[11] Ashkan Hosseinzadeh Namin, "Elliptic Curve Cryptography", Research Centre for Integrated Microsystems Electrical and Computer Engineering, April 2005, http://www.vlsi.uwindsor.ca/presentations/hossei1.pdf .

[12] Dr. Andreas Steffen, "The Elliptic Curve Cryptosystem", Zurcher Hochschule Winterthur, 8 July 2002, KSy_ECC.ppt

[13] Ashkan Hosseinzadeh Namin, "Elliptic Curve Cryptography", Research Centre for Integrated Microsystems Electrical and Computer Engineering, April 2005.

[14] Dr. Andreas Steffen, "The Elliptic Curve Cryptosystem", 2002 Zurcher Hochschule Winterthur, 8 July 2002, KSy_ECC.ppt

[15] Avi Kak, "Elliptic Curve Cryptography and Digital Rights Management ", Avinash Kak, Purdue University, April 20, 2011.ppt

[16] M. Aydos, B. Sunar, and C. K. Koc, "An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication", Electrical & Computer Engineering, Oregon State University, October 1998.

[17] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost(encryption)", Advances in Cryptology – Crypto'97, LNCS 1294, Springer-Verlag, 1997, pp. 165–179.

[18] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions", Monash University Australia, Lecture Notes in Computer Science, Vol.1397, pp.291-312, Springer-Verlag, 1998, http://www-pscit.fcit.monash.edu.au/~yuliang/.

[19] Y. Zheng, and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information Processing Letters, Vol.68, pp.227-233, Elsevier, 1998.

[20] Mohsen Toorani and Ali Asghar Beheshti Shirazi, "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme", International Journal of Network Security, Vol.10, No.1, PP.51 - 56, January 2010.

[21] Feng Bao and Robert H Deng, "A Signcryption Scheme with Signature Directly Veriable by Public Key", Institute of Systems Science National University of Singapore Kent Ridge Singapore, 1998.

[22] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," International Workshop on Practice and Theory in Public Key Cryptography (PKC-99), LNCS 1560, pp.69-81, Springer-Verlag, March 1999.

[23] Y. Han, X. Yang, and Y. Hu, "Signcryption Based on Elliptic Curve and Its Multi-Party Schemes", 3rd ACM International Conference on Information Security (InfoSecu'04), pp.216-217, 2004.

[24] H.Y. Jung, K.S. Chang, D.H. Lee, and J.I. Lim, "Signcryption schemes with forward secrecy," Proceeding of Information Security Application-WISA 2001, pp.403-475, 2001.

[25] Ren-Junn Hwang, Chih-Hua Lai, Feng-Fu Su," An efficient signcryption scheme with forward secrecy based on elliptic curve" , Department of Computer Science and Information Engineering, Tamkang University, Math. Comput. 167 (2005) pp. 870–881, Elsevier ,2004.

[26] C. Popescu," A Secure Authenticated Key Agreement Protocol", University of Oradea, Department of Mathematics, Oradea, Romania, http://q2s.ntnu.no/publications/open/2004/Paper_rev/2004_popescu_SAK.pdf .

[27] M. Toorani, and A.A. Beheshti Shirazi, "Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve," Proceedings of 2008 International Conference on Computer and Electrical Engineering (ICCEE'08), pp.428-432, Thailand, Dec. 2008.

[28] Elsayed Mohamed and Hassan Elkamchouchi, “Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy”, International Journal of Computer Science and Network Security (IJCSNS), VOL.9 No.1 , January 2009.

[29] Padma Bh, D.Chandravathi , P.Prapoorna Roja “Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz’s Method”, International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 05, 2010, 1904-1907.

[30] Brian King, “Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF(2^n)”, Indiana University - Purdue University Indianapolis, International Journal of Network Security, Vol.8, No.2, PP.169 - 176, March. 2009.

[31] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000, http://www.secg.org/download/aid-385/sec1_final.pdf.

[32] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, http://www.secg.org/download/aid-386/sec2_final.pdf.

[33] The Institute for Electrical and Electronics Engineers (IEEE) standard Annex A.7 of the P.1363, “Recommended Elliptic Curves for Federal Government Use”, July 1999.

APPENDIX A

ENCODING AND DECODING A MESSAGE IN THE IMPLEMENTATION OF ELLIPTIC CURVE

ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve not messages. Unfortunately, there are no known polynomial time algorithms for finding a large number of points on an arbitrary curve. But not simply looking for random points on E, here. So, want a systematic way of finding points on $E_p(a,b)$ relating somehow to the plaintext message. Therefore, forcing to use probabilistic algorithms to do this, where the chance of failure is acceptably small. Thus Encoding(message to a point) and Decoding (point to a message) methods are important while Encryption and Decryption [29,30].

A.1. Message Encoding and Decoding

Suppose that, a text file has to be encrypted, a user can encrypt the ASCII code of each and every printable character on the keyboard , let us say he has to encrypt an 8- bit number , can represent 128 characters on the keyboard. All the points on the elliptic curve can be directly mapped to an ASCII value, select a curve on which will get a minimum of 128 points, so that fix each point on the curve to an ASCII value. For example, ‘ENCRYPT’ can be written as sequence of ASCII characters that is ‘ 69’ ‘78’ ‘67’ ‘82’ ‘89’ ‘80’ ‘84’ can be mapped these values to fixed points on the curve. This is easiest method for embedding a message but less efficient in terms of security.

A.2. Koblitz’s Method for Encoding Plaintext

Step1: Pick an elliptic curve $E_p(a,b)$.

Step 2: Assume that E has N points on it.

Step 3: Assume that alphabet consists of the digits 0,1,2,3,4,5,6,7,8,9 and the letters A,B,C,. . . , X,Y,Z coded as 10,11,. . . , 35.

Step 4: This converts our message into a series of numbers between 0 and 35.

Step 5: Now choose an auxiliary base parameter, for example $k = 20$. (both parties should agree upon this)

Step 6: For each number mk (say), take $x = mk + 1$ and try to solve for y.

Step 7: If you can't do it, then try $x = mk + 2$ and then $x = mk + 3$ until you can solve for y.

Step 8: In practice, you will find such a y before you hit $x = mk + k - 1$. Then take the point (x, y). This now converts the number m into a point on the elliptic curve. In this way, the entire message becomes a sequence of points.

Decoding:

Consider each point (x, y) and set m to be the greatest integer less than $(x - 1)/k$. Then the point (x, y) decodes as the symbol m.

APPENDIX B
NIST RECOMMENDED ELLIPTIC CURVES

In the FIPS 186-2 standard, NIST recommended 15 elliptic curves of varying security levels for U.S. federal government use [9]. The curves are of three types:

1. Random Elliptic Curves Over a Prime Field F_p.
2. Random Elliptic Curves Over a Binary Field F_{2^m}.
3. Koblitz Elliptic Curves Over a Binary Field F_{2^m}.

B.1. Random Elliptic Curves Over F_p

Table B.1 lists domain parameters for the five NIST-recommended randomly chosen elliptic curves over prime fields F_p. The primes p were specially chosen to allow for very fast reduction of integers modulo p. The selection $a = -3$ for the coefficient In the elliptic curve equation was made so that elliptic curve points represented In Jacobian projective coordinates could be added using one fewer field multiplication [31,32,33]. The following parameters are given for each curve:

P The order of the prime field F_p.
S The seed selected to randomly generate the coefficients of the elliptic Curve
r The output of SHA-1.
a, b The coefficients of the elliptic curve $y^2 = x^3 + ax + b$ satisfying $rb^2 \equiv a^3 (mod\, p)$.
n The (prime) order of the base point P.
h the cofactor.
x, y the x and y coordinates of P.

Table B.1. NIST-Recommended Random Elliptic Curves over Prime Fields [9].

P-192: $p = 2^{192} - 2^{64} - 1$, $a = -3$, $h = 1$	
S = 0x	3045AE6F C8422F64 ED579528 D38120EA E12196D5
r = 0x	3099D2BB BFCB2538 542DCD5F B078B6EF 5F3D6FE2 C745DE65
b = 0x	64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1
n = 0x	FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
x = 0x	188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
y = 0x	07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811
P-224: $p = 2^{224} - 2^{96} + 1$, $a = -3$, $h = 1$	
S = 0x	BD713447 99D5C7FC DC45B59F A3B9AB8F 6A948BC5
r = 0x	5B056C7E 11DD68F4 0469EE7F 3C7A7D74 F7D12111 6506D031 218291FB
b = 0x	B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4
n = 0x	FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D
x = 0x	B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6 115C1D21
y = 0x	BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199 85007E34
P-256: $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, $a = -3$, $h = 1$	
S = 0x	C49D3608 86E70493 6A6678E1 139D26B7 819F7E90
r = 0x	7EFBA166 2985BE94 03CB055C 75D4F7E0 CE8D84A9 C5114ABC AF317768 0104FA0D
b = 0x	5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
n = 0x	FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
x = 0x	6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
y = 0x	4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5
P-384: $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$, $a =-3$, $h = 1$	
S = 0x	A335926A A319A27A 1D00896A 6773A482 7ACDAC73
r = 0x	79D1E655 F868F02F FF48DCDE E14151DD B80643C1 406D0CA1 0DFE6FC5 2009540A 495E8042 EA5F744F 6E184667 CC722483
b = 0x	B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A C656398D 8A2ED19D 2A85C8ED D3EC2AEF
n = 0x	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973
x = 0x	AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7
y = 0x	3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0 0A60B1CE 1D7E819D 7A431D7C 90EA0E5F
P-521: $p = 2^{521} - 1$, $a = -3$, $h = 1$	
S = 0x	D09E8800 291CB853 96CC6717 393284AA A0DA64BA
r = 0x	000000B4 8BFA5F42 0A349495 39D2BDFC 264EEEEB 077688E4 4FBF0AD8 F6D0EDB3 7BD6B533 28100051 8E19F1B9 FFBE0FE9 ED8A3C22 00B8F875 E523868C 70C1E5BF 55BAD637
b = 0x	00000051 953EB961 8E1C9A1F 929A21A0 B68540EE A2DA725B 99B315F3 B8B48991 8EF109E1 56193951 EC7E937B 1652C0BD 3BB1BF07 3573DF88 3D2C34F1 EF451FD4 6B503F00
n = 0x	000001FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFA 51868783 BF2F966B 7FCC0148 F709A5D0 3BB5C9B8 899C47AE BB6FB71E 91386409
x = 0x	000000C6 858E06B7 0404E9CD 9E3ECB66 2395B442 9C648139 053FB521 F828AF60 6B4D3DBA A14B5E77 EFE75928 FE1DC127 A2FFA8DE 3348B3C1 856A429B F97E7E31 C2E5BD66
y = 0x	00000118 39296A78 9A3BC004 5C8A5FB4 2C7D1BD9 98F54449 579B4468 17AFBD17 273E662C 97EE7299 5EF42640 C550B901 3FAD0761 353C7086 A272C240 88BE9476 9FD16650

B.2. Random Elliptic Curves Over F_{2^m}

Table B.2 lists domain parameters for the five NIST-recommended randomly chosen elliptic curves over binary fields F_{2^m} . The extension degrees m are prime and were selected so that there exists a Koblitz curve over F_{2^m} having almost-prime group order [31,32,33]. The following parameters are given for each curve:

m The extension degree of the binary field F_{2^m}.
$f\ (z)$ The reduction polynomial of degree m.
s The seed selected to randomly generate the coefficients of the elliptic curve.
a, b The coefficients of the elliptic curve $y^2 + xy = x^3 + ax^2 + b$.
n The (prime) order of the base point P.
h The cofactor.
x, y The x and y coordinates of P.

B.3. Koblitz Elliptic Curves Over F_{2^m}

Table B.3 lists domain parameters for the five NIST-recommended Koblitz curves over binary fields, the binary fields F_{2^m} are the same as for the random curves. Koblitz curves were selected because point multiplication can be performed faster than for the random curves [18,19]. The following parameters are given for each curve:

m The extension degree of the binary field 2^m.
$f\ (z)$ The reduction polynomial of degree m.
a, b The coefficients of the elliptic curve $y^2 + xy = x^3 + ax^2 + b$.
n The (prime) order of the base point P.
h The cofactor.
x, y The x and y coordinates of P.

Table B.2. NIST-Recommended Random Elliptic Curves Over Binary Fields [9].

B-163: $m = 163$, $f(z) = z^{163} + z^{7} + z^{6} + z^{3} + 1$, $a = 1$, $h = 2$	
S = 0x	85E25BFE 5C86226C DB12016F 7553F9D0 E693A268
b = 0x	00000002 0A601907 B8C953CA 1481EB10 512F7874 4A3205FD
n = 0x	00000004 00000000 00000000 000292FE 77E70C12 A4234C33
x = 0x	00000003 F0EBA162 86A2D57E A0991168 D4994637 E8343E36
y = 0x	00000000 D51FBC6C 71A0094F A2CDD545 B11C5C0C 797324F1
B-233: $m = 233$, $f(z) = z^{233} + z^{74} + 1$, $a = 1$, $h = 2$	
S = 0x	74D59FF0 7F6B413D 0EA14B34 4B20A2DB 049B50C3
b = 0x	00000066 647EDE6C 332C7F8C 0923BB58 213B333B 20E9CE42 81FE115F 7D8F90AD
n = 0x	00000100 00000000 00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7
x = 0x	000000FA C9DFCBAC 8313BB21 39F1BB75 5FEF65BC 391F8B36 F8F8EB73 71FD558B
y = 0x	00000100 6A08A419 03350678 E58528BE BF8A0BEF F867A7CA 36716F7E 01F81052
B-283: $m = 283$, $f(z) = z^{283} + z^{12} + z^{7} + z^{5} + 1$, $a = 1$, $h = 2$	
S = 0x	77E2B073 70EB0F83 2A6DD5B6 2DFC88CD 06BB84BE
b = 0x	027B680A C8B8596D A5A4AF8A 19A0303F CA97FD76 45309FA2 A581485A F6263E31 3B79A2F5
n = 0x	03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFEF90 399660FC 938A9016 5B042A7C EFADB307
x = 0x	05F93925 8DB7DD90 E1934F8C 70B0DFEC 2EED25B8 557EAC9C 80E2E198 F8CDBECD 86B12053
y = 0x	03676854 FE24141C B98FE6D4 B20D02B4 516FF702 350EDDB0 826779C8 13F0DF45 BE8112F4
B-409: $m = 409$, $f(z) = z^{409} + z^{87} + 1$, $a = 1$, $h = 2$	
S = 0x	4099B5A4 57F9D69F 79213D09 4C4BCD4D 4262210B
b = 0x	0021A5C2 C8EE9FEB 5C4B9A75 3B7B476B 7FD6422E F1F3DD67 4761FA99 D6AC27C8 A9A197B2 72822F6C D57A55AA 4F50AE31 7B13545F
n = 0x	01000000 00000000 00000000 00000000 00000000 00000000 000001E2 AAD6A612 F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173
x = 0x	015D4860 D088DDB3 496B0C60 64756260 441CDE4A F1771D4D B01FFE5B 34E59703 DC255A86 8A118051 5603AEAB 60794E54 BB7996A7
y = 0x	0061B1CF AB6BE5F3 2BBFA783 24ED106A 7636B9C5 A7BD198D 0158AA4F 5488D08F 38514F1F DF4B4F40 D2181B36 81C364BA 0273C706
B-571: $m = 571$, $f(z) = z^{571} + z^{10} + z^{5} + z^{2} + 1$, $a = 1, h = 2$	
S = 0x	2aa058f7 3a0e33ab 486b0f61 0410c53a 7f132310
b = 0x	02F40E7E 2221F295 DE297117 B7F3D62F 5C6A97FF CB8CEFF1 CD6BA8CE 4A9A18AD 84FFABBD 8EFA5933 2BE7AD67 56A66E29 4AFD185A 78FF12AA 520E4DE7 39BACA0C 7FFEFF7F 2955727A
n = 0x	03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF E661CE18 FF559873 08059B18 6823851E C7DD9CA1 161DE93D 5174D66E 8382E9BB 2FE84E47
x = 0x	0303001D 34B85629 6C16C0D4 0D3CD775 0A93D1D2 955FA80A A5F40FC8 DB7B2ABD BDE53950 F4C0D293 CDD711A3 5B67FB14 99AE6003 8614F139 4ABFA3B4 C850D927 E1E7769C 8EEC2D19
y = 0x	037BF273 42DA639B 6DCCFFFE B73D69D7 8C6C27A6 009CBBCA 1980F853 3921E8A6 84423E43 BAB08A57 6291AF8F 461BB2A8 B3531D2F 0485C19B 16E2F151 6E23DD3C 1A4827AF 1B8AC15B

Table B.3. NIST-Recommended Koblitz Curves Over Binary Fields [9].

K-163: $m = 163$, $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$, $a = 1$, $b = 1$, $h = 2$	
$n =$	0x 00000004 00000000 00000000 00020108 A2E0CC0D 99F8A5EF
$x =$	0x 00000002 FE13C053 7BBC11AC AA07D793 DE4E6D5E 5C94EEE8
$y =$	0x 00000002 89070FB0 5D38FF58 321F2E80 0536D538 CCDAA3D9
K-233: $m = 233$, $f(z) = z^{233} + z^{74} + 1$, $a = 0$, $b = 1$, $h = 4$	
$n =$	0x 00000080 00000000 00000000 00000000 00069D5B B915BCD4 6EFB1AD5 F173ABDF
$x =$	0x 00000172 32BA853A 7E731AF1 29F22FF4 149563A4 19C26BF5 0A4C9D6E EFAD6126
$y =$	0x 000001DB 537DECE8 19B7F70F 555A67C4 27A8CD9B F18AEB9B 56E0C110 56FAE6A3
K-283: $m = 283$, $f(z) = z^{283} + z^{12} + z^7 + z^5 + 1$, $a = 0$, $b = 1$, $h = 4$	
$n =$	0x 01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFE9AE 2ED07577 265DFF7F 94451E061E163C61
$x =$	0x 0503213F 78CA4488 3F1A3B81 62F188E5 53CD265F 23C1567A 16876913 B0C2AC24 58492836
$y =$	0x 01CCDA38 0F1C9E31 8D90F95D 07E5426F E87E45C0 E8184698 E4596236 4E341161 77DD2259
K-409: $m = 409$, $f(z) = z^{409} + z^{87} + 1$, $a = 0$, $b = 1$, $h = 4$	
$n =$	0x 007FFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFE5F 83B2D4EA 20400EC4 557D5ED3 E3E7CA5B 4B5C83B8 E01E5FCF
$x =$	0x 0060F05F 658F49C1 AD3AB189 0F718421 0EFD0987 E307C84C 27ACCFB8 F9F67CC2 C460189E B5AAAA62 EE222EB1 B35540CF E9023746
$y =$	0x 01E36905 0B7C4E42 ACBA1DAC BF04299C 3460782F 918EA427 E6325165 E9EA10E3 DA5F6C42 E9C55215 AA9CA27A 5863EC48 D8E0286B
K-571: $m = 571$, $f(z) = z^{571} + z^{10} + z^5 + z^2 + 1$, $a = 0$, $b = 1$, $h = 4$	
$n =$	0x 02000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 131850E1 F19A63E4 B391A8DB 917F4138 B630D84B E5D63938 1E91DEB4 5CFE778F 637C1001
$x =$	0x 026EB7A8 59923FBC 82189631 F8103FE4 AC9CA297 0012D5D4 60248048 01841CA4 43709584 93B205E6 47DA304D B4CEB08C BBD1BA39 494776FB 988B4717 4DCA88C7 E2945283 A01C8972
$y =$	0x 0349DC80 7F4FBF37 4F4AEADE 3BCA9531 4DD58CEC 9F307A54 FFC61EFC 006D8A2C 9D4979C0 AC44AEA7 4FBEBBB9 F772AEDC B620B01A 7BA7AF1B 320430C8 591984F6 01CD4C14 3EF1C7A3

ملخص الرسالة

نظراً للتطور الكبير في وسائل الإتصالات وخاصة شبكات الحاسب الآلي واستخدامها للربط بين الأفراد والشركات في جميع أنحاء العالم لنقل البيانات بكافة أشكالها (فيديو – صوت – بيانات) وبإختلاف أهميتها وخاصة في عمليات التجارة الإلكترونية ونقل الحسابات البنكية وغيرها من الأمور، مما يتطلب وجود طرق أكثر أماناً لنقل هذه البيانات عبر شبكات الحاسب الآلي وشبكة الإنترنت مع الحفاظ على سلامتها وسريتها وخاصة مع تطور أساليب المخترقين. ولذلك تم استخدام خوارزمات وتقنيات كثيرة لتشفير البيانات المرسلة لضمان سريتها وصحتها ومن بين هذه التقنيات، تقنية حماية برتوكول شبكة الإنترنت والتي تستخدم منذ بضع سنوات وهي تتضمن مجموعة من البروتوكولات المختلفة التي تستخدم لتشفير وتوثيق البيانات أثناء إنتقالها بين نقطتين عبر شبكات الحاسب الآلي .

ويتضمن موضوع الرسالة دراسة تفصيلية لحماية شبكات الحاسب الآلي ودراسة برتوكول حماية شبكة الإنترنت المستخدم وتطبيقه عملياً وكذلك دراسة تفصيلية لنظم التشفير وتوثيق البيانات باستخدام المفتاح العام ودراسة بعض الخوارزمات التي استحدثت بعد ذلك ومن أهمهم خوارزم التوقيع التشفيري الذي يقوم بعملية تشفير وتوثيق البيانات في خطوة واحدة وبتكلفة أقل من الطريقة التقليدية وهي توثيق الرسالة ثم تشفيرها، وأيضاً دراسته في حالة ارسال رسالة إلى أكثر من فرد.

ونقدم خوارزم جديد باستخدام المنحنيات الناقصة حيث يعمل على توثيق وتشفير البيانات بتكلفة أقل تتمثل في استخدام حيز موجي أقل يصل إلى ٥٠% مقارنة بالطريقة التقيلية مع تحقيق جميع الخواص الأمنية المطلوبة وبسرية اكبر من الخوارزمات السابقة حيث يقوم باستخدام مفتاح تشفير يعتمد علي قيمة عشوائية بالإضافة إلى المفتاح الخاص بالمرسل وأيضاً يمكن من خلاله التأكد من توثيق البيانات دون الحاجة إلى المفتاح الخاص بالمرسل إليه الرسالة أي دون الحاجة إلى فك الرسالة ويمكن الاستفادة من ذلك في عمل برامج حماية الشبكات حيث يمكنه من تمرير البيانات من أفراد معينة دون الحاجة إلى فك الرسالة.

وقد تم مقارنة الخوارزم الجديد بالخوارزمات السابقة وتطبيقه في حالة ارسال رسالة إلى أكثر من فرد وكيفية إدخاله على تقنية حماية برتوكول شبكة الإنترنت لتقليل الحيز الموجي المستخدم وزيادة سرية وأمان البيانات أثناء انتقالها عبر شبكات الحاسب الألي.

وتتكون الرسالة من ستة أبواب بيانهم كالأتي :

- <u>الباب الأول</u> : يضم هذا الباب تعريف لحماية البيانات علي شبكات الحاسب الآلي وشرح مفصل لتقنية حماية برتوكول شبكة الإنترنت وأهميتها والبروتوكولات التي تتكون منها وكيفية استخدامها في تشفير وتوثيق البيانات أثناء انتقالها عبر شبكات الحاسب الآلي .

- <u>الباب الثاني</u> : يضم الباب الثاني ملخص للأساسيات الرياضية والنظريات المتعلقة بنظم التشفيروهي مقدمة في نظرية الأرقام وتتضمن تعريف الأعداد الأولية والمقسومات ونظرية فيرمات و نظرية آويلر ودالة آويلر وهم الأكثر استخداما في حسابات نظم التشفير بالإضافة إلى شرح للمنحنيات الناقصة والعمليات الحسابية الخاصة بها .

- <u>الباب الثالث</u> : يضم الباب الثالث شرح لنظم التشفير الغير متماثلة وعلاقتها بنظرية الأرقام وكيفية استخدامها في تشفير وتوثيق البيانات والمقارنة بينهم ومن أهم نظم التشفير الغير متماثلة التشقير باستخدام المنحنيات الناقصة. ويضم أيضا شرح للخوارزمات التي استحدثت بعد ذلك ومن أهمها خوارزم التوقيع التشفيري و تطبيقه في حالة ارسال الرسالة إلى أكثر من فرد .

- الباب الرابع : يقدم الباب الرابع شرح لخوارزم جديد باستخدام المنحنيات الناقصة حيث يعمل على توثيق البيات وتشفيرها معا بتكلفة أقل تصل إلى ٥٠% وتحقيق درجة أمان عالية. وكيفية حساب التكلفة ومقارنة الخوارزم الجديد بالخوارزمات السابقة.

- الباب الخامس : يعرض الباب الخامس كيفية تطبيق الخوارزم الجديد في حالة إرسال الرسالة إلى أكثر من فرد وكيفية إدخاله على تقنية حماية برتوكول شبكة الإنترنت.

- الباب السادس : يضم الباب السادس توضيح لما ورد في الرسالة وعرض موجز للخوارزم الجديد وكيفية تطبيقه في المستقبل على تقنية حماية برتوكول شبكة الإنترنت في حماية البيانات أثناء انتقالها خلال شبكات الحاسب الآلي .

تأمين إتصالات شبكات الحاسب الآلي

رسالة علمية

مقدمة إلى الدراسات العليا بكلية الهندسة – جامعه الأسكندرية
إستيفاء للدراسات المقررة للحصول على درجة

ماجستير العلوم

فى

الهندسة الكهربية

مقدمة من

المهندس / محمد حسن محمد حسن العتيقي

٢٠١٤

تأمين إتصالات شبكات الحاسب الآلي

مقدمة من

المهندس / محمد حسن محمد حسن العتيقي

للحصول على درجة

ماجستير العلوم

في

الهندسة الكهربية

لجنة المناقشة والحكم على الرسالة موافقون

أ.د. حسن محمد الكمشوشي ....

أ.د. محمد السعيد نصر ....

أ.د. نور الدين حسن اسماعيل ....

وكيل الكلية للدراسات العليا والبحوث
كلية الهندسة – جامعة الاسكندرية

أ.د. هبه وائل لهيطه

لجنة الاشراف

أ.د. حسن محمد الكمشوشي ....

د. محمد محمود علي ....