Proposal for Complex AES Security using Key Generator and Text Permutation

Shatha Habeeb
Computer Science Department, University of Technology/ Baghdad
Email: shathahabeeb@yahoo.com

Received on: 31/5 /2011 & Accepted on: 5/4/2012

ABSTRACT

Advanced Encryption Standard (AES) is a symmetric-key encryption each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key[1,2].

This research proposes a technique intended to make the Advanced Encryption Standard (AES) more safe and secure. Through the generation of random key, and permutation key sites in each round, instead of the process of expanding key locations in addition to the proposed permutation the plaintext before entering the encryption and inverse permutation for resulting ciphertext.

Keywords: AES, symmetric ,key, encryption , ciphertext.

تعضيد أمنية (AES) باستخدام التوليد العشوائي للمفتاح ومتعددة النص

الخلاصة

معيار التشفير المتقدم (AES) هو تشفير المفتاح المتماثل كل من هذه الشفرات لديها حجم كتلة 128 بت، مع أحجام المفتاح 128 و 192 و 256 بت يتم تحديد الشفرات معيار التشفير المتقدم (AES) وتكرار عدد من الجولات مساهمة في الناتج النهائي للنص المشفر. كل جولة يتكون من عدة خطوات المعالجة، بما في ذلك تلك التي تعتمد على مفتاح التشفير.

يقدم البحث تقنية الهدف منها هو جعل معيار التشفير المتقدم (AES) أكثر آمنا ومأمونا. ذلك من خلال توليد مفتاح بطريقة عشوائية، وتبديل المواقع المفتاح في كل جولة وبدلا من عمليـــة توسيع المفتاح بالاضافة الى تبديل مواقع النص الاصلي قبل الدخول فـــي التشـــفير ومعكـــوس مصفوفة التبديل على النص المشفر.

INTRODUCTION

Advanced Encryption Standard (AES) has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum. AES operates on a 4×4 matrix of bytes, termed the *state* (versions of

https://doi.org/10.30684/etj.2012.57252
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key [3-7].

Description of the algorithm, see figure (1)

1. Key Expansion—round keys are derived from the cipher key using Rijndael key schedule
2. Initial Round
- AddRoundKey—each byte of the state is combined with the round key using bitwise xor
3. Rounds
- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey
4. Final Round (no Mix Columns)
- SubBytes
- Shift Rows
- AddRoundKey

For more explanation will present full example for AES work, see figure (2) and figure (3) [7, 8].

THE PROPOSAL SYSTEM DESIGN

In the proposed research, the aim is to strengthen (AES) algorithm. Where the proposal consists of two parts the first generation of random key. Where the user of the algorithm determines the length of the key 128-bit and all four bits number is hexadecimal or 32 number hexadecimal, and so if the length of the key 192-bit or 256-bit is equivalent to 48 or 62, No. hexadecimal, and then do permutation positions the key using a matrix consisting of 32 No. hexadecimal dimensions (4 X 8), represent the key length if 128-bit . Repeated a number of permutation rounds if the number of bits of a 128-bit repeated 10 times in each round so that the key to this allowance for the expansion of the key .

The other part includes the process of permutation or switching positions on the original text so that the matrix of either 128-bit dimensions are (8x16) or converted to hexadecimal system and its dimensions are (4 x 8) and then enter the encryption operations in the future be the same operations with the inverse matrix permutation. see figure (5)

DESCRIPTION OF THE PROPOSAL ALGORITHM

1. Key generation and permutation —round keys are derived from the cipher key using Rijndael's key schedule
2. plain text permutation
3. Initial Round
- AddRoundKey—each byte of the state is combined with the round key using bitwise xor
4. Rounds
- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey
5. Final Round (no Mix Columns)
- SubBytes
- Shift Rows
- AddRoundKey

THE IMPLEMENTATION OF THE PROPOSAL SYSTEM

The implementation of the proposal done by using javascript run the implementation and vb6 to Description of Work Map the operations as mentioned in previous sections, the proposal aim to strength the AES algorithm in figure (6) consists of five functions, first function to choose a key length 128, 192 or 256-bit and then move to the second function to generate a key the third function is to convert the key generator to hexadecimal Fourth function is the work of the key permutation and permutation to the text of the original entrance Then complete the operations as the encryption algorithm AES, But on the other side the same for the key generation process with the use of inverse permutation key and cipher text .

In figure (6) implementation function to choose a key length 128, 192 or 256-bit to generator.

In figure (7) implementation to key generation by used randomize and convert to hexadecimal.

In figure (8) implementation initial array permutation key and plaintext.

In figure (9) implementation array of inverse initial permutation key and cipher text**.**

In figure (10) the full implementation of the proposal through the application of an example of generating a random key number and convert the hexadecimal system and permutation the key and the original text and then enter the other operations in the algorithm (AES)

CONCLUSIONS

By studying the AES algorithms and analysis it is work, this research present some modification on it. By implementing the proposed modified AES there is some point concluded these are:

1. The encryption of AES has some thing danger, that it is an algorithm depend on symmetric key, so if the key is discovered that will destroy the AES security.
2. from previous point, the research propose key generation method aim to reduce the danger of symmetric keys by taking short key and from it the overall key will be generated, so this short key only will be known previously by sender and receiver.
3. AES depend on key expansion, and this expansion is static method. in this research the dependency on a proposed key generation preserve the randomness by permutation in each round.
4. AES without secure dealing with plaintext, so this research aim to enter the plaintext in the security process. That by applying initial permutations on the plaintext and finally applying the inverse permutations on resulted ciphertext.

REFERENCES

[1]- Gladman, " B. The AES Algorithm (Rijndael) in C and C++, performance of the optimized implementation," from http://fp.gladman.plus.com/cryptography_technology/rijn dael/index.htm

[2]-http://www.saylor.org/site/wp-content/uploads/2011/03/Advanced-Encryption-Standard.pdf

[3]- Satheesh Kumar, R. E.Pradeep, K.Naveen and R.Gunasekaran "A Novel Approach for Enciphering Data of Smaller Bytes" International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010 8201-1793

[4]- Venkateswaran, R. Dr. V. Sundaram, Research Scholar- Ph.D Director-Computer Applications, Karpagam Academy of Higher Education Karpagam College of Engineering , Karpagam University, Affiliated to Anna University Coimbatore, Tamilnadu, India. Coimbatore, Tamilnadu, India " Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.7, June 2010

[5}- Karthigaikumar, P. Asst.Professor (SG) Department of Electronics and Communication, Karunya University,Coimbatore , Soumiya Rasheed M.Tech Department of Electronics and Communication Karunya University,Coimbatore "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011 166

[6] Joan Daemen, "The Rijndael Block Cypher: AES Proposal", Vincent Rijmen. First AES Candidate Conference (AES1), August 1998.

[7]-http://pdfdownloads.blogspot.com/2010/10/design-of-rijndael-aes-advanced.html

[8]-http://en.wikipedia.org/wiki/ Advanced_Encryption_Standard

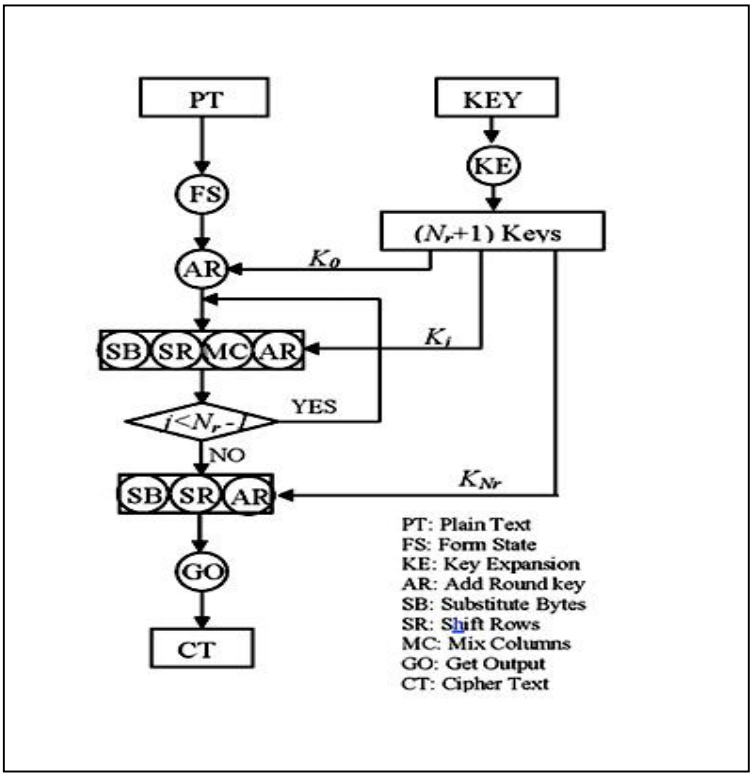

Figure (1): The flowchart of AES

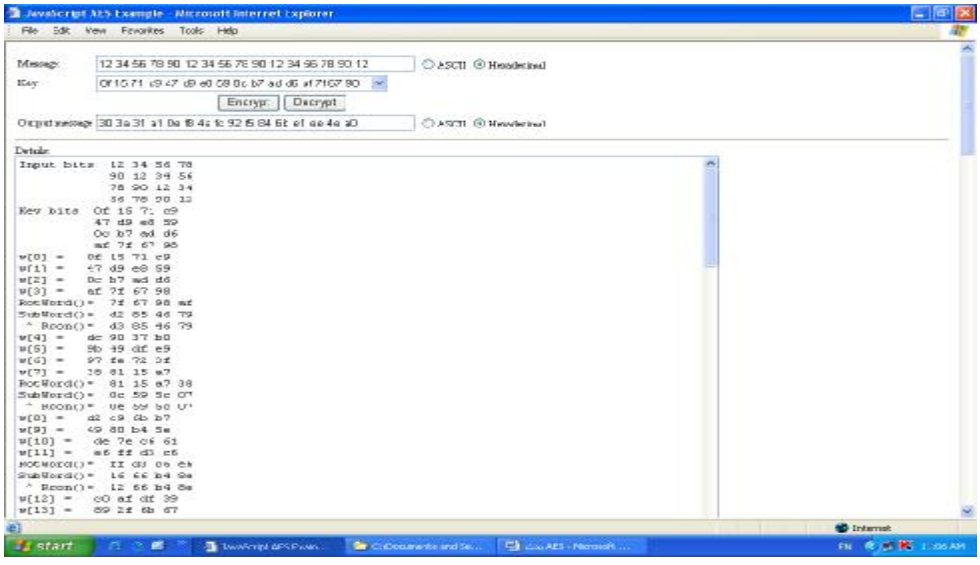

Figure (2) This form displays the overall process of AES encryption.

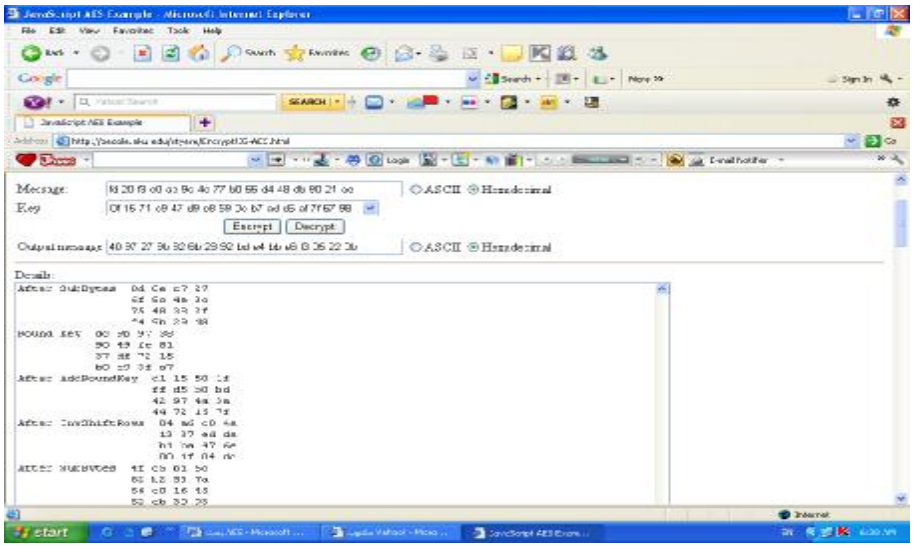

Figure (3): This form displays the overall process of AES decryption.

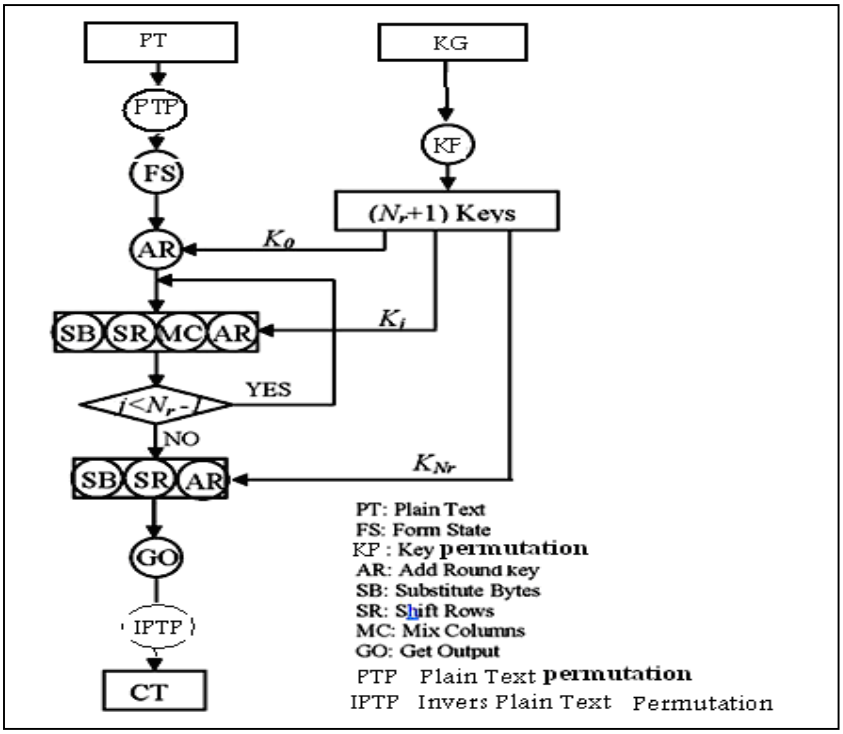

Figure (4): The flowchart of the proposed algorithm.

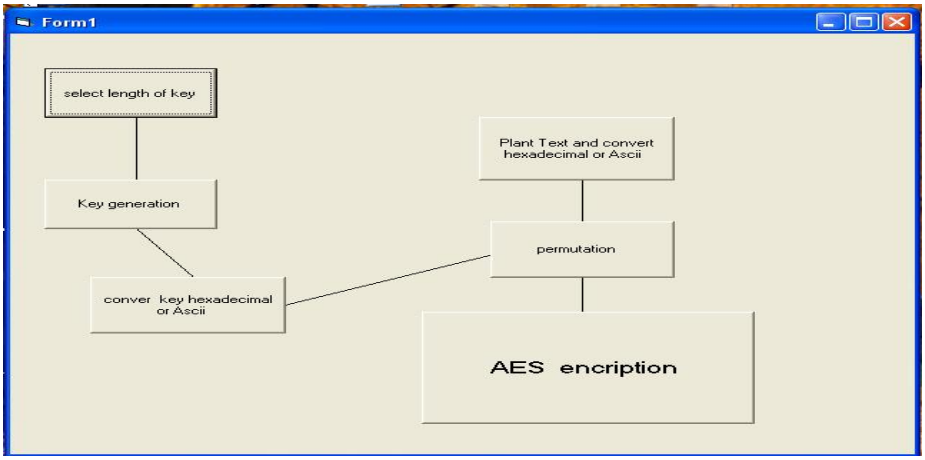

Figure (5): The implementation steps for proposed modifications on AES.

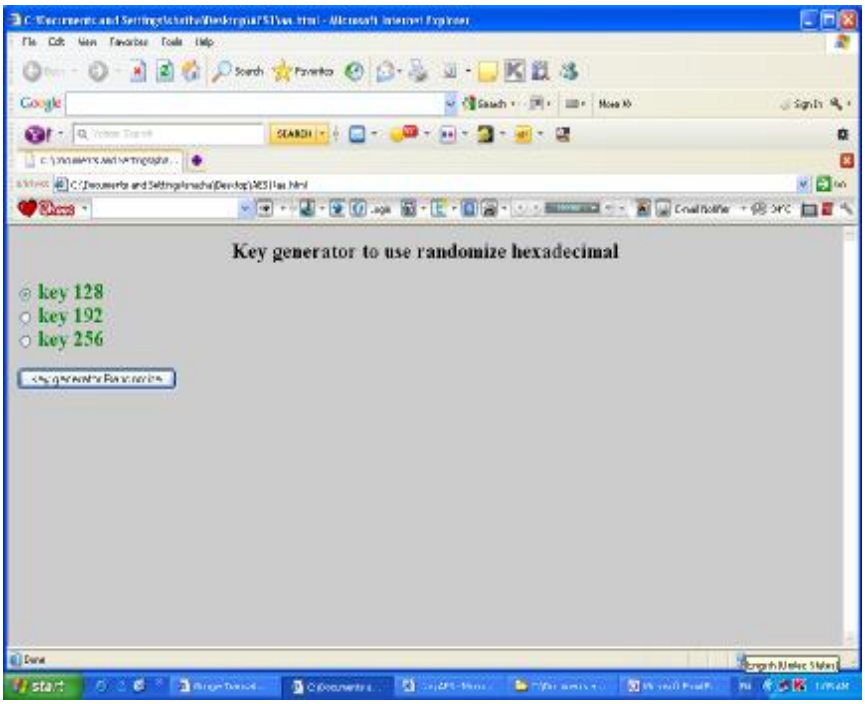

Figure (6): Form of choosing the key.

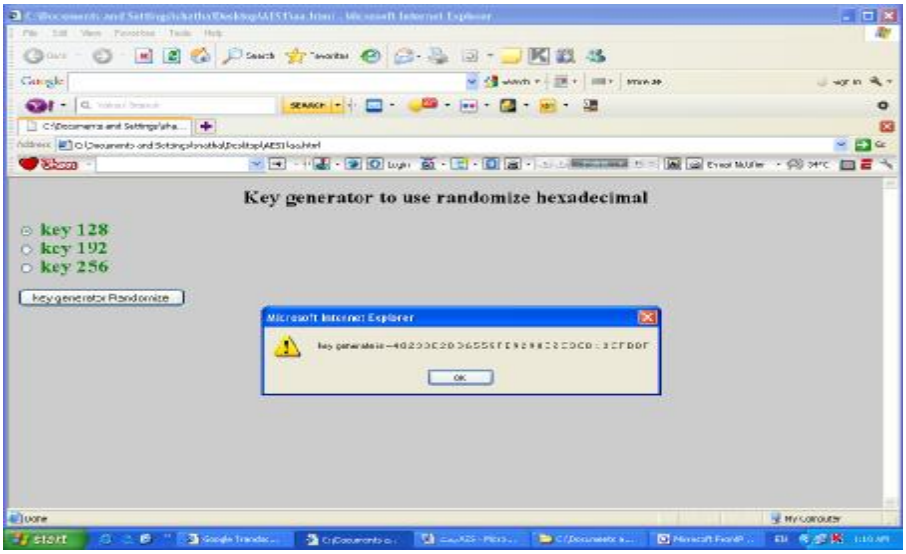

Figure (7): Form of key of generation and implementation.

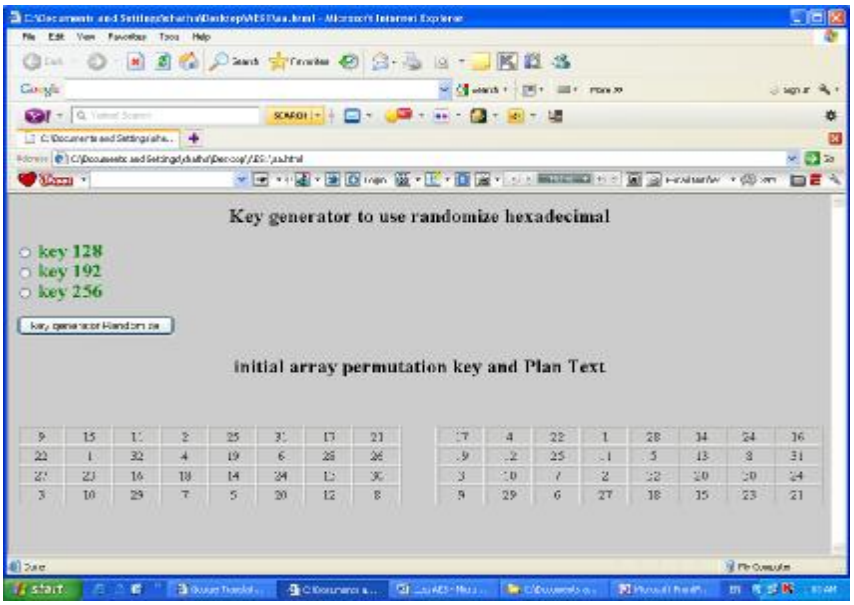

Figure (8): Form of generating initial permutation Arrays applyingon key and plaintext.

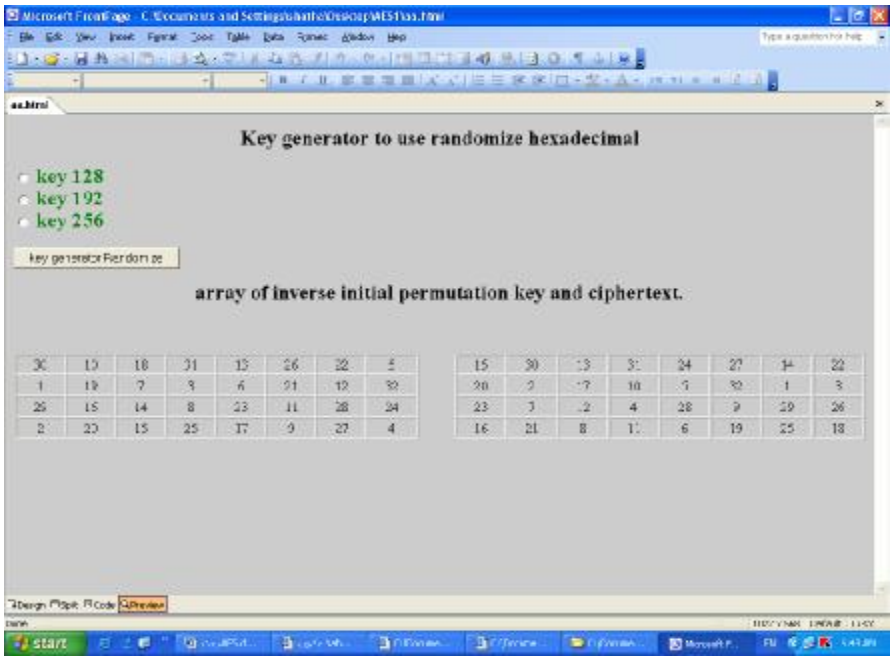

Figure (9): Form of generating initial permutation arrays applying on key and cipher text

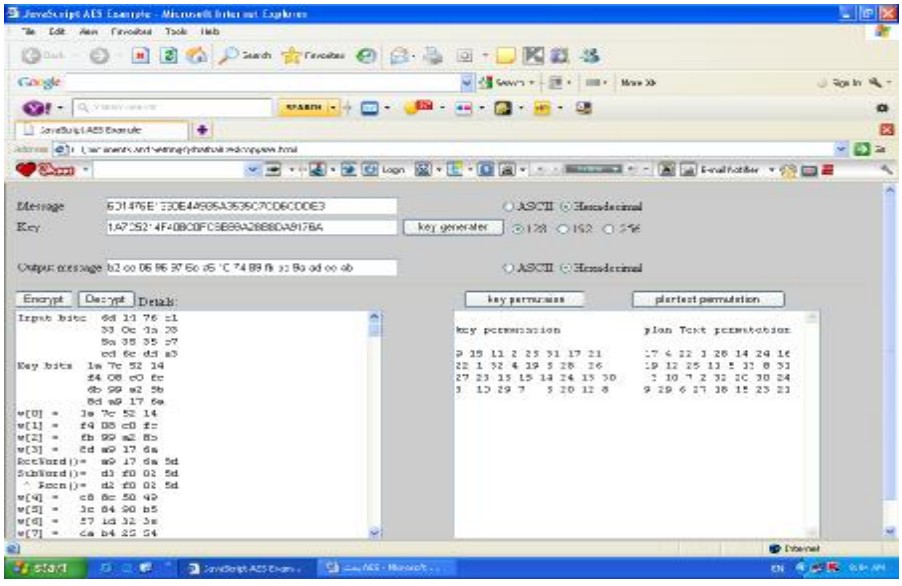

Figure (10): Form presenting all the implementation of proposed modified AES.