256 Bits Symmetric-key BLOCK CIPHER ALGORITHM

2695 –1817 –ISSN

Basim Sahar Yaseen
Computer Science, Shatt Alaraab UniversityCollege
E-mail:basim_yaseen2000@yahoo.com

((Received 24/3/2009, Accepted 14/12/2009))

ABSTRUCT :

The design and implementation operations of a cipher algorithm are considered an important in any cryptography work because it will be executed as a last stage to the study and analysis of the cipher characteristics like: weakness points and how we will remove it , strong points and how we will increase its power , and how to homogenize the algorithm parts(outputs of parts),so, the paper suggests that a cipher algorithm combines strong features in the block cipher and stream cipher together .

In the present version ,the algorithm is composed of two Erasable Programmable Read Only Memories (EPROMs) which has 64 bits storage size ,eight Linear Feed back Shift Registers(LFSRs) which has lengths are: 37 stages ;33 stages 31 stages;29 stages;23 stages;19 stages;33 stages; and 37 stages ,16 bits shifted memory, and set of logic gates. Algorithm inputs are : blocks of plain text each block has 256 bits size , basic encryption/decryption key (has length 20 alphabetic characters) , secondary encryption/decryption key (has length 8 alphabetic characters) , and the specific initial state of EPROMs .

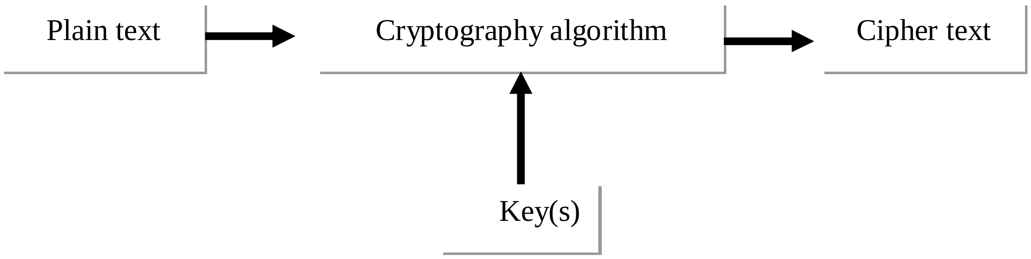
The base process In the online(stream cipher) and offline(block cipher) applications is adding the bits of input blocks with the bits of final result of the algorithm components to produce the cipher blocks in same synchronous bits. The additional process that serve the offline applications ,as soon as a block cipher, is reordering locations of bits depend on a scheme ,for all cipher text blocks.

Keywords: Stream cipher, block cipher , cryptography, designing.

1. *Introduction*

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files."**[6]**

Any cryptography system composed from the following main parts :



Where :

Plain text is the clear meaning text in a natural language .

Cryptography algorithm is set of steps to encrypt the plain text.

Cipher text is ununderstanding text that resulted from cryptography algorithm.
Key(s) are a control inputs on encryption process .

Algorithms classified as symmetric like as traditional, stream and block cipher, and asymmetric like as public key systems**.[5].** A block cipher is a function which maps n-bit plaintext blocks to n-bit cipher text blocks; n is called the *block length*. It may be viewed as a simple substitution cipher with large character size. The function is parameterized by a k-bit key K,1 taking values from a subset K (the *key space*) of the set of all k-bit vectors Vk. It is generally assumed that the key is chosen at random. Use of plaintext and cipher text blocks of equal size avoids data expansion. To allow unique decryption, the encryption function must be one-to-one (i.e., invertible).
Cryptography can be *strong* or *weak*. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of *strong cryptography* is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time—even a billion computers doing a billion checks a second—it is not possible to decipher the result of strong cryptography before the end of the universe**.[2][3][4]**

1-1 Measures of any designing cryptographic work :

(1) privacy or confidentiality
(2) data integrity
(3) authentication
(4) non-repudiation
1. *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible**.[1][2][6]**
2. *Data integrity* is a service which addresses the unauthorized alteration of data. To
assure data integrity, one must have the ability to detect data manipulation by an authorized parties. Data manipulation includes such things as insertion, deletion, and
substitution.**[1][2][6]**
3. *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin ,date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).**[1][2]**
4. *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute. A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities**.[1][2][6]**
.

1-2 Criteria for evaluating block ciphers

Many criteria may be used for evaluating block ciphers in practice, including:
1. *estimated security level*. Confidence in the (historical) security of a cipher grows if it has been subjected to and withstood expert cryptanalysis over a substantial time period,e.g., several years or more; such ciphers are certainly considered more secure than those which have not. This may include the performance of selected cipher components relative to various design criteria which have been proposed or gained favor in recent years. The amount of cipher text required to mount practical attacks often vastly exceeds a cipher's unicity distance (Definition 7.69), which provides a theoretical estimate of the amount of cipher text required to recover the unique encryption key.
2. *key size*. The effective bit length of the key, or more specifically, the entropy of the key space, defines an upper bound on the security of a cipher (by considering exhaustive search). Longer keys typically impose additional costs (e.g., generation, transmission, storage, difficulty to remember passwords).
3. *throughput*. Throughput is related to the complexity of the cryptographic mapping

and the degree to which the mapping is tailored to a particular implementation medium or platform.

4. *block size*. Block size impacts both security (larger is desirable) and complexity(larger is more costly to implement). Block size may also affect performance, for example, if padding is required.

5. *complexity of cryptographic mapping*. Algorithmic complexity affects the implementation costs both in terms of development and fixed resources (hardware gate count or software code/data size), as well as real-time performance for fixed resources(throughput). Some ciphers specifically favor hardware or software implementations.

6. *data expansion*. It is generally desirable, and often mandatory, that encryption does not increase the size of plaintext data. Homophonic substitution and randomized encryption techniques result in data expansion.

7. *error propagation*. Decryption of cipher text containing bit errors may result in various effects on the recovered plaintext, including propagation of errors to be sequent plaintext blocks. Different error characteristics are acceptable in various applications. Block size (above) typically affects error propagation**.[1][5]**

2.Algorithm structure

The main algorithm parts :

1- Two EPROMs**[5]** has size 64 bits for each one .The initial state of both will be generated randomly .Each EPROM works as like as a hash table .

2- Eight LFSRs**[5]** has lengths are :37,33,31,29,23,19,33, and 37. The initial content of this system is a mixture from two keys ,the first is the basic key and the second is the modifier or secondary key.

3- 16 bits shift memory**[5]** . The first initial for this memory will be represented by bits evaluated from secondary key, then during the work , memory content is the initial state of its plus the summation of all LFSRs outputs and it works as delay stage.

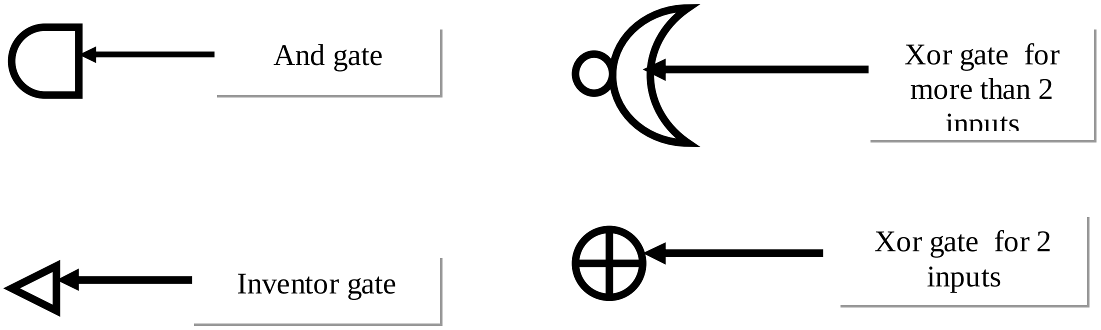
4- 6 bits address encoder**[7]** .convert the output of first six LFSRs to the decimal digit represents address in the EPROM.

5- 8 bits address encoder. convert the output of eight LFSRs to the decimal digit represents bit location in the resulted block.

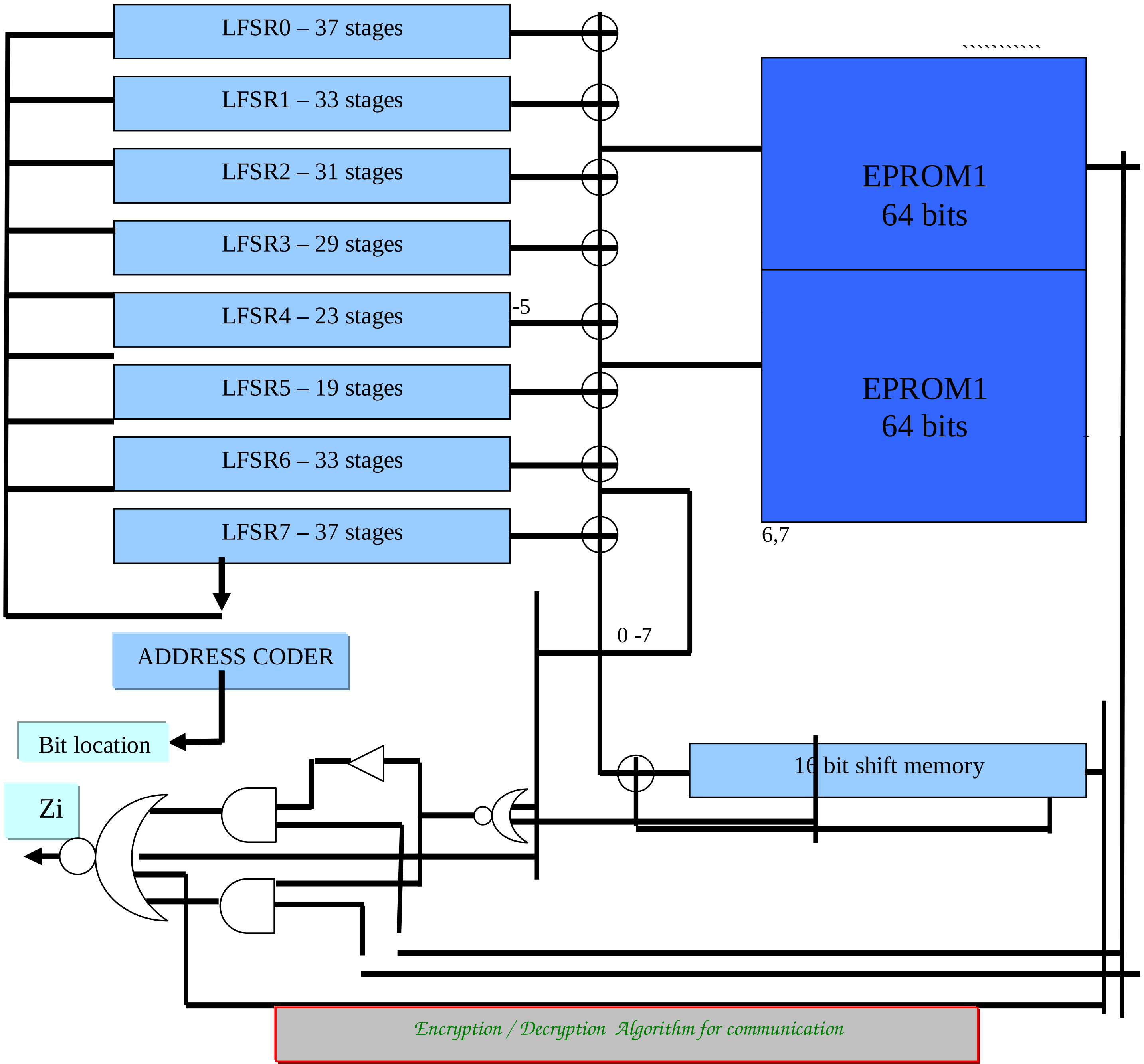
6- Set of logical gates **[7].** describe below .

7- 16 bits memory to store and delay output of LFSRs set.

The algorithm receives 256 bits of plain text and it treats with this bits individually, at each movement ,the algorithm produces key bit to add with the plain bit and address of the resulted cipher bit. The stream cipher generating part was passed successfully in all stream cipher tests like:[auto correlation test , poker test, run test, frequency test, and serial test]**[5].**



Explain of Gates symbols in the algorithm graph



Encryption / Decryption Algorithm for communication

Algorithm needs two key types :
Basic key has 20 characters length ,all them from alphabetic set.
Secondary key has 8 characters length, all them from alphabetic set.

3.The processing

3-1 Algorithm requirements :

1-128 initial bits for 2 EPROMs .
2- 20 alphabetic characters as a basic key distributes (in the bits form) on the LFSRs .
3- 8 alphabetic characters as a modifier key adds with the basic key bits in the LFSRs and initial state bits in the EPROMs .
4- addition and modifier key bits considers the initial basic inputs to the 16 shift memory .

3-2 Algorithm input : text or n blocks ,each block has 256 plain bits.

3-3 Algorithm steps:

Step1: read plain bit(i).

Step2: move the LFSRs system one movment to determine EPROMs address and cipher bit location.

Step3: compute Z(i) bit(final key bit) from stream part of algorithm.

Step4: adding by xor gate the plain bit(i) with Z(i) to produce cipher bit(i).

Step5: locate cipher bit(i) in the location that evaluated in the step 2.

Step6: repeat from step no.1 on the next plain bit (i+1).

Step7: reset the counter of block (i=1) ,and then repeat the work on the next block .

3-4 Algorithm output: n blocks ,each block has 256 cipher bits.

4-Results of Algorithm randomness tests .

Test name	Test value	The result
Auto correlation	≈ 0.50	Success
poker	≈ 16.92	Success
Frequency	≈ 3.75	Success
Run	≈ 3.5	Success
Serial	≈ 5.90	Success

5-Example

If we have the following information:

Message="SECURITY OF COMMUNICATION MEDIA00"
Coding alg=ASCII-8 (to convert the message from characters form to binary form)
Basic key=BASRAHCITYISABUTIFUL
Modifier key=COMPUTER

Then the cipher bits sequence="
0110100011101010011100001010000011100001
1101001100110100110101101001001010000110
1001100011101101111100110011000001101011
0011001100110001101111100000101110101000
0111010100011101010001110100011010100001
1011000100110011010111101010010101010010
00101010111100010"

And the real locations of these bits are:

bit 1 bit 9 bit221 bit 52 bit 70 bit172 bit 82 bit 42 bit 96 bit109 bit 21 bit122 bit 19 bit216 bit 16 bit 76 bit235 bit 95 bit199 bit 84 bit179 bit217 bit184 bit 79 bit 85 bit120 bit 64 bit212 bit 72 bit124 bit 39 bit224 bit 74 bit198 bit250 bit127 bit228 bit 6 bit 37 bit129 bit152 bit 3 bit167 bit182 bit143 bit 53 bit175 bit245 bit165 bit256 bit 63 bit174 bit 22 bit226 bit131 bit147 bit176 bit 87 bit 2 bit181 bit254 bit192 bit 51 bit234 bit201 bit151 bit222 bit177 bit 24 bit162 bit225 bit140 bit246 bit 45 bit 41 bit 69 bit 46 bit148 bit128 bit 40 bit157 bit190 bit 20 bit 28 bit204 bit207 bit 98 bit112 bit 88 bit210 bit 18 bit 50 bit173 bit 59 bit 66 bit 94 bit215 bit 81 bit169 bit178 bit232 bit123 bit197 bit142 bit186 bit106 bit139 bit153 bit 29 bit121 bit104 bit 30 bit 14 bit141 bit236 bit238 bit 71 bit180 bit189 bit170 bit243 bit 33 bit253 bit 27 bit 26 bit 5 bit 80 bit138 bit114 bit231 bit 89 bit 91 bit125 bit218 bit195 bit 47 bit237 bit229 bit 54 bit160 bit115 bit 48 bit255 bit 25 bit 60 bit183 bit113 bit251 bit 11 bit 97 bit102 bit117 bit130 bit118 bit146 bit 65 bit150 bit156 bit 93 bit200 bit193 bit247 bit 49 bit 4 bit 58 bit 83 bit196 bit248 bit 67 bit203 bit168 bit145 bit230 bit227 bit108 bit136 bit171 bit206 bit134 bit 12 bit 55 bit188 bit219 bit 13 bit126 bit249 bit 7 bit158 bit 92 bit166 bit208 bit163 bit244 bit 62 bit205 bit119 bit 44 bit202 bit223 bit111 bit 57 bit239 bit185 bit252 bit144 bit154 bit 56 bit155 bit 75 bit220 bit 10 bit 90 bit209 bit105 bit132 bit107 bit 38 bit 35 bit211 bit159 bit149 bit135 bit187 bit 77 bit103 bit 61 bit100 bit 99 bit101 bit 17 bit164 bit 31 bit241 bit 86 bit110 bit 73 bit242 bit233 bit240 bit 15 bit 36 bit 34 bit 68 bit 8 bit213 bit116 bit 23 bit 78 bit161 bit 32 bit191 bit 43 bit137 bit194 bit214 bit133

6. Discussion

Favor characteristics of the suggested algorithm can be a limit when compares with practical complexity , are chosen just for uses to explain the basic idea of the paper. So, to design and implement a cryptography stronghold depends on this idea in order to protect the secrete information from unauthorized processes. This requires the increasing in the lengths and sizes for components. We should make more clear relationships cut in way to decrease the keys dependency for the components .

The main aim behind this idea is combining strong features for the stream cipher with the block cipher technique and producing a duel algorithm technique .The present characteristics for parts gives key space around 28 power 26 ,if we don’t care the EPROMs initials as well as in some of attacks , this key space equal to 2 power 104 as an initials devices .Algorithm treated with keys has alphabetically type and binary values for some devices , and easeful of keys management .The plain texts types are all data and information in textual form ,or any data file in binary form can be encrypted by using algorithm.

7. conclusion

1- The features of stream cipher like cipher power , speed and sequencing or synchronization of the key bits are favorite in some applications .
2- Much of block cipher techniques don’t need an entered key(s) , and this state is favorite in more than application.
3- As a trail to add main features in points (1) and (2) together it will succeed in finding a new strong cipher for high level security application which is considered as a duel work algorithm (i.e. it can be stream cipher algorithm ,block cipher algorithm ,or the two types together .
4- To increase the cipher complexity and make a relationship between the resulted blocks can be done by replacing EPROM set with the plain block(s).

8-References

1."Hand book of cryptography"A.J.Menezes , P.C.VanOorschot and S.A.Vanstone ,U.S.A,1996 .

2."An introduction to cryptography ",Network Associates, Inc.and its Affiliated companies, version 6 ,1990-1998 U.S.

3."Java cryptography" ,Jonathan B.Knudsen, First edition, may 1998,U.K.

4."Algorithm and complexity" ,Herbert S.Wilf ,university of Pennsylvania , Philadelphia, ,internet edition,summer ,1994,U.S.A.

5."computer security handbook" ,national institute of standards and technology,,special publication 800-12, 2004,U.S. Department of commerce.

6. " Applied Cryptography: Protocols, Algorithms, and Source
Code in C", Bruce Schneier**,** 2006,USA

7."Elecetronic Logic and circuits" ,H.E.Shanoon, Springer house , 2007.

خوارزمية تشفير كتلية متناظرة المفتاح بحجم 256 ثنائية

باسم سهر ياسين
قسم علوم حاسبات – كلية شط العرب الجامعة الأهلية
E-mail:basim_yaseen2000@yahoo.com

المستخلص :

تعتبر عمليات تصميم وتنفيذ الخوارزميات جدا مهمة في أي عمل ضمن مجال التشفير وذلك لكونها النواتج النهائية من مراحل دراسة وتحليل موصفات أي نوع من أنواع التشفير كإيجاد نقاط الضعف وكيفية التغلب عليها , نقاط القوة وكيفية تعزيزها , وكيفية جعل مخرجات الأجزاء تتجانس لإعطاء مخرجات نهائية قوية.

أقترح في ملخص البحث خوارزمية الكترونية للتشفير تجمع مواصفات القوة للتشفير الانسيابي مع مثيلاتها في التشفير الكتلي . (وهي إحدى نقاط تميز هذه الخوارزمية عن مثيلاتها في الأعمال المماثلة) .

في النسخة الحالية فأن حجم البيانات التي يتم التعامل معها هي 256 ثنائية من ثنائيات النص الواضح ,وبالتالي فان عدد ثنائيات المفتاح النهائية التي تجمع مع ثنائيات النص الواضح المبعثرة من الخوارزمية سيكون أيضا 256 ثنائية , وتتكون من : ذاكرتي EPROM (ذاكرة قراءة فقط قابلة للمسح والبرمجة) كل منها بحجم 64 ثنائية ,منظومة من مسجلات الإزاحة الخطية مهمتها تحديد عنوان لثنائية من الذواكر أعلاه وتحديد عنوان نهائي لترتيب الثنائية المشفرة , ذاكرة زاحفة بحجم 16 ثنائية , ومجموعة من البوابات المنطقية التي تربط الأجزاء المختلفة للخوارزمية.

للخوارزمية المقترحة مفتاحان رئيسيان الأول بطول 20حرف أبجدي تملى بها منظومة المسجلات ,بالإضافة إلى مفتاح بحجم 8 أحرف يستخدم لتصحيح محتويات المسجلات بعد إملائها بالمفتاح الأول , الجزء الثالث هو محتويات متغيرة بصورة دورية لذواكر EPROMs بقدر 128 ثنائية . تعمل الخوارزمية بواسطة قراءة النص الواضح إما بشكل ثنائيات او ككتلة متكونة من 256 ثنائية ,تجمع كل ثنائية مع ثنائية ناتجة من تجمع لأجزاء الخوارزمية وتعطى الثنائية النهائية موقع يحدد بواسطة الأجزاء المتخصصة لتحديد العنوان.

الهدف من البحث هو اقتراح فكرة أولية لنوع جديد من خوارزميات تشفير تخدم تطبيقات المعلومات عالية السرية وهذه الفكرة قابلة للتطوير بتعديل المواصفات وإصدار نسخ أخرى متقدمة.

الكلمات المفتاحية :التشفير الانسيابي , التشفير الكتلي , علم التشفير ,التصميم.