

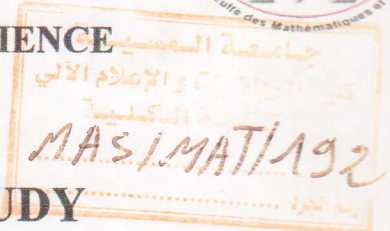
POPULAR AND DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH



UNIVERSITY MOHAMED BOUDIAF - M'SILA
FACULTY OF MATHEMATICS AND
COMPUTER SCIENCE



DEPARTMENT OF COMPUTER SCIENCE



MEMORY OF END OF STUDY

Presented for the obtention of MASTER Degree

Domaine: Mathematics and Computer Science

Branch: Computer Science

Spéciality: Advanced Information Systems.

By: GUESMIA Seyf Eddine

TOPIC

**Design and Realization of Multimedia Data Encryption
System**

Publicly defended: / /2016 before a Jury composed of:

Last and first Name of teachers

Pro. BOUDERAH Brahim

Université de M'sila

Supervisor

Dr. ASSAS Ouarda

Université de M'sila

Supervisor

.....

Université de M'sila

Chair

.....

Université de M'sila

Examiner

.....

Université de M'sila

Examiner

Promotion : 2015 /2016

List of contents

Thanks	--
List of Figures	--
List of Tables	--
General Introduction	01

CHAPTER I: Introduction to Cryptography

1. Introduction	04
2. Security Properties	04
2.1. Authentication	04
2.2. Non-Repudiation	04
2.3. Confidentiality	05
2.4. Integrity	05
3. Cryptology	05
4. Cryptography	06
4.1. Symmetric Key Encryption	06
4.1.1. Principle	06
4.1.2. Small taxonomy of classic symmetric encryption	07
4.1.2.1. Caesar cipher	07
4.1.2.2. Vigenere cipher	07
4.1.3. Substitution and transposition (or confusion and diffusion)	08
4.1.4. Modern and powerful techniques	08

08	4.1.4.1. DES (Data Encryption Standard)
09	4.1.4.2. Triple DES
10	4.1.4.3. AES (Advanced Encryption Standard)
11	4.2. Public Key Encryption
11	4.3. Key security
11	4.3.1. Key Distribution
12	4.3.1.1. Case of Symmetric Key Encryption
12	4.3.1.2. Case of Public Key Encryption
12	4.3.2. Key Exchange
12	4.3.2.1. Diffie-Hellman protocol
13	4.3.2.2. Quantum key Distribution
14	4.4. Difference between Symmetric Key and Public Key Encryption
15	4.5. Complexity of cryptographic algorithms
15	4.6. Encryption modes
15	4.6.1. Block cipher mode
15	4.6.1.1. Electronic Code Book (ECB) mode
16	4.6.1.2. Cipher Block Chain (CBC) mode
17	4.6.1.3. Cipher Feedback (CFB) mode
18	4.6.1.4. Output Feedback (OFB) mode
18	4.6.1.5. Counter (CTR) mode
19	4.6.2. Stream cipher mode
19	4.7. Hash function
20	4.8. Digital signature

5. Cryptanalysis	21
5.1. Ciphertext only attacks (COA)	21
5.2. Known plaintext attacks (KPA)	21
5.3. Chosen plaintext attacks (CPA)	21
5.4. Chosen ciphertext attacks (CCA)	21
5.5. Man-in-the-middle attacks (MITMA)	21
5.6. Side Channel Attacks (SCA)	22
5.7. Brute Force Attacks (BFA)	22
6. Conclusion	23

CHAPTER II: AES Cipher

1. Introduction	25
2. Mathematical preliminaries	25
2.1. Addition	25
2.2. Multiplication	26
2.3. Polynomials with coefficients in $GF(2^8)$	27
3. AES Algorithm Using 512 Bit Key (specification)	29
3.1. Cipher	29
3.1.1. SubBytes()	30
3.1.2. ShiftRows()	31
3.1.3. MixColumns()	32
3.1.4. AddRoundKey()	32
3.2. Inverse cipher	33

42	1. Introduction
42	2. The proposed algorithm
42	2.1. The Encryption Algorithm (E)
43	2.1.1. General Schemes of the encryption algorithm
44	2.1.2. Overview of the operation
44	2.1.3. The encryption algorithm transformations
44	2.1.3.1. Bytes substitution
45	2.1.3.2. SH-Z transformation

CHAPTER III: High Lightweight Encryption Standard (HLES)

33	3.2.1. InvSubBytes()
34	3.2.2. InvShiftRows()
34	3.2.3. InvMixColumns()
34	3.2.4. Inverse of AddRoundKey()
35	4. Key management
35	4.1. Key length requirements
35	4.2. Key expansion and rounds
37	5. Advantages and disadvantages of 512-bits AES
37	6. Complexity analysis
38	7. Experiences and results (memory space and encryption time)
39	8. Explanatory example
40	9. Conclusion

2.1.3.3. Key-Xor and L-Xor transformations	48
--	----

2.2. Decryption algorithm (D)	48
-------------------------------------	----

2.2.1. Overview of the operation	48
--	----

2.2.2. Details of the decryption algorithm	49
--	----

2.2.2.1. Inverse of S-Box	49
---------------------------------	----

2.2.2.2. Inverse of SH-Z	50
--------------------------------	----

2.2.2.3. Inverse of Key-Xor and L-Xor transformations	50
---	----

2.3. Sub key generator	50
------------------------------	----

2.4. Complexity of the algorithm	52
--	----

2.5. Analysis of Security of the method	52
---	----

2.6. Analysis of performance of the algorithm	53
---	----

3. Conclusion	54
---------------------	----

CHAPTER IV: Implementation & Experimental Results

1. Introduction	56
-----------------------	----

2. Environment of development	56
-------------------------------------	----

2.1. Operating system	56
-----------------------------	----

2.2. Programming language	56
---------------------------------	----

2.3. Programming tool, platform, and environment	57
--	----

3. Architecture of the application	57
--	----

3.1. GUE (Graphical User Interface)	57
---	----

3.2. The principal classes	58
----------------------------------	----

4. Tests and experimental results	64
---	----

4.1. Criteria of the encryption time	64
--	----

64	4.1.1. Tests and results
69	4.1.2. The encryption evolution vis-a-vis the file size
70	4.2. Evolution of the memory space
71	4.3. Study of the method security
72	5. Conclusion
73	General Conclusion.....

General Introduction

In today's scenario, people share information to another people frequently using network. Due to this, more amount of information are so much private but some are less private. Therefore, the attackers (or the hackers) take the advantage and start attempting to steal the information since 2001. the symmetric encryption algorithm called 512-bit AES that was designed in 2011 provides high level of security, but it's almost be impossible to be used in multimedia transmissions and mobile systems because of the need for more design area that effect in the use of memory space in each round and the Encryption / Decryption time that it takes.

This work presents an improvement of 512-bit AES algorithm with efficient utilization of resources such as processor and memory space. The proposed approach resists a different encryption analysis and attacks, and provides high security level using a 512-bit size of key block and data block and ameliorates the performance by minimizing the use of memory space and Encryption / Decryption time to be able to work in specific characteristics of resource-limited systems.

The first chapter discuss in detail the technical and applicative aspects of cryptology with its two branches: cryptography and cryptanalysis.

The second chapter is devoted to Mathematical preliminaries required in encryption and decryption methods, and a detailed study of a new variation of the original 128-bit AES algorithm called 512 bit AES that was appeared to provide more security.

The third chapter talks about the proposed algorithm that is given as an alternative to the one that called "512-bit AES" for improving the performance level, explaining its transformations methods including the general architecture and key expansion.

In the fourth chapter, we talk about the environment of the implementation that we have done to make the comparison between algorithms, and the tests that we have done including the results that prove the amelioration of the performance level.

Finally, we conclude the work with a general thought about HLES algorithm as a general conclusion.

General Conclusion

Over the past 2,500 years, cryptography has developed numerous types of systems to hide messages and subsequently a rich vocabulary in which to describe them. The focus of this work was stationed in the field of Symmetric Key Encryption. The improved AES algorithm that use 512 bit of key and data block provides high level of security, because of the use of a key size larger than the original 128-bit AES key. However, it has a deficiency in performance, the encryption process become heavy when it comes to the modern communicating world that depends on the resource-limited systems and real-time operations. The main objective of this work was designing an alternative algorithm that keeps the level of security that the 512-bit AES provides, and minimizes the cost of memory space used and encryption time that it takes.

We started our work with a general introduction that speak about security of the transmission over the internet in general.

The first chapter talks about the technical and applicative aspects of cryptology with its two branches: cryptography and cryptanalysis.

In the second chapter, we talk about Mathematical preliminaries required in encryption and decryption methods, and a detailed study of a new variation of the original 128-bit AES algorithm called 512 bit AES that was appeared to provide more security.

The third chapter explain in detail the proposed algorithm that is given as an alternative to the one that called "512-bit AES" for improving the performance level, explaining its transformations methods including the general architecture and key expansion.

The fourth chapter talks about the environment of the implementation that we have done to make the comparison between algorithms, and the tests that we have done including the results that prove the amelioration of the performance level.

The experimental results on several data (text, image, sound, video) show that the used memory space is reduced to quarter, and the encryption time is reduced almost to the half. Therefore, the adopted method is very effective for encryption of multimedia data.

Bibliography:

- [1] Web site: Guide to Cryptography, The free and open software security community, https://www.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Functions. Consulted in 15 June 2016.
- [2] Web site: Network Associates International, « Introduction à la cryptographie, Gatwickstraat 25 NL-1043 GL Amsterdam » <http://www.nai.com>. Consulted in 15 June 2016.
- [3] Web site: Microsoft Research, Cryptography Research, <http://research.microsoft.com/en-us/groups/crypto/>. Consulted in 15 June 2016.
- [4] Web site: « Difference between symmetric key encryption and public key encryption », <http://www.differencebetween.com/difference-between-symmetric-key-encryption-and-vs-public-key-encryption/>. Consulted in 15 June 2016.
- [5] Web Site: Maplesoft, « Caesar Cipher », <http://www.maplesoft.com/support/help/Maple/view.aspx?path=MathApps/CaesarCipher>. Consulted in 15 June 2016.
- [6] Web Site: Crypto Museum, <http://www.cryptomuseum.com/crypto/vigenere/>. Consulted in 15 June 2016.
- [7] Web Site: « Understanding Cryptography in Modern Military Communications », <http://www.idga.org/communications-engineering-and-it/articles/understanding-cryptography-in-modern-military-comm/>. Consulted in 10 July 2016.
- [8] Web Site: Wolfram MathWorld, « Diffie-Hellman Protocol », <http://mathworld.wolfram.com/Diffie-HellmanProtocol.html>. Consulted in 10 July 2016.
- [9] Web Site: ECRIM NEWS Online Edition, « Hight speed Quantum Key Distribution and Beyond », <http://ercim-news.ercim.eu/en85/special/high-speed-quantum-key-distribution-and-beyond>. Consulted in 10 July 2016.
- [10] Web Site: Atmel, Bits & Pieces, « Symmetric VS. Asymmetric Encryption: Which Way is Better? » <http://blog.atmel.com/2013/03/11/symmetric-vs-asymmetric-encryption-which-way-is-better/>. Consulted in 10 July 2016.
- [11] Jacques Stem, Louis Grandboulan, Phong Nguyen, David Pointcheval « Conception et preuves d'algorithmes cryptographiques » Edition 2004. Consulted in 10 July 2016.
- [12] Web Site: eHow, David Dunning, « What Is the Difference Between Stream Ciphers & Block Ciphers? » http://www.ehow.com/info_12040172_difference-between-stream-ciphers-block-ciphers.html. Consulted in 10 July 2016.

[13] Web Site: CRYPTO-IT, http://www.crypto-it.net/eng/theory/modes_of_block_ciphers.html. Consulted in 8 August 2016.

[14] Web Site: Entrust Datacard, « Securing Digital Identities & Information », <https://www.entrust.com/digital-signatures/>. Consulted in 8 August 2016.

[15] Web Site Experts Exchange, Giovanni Heward, « Cryptanalysis and Attacks », <http://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html>. Consulted in 8 août 2016.

[16] Web Site: Computer Hope, Free computer help and information, <http://www.computerhope.com/jargon/m/mitma.htm>. Consulted in 8 août 2016.

[17] François-Xavier Standaert, « Introduction to Side-Channel Attacks'' Chapter 2 ».

[18] « Announcing the ADVANCED ENCRYPTION STANDARD (AES) » Federal Information Processing Standards Publication 197, November 26, 2001.

[19] R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, M. Sanap « AES Algorithm Using 512 Bit Key Implementation for Secure Communication » International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE), March 2014, Rahuri Factory, India, pp 3516-3522.

[20] D.J. E. Gounmudi, F. Hachouf, « Modified confusion-diffusion based satellite image cipher using chaotic standard » logistic and sine maps, 2nd European Workshop on Visual Information Processing (EUVIP), 2010, 5-6 July 2010, Paris, France, pp: 204-209.

[21] J. J. Tay, M. M. Wong, I. Hijazin, « Compact and Low Power AES Block Cipher Using Lightweight Key Expansion Mechanism and Optimal Number of S-Boxes » IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2014, 1-4 December 2014, Kuching, Malaysia, pp: 108-114.

[22] D. R Grandh, V. Kamalakannan, R. Balamurugan, S. Tamiliselvan, « FPGA Implementation of Enhanced Key Expansion Algorithm for Advanced Encryption Standard » International Conference on Contemporary Computing and Informatics (IC3I), 2014, 27-29 November 2014, Mysore, India, pp: 409-413.

[23] D. Chen, D. Qing, D. Wang, « AES Key Expansion Algorithm Based on 2D Logistic Mapping » 5th International Workshop on Chaos-fractals Theories and Applications (IWCF TA), 2012, 18-21 October 2012, Dalian, China, pp: 207-211.

ملخص :

علم التشفير هو واحد من أكثر العلوم التي لا غنى عنها في ضمان سرية المعلومات المتبادلة. هذا العلم يختص بإنشاء ودراسة الخوارزميات التي تؤمن نقل المعلومات عبر الإنترنت. ظهرت خوارزمية جديدة في عام 2011، على غرار خوارزمية AES 128-bit الأصلية، توفر المزيد من الأمن من خلال تعزيز الموثوقية ضد هجوم البحث الشامل في مفتاح التشفير. لكنها لا تستطيع التعامل مع حمل معالجة التشفير الثقيل مع وجود النظم الحديثة ذات الموارد المحدودة. يعرض عملنا تصميم محسن لخوارزمية AES 512-bit يوفر مستوى أمان عالي ويرفع من الأداء عن طريق التقليل من استخدام مساحة الذاكرة المستعملة و الوقت المستغرق في التشفير من أجل القدرة على العمل في خصائص محددة للأنظمة ذات الموارد المحدودة.

الكلمات المفتاحية: علم التشفير، سرية المعلومات المتبادلة، الأنظمة ذات الموارد المحدودة.

Abstract:

The Cryptology is the most indispensable science used in the guarantee of the confidentiality of the exchanged information. It consist of creating and studying algorithms that secure the transmission over the internet. A new algorithm appeared in 2011, similar to the original AES algorithm, provides more security by enhancing the reliability against the brute force attack. However, it cannot handle the heavy encryption-processing load with the existence of the modern resource-limited systems. Our work presents an improvement design of 512-bit AES algorithm that provides high security level and ameliorates the performance by minimizing the use of memory space and time encryption to be able to work in specific characteristics of resource-limited systems.

Keywords: Cryptography, Confidentiality, resource-limited systems.

Résumé :

La cryptologie est la science la plus indispensable utilisé dans la garantie de la confidentialité des informations échangées. Il consiste à créer et étudier des algorithmes qui sécurisent la transmission sur Internet. Un nouvel algorithme est apparu en 2011, similaire à l'algorithme AES original, fournit plus de sécurité en améliorant la fiabilité contre l'attaque de la recherche exhaustive. Cependant, il ne peut pas gérer la lourde charge du processus de chiffrement avec l'existence des systèmes de ressources limitées modernes. Notre travail présente une amélioration de l'algorithme 512-bits AES qui fournit haut niveau de sécurité et améliore les performances en réduisant l'utilisation de l'espace mémoire et le temps de chiffrement pour être en mesure de travailler dans les caractéristiques spécifiques des systèmes de ressources limitées.

Mots clé : Cryptographie, Confidentialité, Systèmes de ressources limités.