Applying Quran Security and Hamming Codes For Preventing of Text Modification

*Mokhtar M. Hassan** *Ahmed A. Abdul Redha**

Received 5, October, 2009
Accepted 20, June, 2010

Abstract:

The widespread of internet allover the world, in addition to the increasing of the huge number of users that they exchanged important information over it highlights the need for a new methods to protect these important information from intruders' corruption or modification.

This paper suggests a new method that ensures that the texts of a given document cannot be modified by the intruders.

This method mainly consists of mixture of three steps. The first step which barrows some concepts of "Quran" security system to detect some type of change(s) occur in a given text. Where a key of each paragraph in the text is extracted from a group of letters in that paragraph which occur as multiply of a given prime number. This step cannot detect the changes in the reordering letters or words of the paragraph and text without changing the letters themselves. So, the next step uses one of the error detection methods which is named Hamming Codes to find out the locations of the change in the received text. After that; at the third step, RSA as a primary encryption method has been used to encrypt the keys extracted to the first step and second step in order to prevent the intruders to break down the security of the method.

Key words: Security systems, Hamming Codes, Error detection and correction, Encryption algorithms, public key encryption, RSA Encryption Algorithm.

Introduction:

The Quran security system depends on a given key number which is the prime number 19. This number represents the total letters of the starting phrase of Quran subparts which is called "Sora" in Arabic. the Quran which is the holly book of Muslims divided into parts , each part divided by turn into subparts called "Sora" , each "Sora" has name and consists of a set of phrases or sentences , each "Sora" started with the same phrase which is called "Al Basmala" and written in Arabic as this " بسم الله الرحمن الرحيم" . the meaning of phrase is "By The Name Of God The Mercy And Mercyful". Each phrase of any "Sora" called "Aaia" which means GOD Sign. The Quran Security System aim to prevent holly text of Quran from any modification by adding, deleting, and changing not only words of holly text but also every letters of text. This preventing occurs through tying the whole text with the number 19 (the number of letters of "Al Basmala" sign). The security system associates the Arabic letters of this phrase (without repetitions) with Arabic text of whole Quran (the language of holly Quran is Arabic) through this number. The main concept of the system is that each letter of "Al Basmala" occur in whole text as multiply of 19, the number of all letters consist of the whole text are multiple

*Computer Science Dept. – College of Science for Women- Baghdad University

of 19, also the number of subparts , "Sora" (s), are multiple of 19, the number of phrases (signs) or in Arabic ("Aaia"s) in whole Quran are multiple of 19. in addition there are some subparts ("Sora"s) started with set of letters which is called prefixes letters , these letters act as security key for these subparts("Sora"s) (i.e. subparts started with the same prefix) ,so that each letter of these prefixes (keys) occurred multiple of 19 in these subparts together [1]. This security system is an additional miracle to the forever miracle of Quran if we know that the subparts and "Aaia"s of Quran distributed over 23 years the duration of prophet Mohammed after he became the messenger of GOD , and the time of deceleration of subparts and ("Aaia"s or signs) depend on some events associated with the time of declaration.

In this research we will make use of some concepts of the Quran security system and hybrid it with hamming code to build no modifiable text documents system and then after, RSA algorithm will be used.

Proposed System: Introduction

The growth of computer networks and digital communication systems in the 1980's led to establish the internet (the global international network). The wide spread of the internet and its applications over years led to a huge amount of information and documents of different types to be transferred over the net for several purposes every time. These huge number of documents transferred via the internet have different types like commercial, political, or security documents, etc. This curious hackers and intruders to hack these documents to corrupt or modify them. This highlighted the need for developing new methods of document security to prevent intruders from corrupting or modifying the important information documents exchanged across the global network.

In this paper we suggest a new method to prevent text document from any modification. The method is hybrid between some concepts of Quran security system and security methods.

The suggested method consists of two steps , the first step is to build the reference table which is consist of a list of paragraphs key calculated from each paragraph in the document. The paragraph key consists of set of letters in the paragraph that their frequencies in the paragraph dividable by specific selected prime number as mentioned before.

This key indicates that the modification in the text of the associated paragraph either intended or accidentally was occurred unless it maintains the above relation between the key and associated text.

The second step is to compute the hamming code for each paragraph of the document in the reference table and then use this code to detect if there is any change of any letter in the paragraph that are not belongs to the key; all extracted information will be registered in the reference table.

Later, the reference table will be encrypted using RSA algorithm that uses public key scheme to ensure that this useful extracted information stays secure.

The system doesn’t work on the paragraph level only, but also it works on the whole text file level (i.e level 0 of text file structure) where the system generate file key in addition to the paragraphs keys.

Standard Security Algorithms:

As mentioned before, the proposed system uses hamming code and RSA algorithm in addition to Quran security method, in the next sections, a brief of these security algorithms will be discussed.

The purpose of the first step of the proposed system discussed above is to ensure that the occurrence of some selected letters (the paragraph key letters) in the text for each paragraph are not changed, but this does not ensure that the positions of these letters are not changed. So, to ensure that the letters positions are not changed one of the error detection and correction methods is used. This method is Hamming Codes.

In the second step, the proposed system generates the hamming code bits for each paragraph in the text file and registers this code to the reference table entry associated with each paragraph.

Any paragraph has a unique sequence of binary sequence, and if any change in the paragraph happens, the sequence of binary stream will be different. So, since hamming code operates on binary input, any change in the paragraph sequence will lead to change in binary stream , and consequently, it will be detected by hamming code algorithm[2].

1. Hamming Code

This algorithm works on a binary representation of a given input data, and tries to form some redundancy bits that work as an eye for any text change, so, if any intruder tries to change any bit in the original text, the hamming codes will be different when reevaluated and text modification will be discovered[3][4].

1.1 Hamming Code Algorithm [5][6]

Get the input text

Convert the input text into binary representation

Form a long stream of binary locations numbered from 1 to the end of input binary

Fill all locations except 2^x with the input binary bits respectively.

Calculate the 2^x bits using XOR methods with some selected binary bits

The locations of 2^x is the output redundancy bits

2 .Public Key Encryption: RSA Method [7]

After applying Quran security and Hamming code and producing a reference table, the receiver needs that reference table to check the validity of received text file. So, for more protection RSA, as a public key cryptography method, is used to cipher the reference table before send it to the receiver to prevent the intruder from corrupting or modifying the information on it.

Public-key cryptography is a cryptographic approach, employed by many cryptographic algorithms and cryptosystems, whose distinguishing characteristic is the use of asymmetric key algorithms which means that the key used to encrypt a message is not the same as the key used to decrypt. The keys are related mathematically, but the private key cannot be feasibly (ie, in actual or projected practice) derived from the public key. Figure 1 shows the keys generation for RSA algorithm that is written according to some standards [8], figure 2 shows the encryption and decryption of the message using the generated keys[9][10].

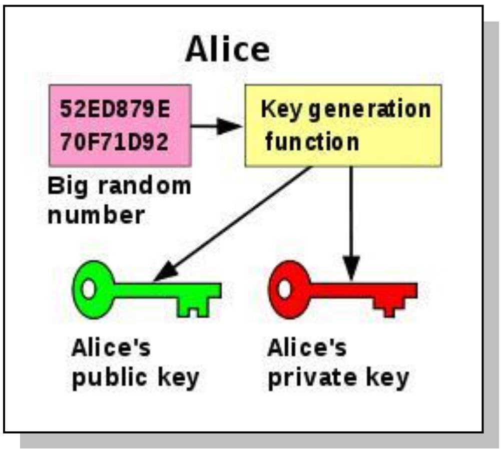


Fig. 1: keys generation

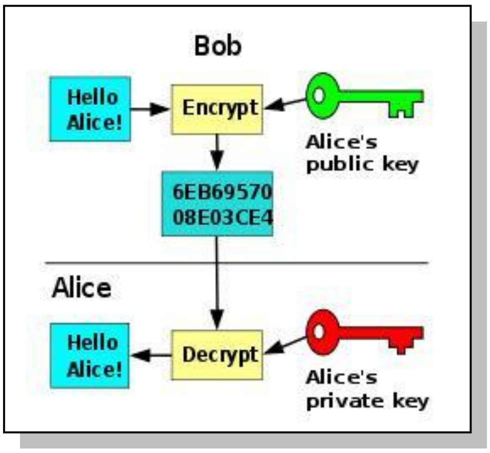


Fig. 2: encryption and decryption

2.1 RSA algorithm [11][12]

- Selecting two large primes at random (~100 digit), p, q
- Computing their system modulus N=p.q
- Selecting at random the encryption key e, where e<N, gcd(e,ø(N))=1
- Solving the following congruence to find the decryption key d:

e.d≡1 mod ø(N) and 0<=d<=N

- Making public their public encryption key: Kr={er,Nr}
- Keeping secret their private decryption key: K^{-1}r={d,p,q}

System Description

In the following pages, the proposed system application will be discussed to understand the system clearly.

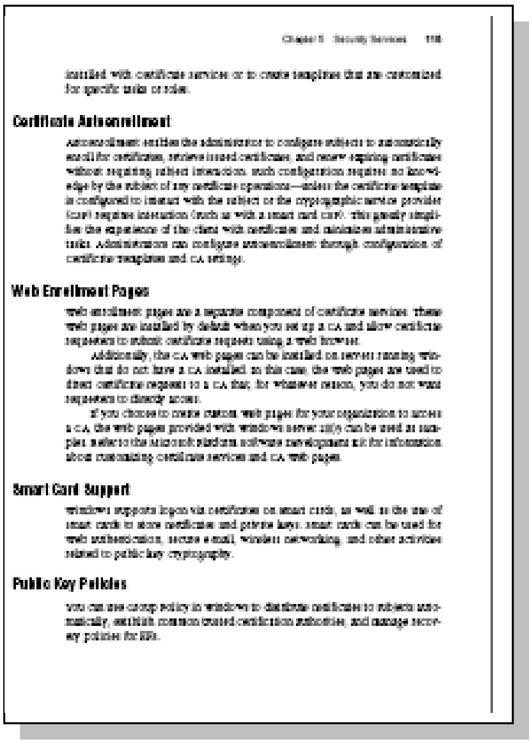
The proposed system consists of three stages named as:
First Stage: local extracted information
Second Stage: global extracted information
Stage Three: reference table encryption
So, the following sections illustrated the above points independently, and after that an example is taken to show the operation of this proposed scheme.

1. Local Extracted Information

This stage tries to extract information from one paragraph and store it in the reference table, these extracted information can be divided into two sections:

1.1 Local Key

This local key represents the information taken from each paragraph of input text independently. Assume that the input text is broken down into a number of paragraphs, as shown in figure 3, and each paragraph consists of many lines of words of characters in turn.



Chapter 5 Security Services 118

installed with certificate services or to create templates that are customized for specific tasks or roles.

Certificate Autoenrollment

Autoenrollment enables the administrator to configure subjects to automatically enroll for certificates, retrieve issued certificates, and renew expiring certificates without requiring subject interaction. Such configuration requires no knowledge by the subject of any certificate operations—unless the certificate template is configured to interact with the subject or the cryptographic service provider (CSP) requires interaction (such as with a smart card CSP). This greatly simplifies the experience of the client with certificates and minimizes administrative tasks. Administrators can configure autoenrollment through configuration of certificate templates and CA settings.

Web Enrollment Pages

Web enrollment pages are a separate component of certificate services. These web pages are installed by default when you set up a CA and allow certificate requesters to submit certificate requests using a web browser.

Additionally, the CA web pages can be installed on servers running Windows that do not have a CA installed. In this case, the web pages are used to direct certificate requests to a CA that, for whatever reason, you do not want requesters to directly access.

If you choose to create custom web pages for your organization to access a CA, the web pages provided with Windows Server 2003 can be used as samples. Refer to the Microsoft Platform Software Development Kit for information about customizing certificate services and CA web pages.

Smart Card Support

Windows supports logon via certificates on smart cards, as well as the use of smart cards to store certificates and private keys. Smart cards can be used for web authentication, secure e-mail, wireless networking, and other activities related to public key cryptography.

Public Key Policies

You can use Group Policy in Windows to distribute certificates to subjects automatically, establish common trusted certification authorities, and manage recovery policies for EFS.

Fig. 3: Page Layout

The local extracted features operates on one paragraph in a time and produces a key for each one paragraph, this key is computed from the number of occurrence of each letter in this paragraph, so, the paragraph is broken down into the original composed letters and find out the occurrences of each letter, and after that; these occurrences are divided by selected primary numbers starting from 3 up to 29, the reason of selecting these numbers will be discussed later, the next step is to divide the occurrences of letters by the primary numbers and get maximum number of letters that is satisfy the condition which is dividable by primary numbers without remainder. These letters are used as the key for that paragraph.

It is obvious that as increasing the primary number value as reducing the number of dividable letters, so by experience 29 is good enough as maximum primary number, table 1 illustrates the relation between the number of letters in case of increasing the primary number value for different paragraph samples.

Table 1: Primary Numbers and Their Letter Frequencies

Sample Number	Primary Number Value	Number of Letters
1	3	4
1	5	2
1	7	4
1	11	3
1	13	1
1	17	1
1	19	2
1	23	1
1	29	1
2	3	8
2	5	4
2	7	2
2	11	3
2	13	1
2	17	1
2	19	1
2	23	0
2	29	0

Figure 4 and Figure 5 illustrate the relations between increasing the primary numbers and the decreasing the number of letters (the key length).

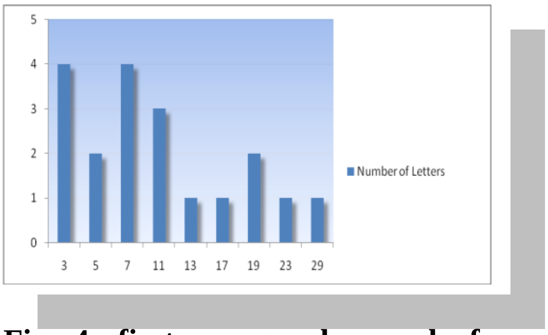


Fig. 4: first paragraph sample for key length

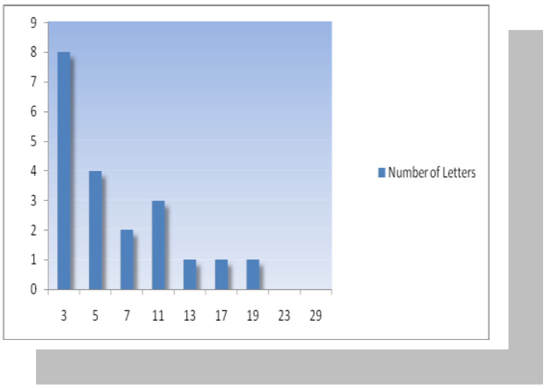


Fig. 5: second paragraph sample for key length

As notices in the above figures, as the increasing the primary number value, the key length (the letters equal to the maximum number of letter in the paragraph) is decreased.

Practically, the primary number 3 is chosen to be used in the proposed system because this number produces maximum key length and this is the reasons of choosing lower primary number, off course the number 1 (one) cannot be chosen as the lowest in spite o the fact that it is primary because in the division process every number divided by 1 will stay the same.

1.2 Local Bits

After extracting the local key from the given paragraph, now it is the time for extracting local bits from the same paragraph, these bits are extracted using Hamming Code method because it is the best method for finding the shortest bits extracted from the paragraph and this method does not used for encryption, for example, if the paragraph was 80 words with 10 characters each, so the total letters will be 10*80=800 letters, the total number of bits are:

800 * 8 = 6400 bits

So, in hamming code, the redundant bits required are : 12 bits

Because 6400 are the next number after 4096 (212).

Now, the extracted information is composed of two components which are:

Local Key and the Local Bits

2. Global Extracted Information

After extracting the local information for each paragraph independently and storing them in a reference table, now it is the time for extracting the global information from the whole text.

In this case, the paragraphs that composed the input text are merged together to form one big paragraph, i.e. using the whole input text without separation into paragraphs, in the same manner of extracting the local information is used again to extract the global information, so, if the input text consists of 10 paragraphs, then the total extracted information is 10 information for each paragraph and one additional information for the whole text, the sum will be eleven extracted information will be saved in the reference table, notice that each one information is composed of two components as discussed before, the local key and the local bits, and in the case of global extracted information, this consists of the global key and the global bits.

3. Reference Table Encryption

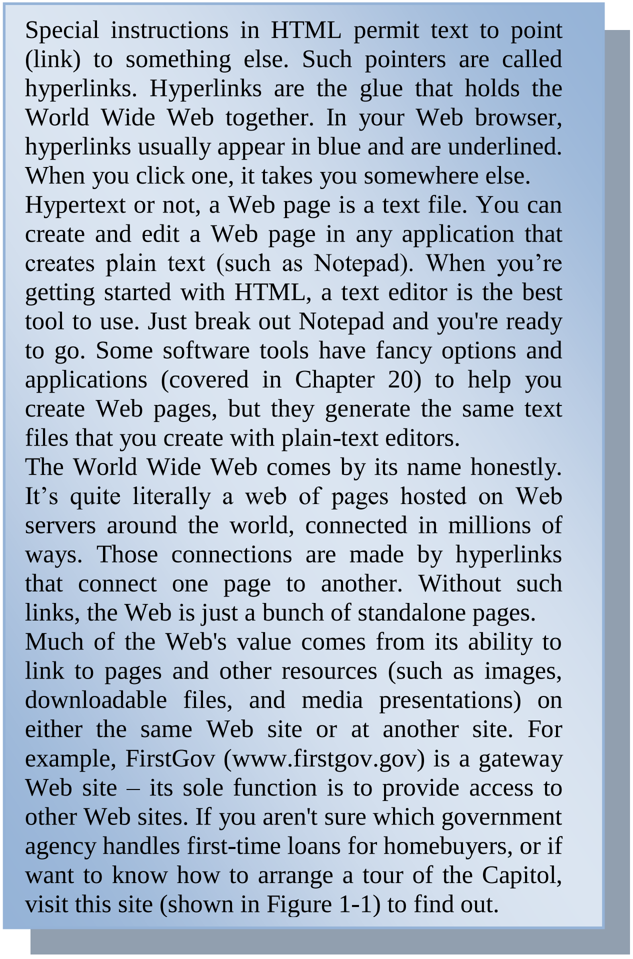
After collecting all the information from the input text, the final step is to encryption the reference table using RSA algorithm so no can see read the information inside the reference table.

The receiver produces the keys for RSA algorithm and sends the public key for the sender and holds the private key to him, the sender in turn uses that public key to encipher the reference table and send the results to the receiver, the receiver and after receiving the encrypted reference table; he decrypts it and use it for checking the received text if any change happened to it.

The following section illustrated an example of the proposed system.

Experimental Example:

Consider that the following input text with four paragraphs:



Special instructions in HTML permit text to point (link) to something else. Such pointers are called hyperlinks. Hyperlinks are the glue that holds the World Wide Web together. In your Web browser, hyperlinks usually appear in blue and are underlined. When you click one, it takes you somewhere else.

Hypertext or not, a Web page is a text file. You can create and edit a Web page in any application that creates plain text (such as Notepad). When you’re getting started with HTML, a text editor is the best tool to use. Just break out Notepad and you're ready to go. Some software tools have fancy options and applications (covered in Chapter 20) to help you create Web pages, but they generate the same text files that you create with plain-text editors.

The World Wide Web comes by its name honestly. It’s quite literally a web of pages hosted on Web servers around the world, connected in millions of ways. Those connections are made by hyperlinks that connect one page to another. Without such links, the Web is just a bunch of standalone pages.

Much of the Web's value comes from its ability to link to pages and other resources (such as images, downloadable files, and media presentations) on either the same Web site or at another site. For example, FirstGov (www.firstgov.gov) is a gateway Web site – its sole function is to provide access to other Web sites. If you aren't sure which government agency handles first-time loans for homebuyers, or if want to know how to arrange a tour of the Capitol, visit this site (shown in Figure 1-1) to find out.

Fig. 6: Input Text Sample

How, this text will go in three different stages as illustrated before, first stage computes the local information for each paragraph alone and save it in the reference table, second stage computes the global information for the whole text and save it in the reference table, and the final stage encrypts the reference table.

1. Local Information Calculation

After breaking the input text into four paragraphs (the above text), the local information will be computed from each one independently.

The following figures show the key length for the four samples paragraphs.

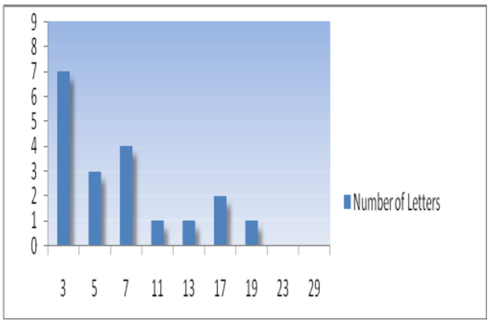


Fig. 7: First Paragraph Sample.

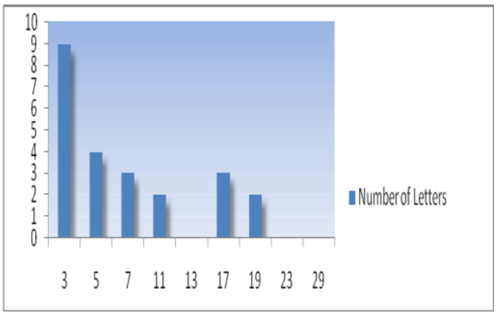


Fig. 8: Second Paragraph Sample.

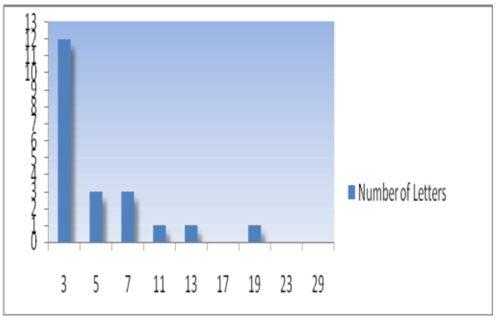


Fig. 9: Third Paragraph Sample.

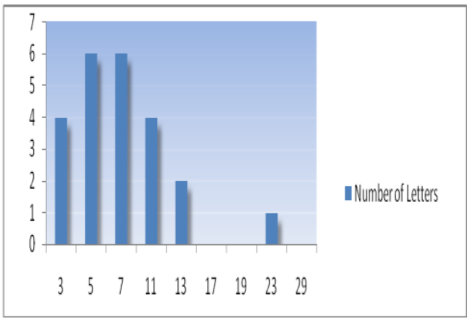


Fig. 10: Fourth Paragraph Sample.

The following table shows the keys used for each paragraph respectively.

Table 2: Local Keys Used

Paragraph Number	**Key Length**	**Key Value**
1	**7**	**PCILOKG**
2	**9**	**PETXOABSM**
3	**12**	**THEWORCYAUFG**
4	**4**	**OTRI**

After computing the local keys, the next stage is to compute the local bits for each paragraph, these bits are calculated using Hamming Code (as noticed before), the following table shows the local bits for each paragraph respectively.

Table 3: Local Bits Used

Paragraph Number	Total Letters	Total Bits	Nearest 2^x	Bits Length Used	Bits Value
1	305	2440	$2048=2^{11}$	11	11010010001
2	461	3688	$2048=2^{11}$	11	01101111000
3	298	2384	$2048=2^{11}$	11	11100000100
4	516	4128	$4092=2^{12}$	12	000000100111

Now, the local information for each paragraph is extracted and ready, these information will kept in a reference table as mentioned before.

2. Global Information Calculation

Now, the global information must be calculated for the whole input text, as mentioned before, the method of computing of the Global Information is the same as the Local Information except that the input text this time is the whole text and not just one paragraph.

Figure 11 shows the key length used for the global information extraction.

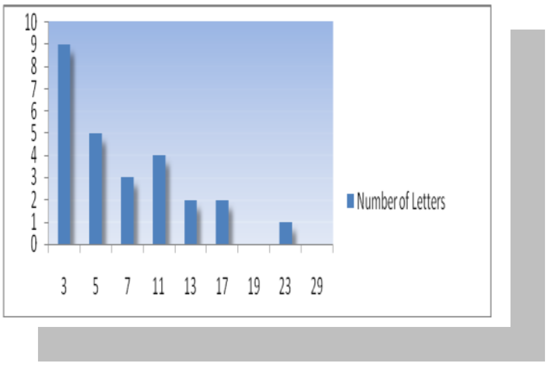


Fig. 11: Key Length

As noticed, the best choice for the key length is the length 3, the key value and the bits information are expressed in the following tables.

Table 4: Global Keys Used

Key Length	Key Value
7	PECANOMBF

Table 5: Global Bits Used

Total Letters	Total Bits	Nearest 2^x	Bits Length Used	Bits Value
1578	12624	$8192=2^{13}$	13	1001100000101

After this stage, the local and global information are extracted and kept in the reference table.

3. Reference Table Encryption

After finishing the calculation of local and global information, the final step is to encrypt the reference table that holds the above calculated information, the reference table looks like this:

Table 6: Reference Table Layout

Paragraph Number	Info Type	Length	Value
1	0	7	PCILOKG
2	0	9	PETXOABSM
3	0	12	THEWORCYAUFG
4	0	4	OTRI
1	1	11	11010010001
2	1	11	01101111000
3	1	11	11100000100
4	1	12	000000100111
0	0	7	PECANOMBF
0	1	13	1001100000101

Where:
Info Type: 0 means key information, 1 means bits information
Length: is the length of the information whether key or bits information
Value: is the value of the key or bits information

In the case of global information, the Paragraph Number contains the number 0.

The RSA method was used to encrypt this table with the following public and private keys.

Public Key (23, 323), Private Key (263, 323), and the encrypted reference table is:

Table 7: the Encrypted Reference Table

Before Encryption	After Encryption
107PCILOKG	178 193 234 245 288 61 304 224 284 181
209PETXOABSM	84 193 133 245 103 50 198 224 278 263 144 172
3012THEWORCYAUFG	204 193 178 84 50 268 103 26 224 176 288 166 278 187 128 181
404OTRI	86 193 86 224 50 176 61
1x111x11010010001	178 290 178 178 178 290 178 178 193 178 193 193 178 193 193 193 178
2x111x01101111000	84 290 178 178 178 290 193 178 178 193 178 178 178 178 193 193 193
3x111x11100000100	204 290 178 178 178 290 178 178 178 193 193 193 193 193 178 193 193
4x112x000000100111	86 290 178 178 84 290 193 193 193 193 193 193 178 193 193 178 178 178
007PECANOMBF	193 193 234 245 103 288 278 260 224 172 263 128
0x112x1001100000101	193 290 178 178 84 290 178 193 193 178 178 193 193 193 193 193 178 193 178

The encrypted information can be sent now to the receiver who is the only one that can decrypt the reference table because he has private key for decryption.

So, any change in any letter of the text or change of the positions of the letter will be detected at the receiver as the following example.

Consider that the second paragraph had some change at the first line by replacing the word CREATE by the word CRAETE (changing the sequence of E and A), as you see this kind of error is difficult to recognize, because the letters stay as it just transposition of two adjustment letters.

The extracted information will be:

Table 8: Key Information

Key Length	Key Value
9	PETXOABSM

Table 9: Bits Information

Total Letters	Total Bits	Nearest 2^x	Bits Length Used	Bits Value
461	3688	2048=2^{11}	11	01101110000

So, local key information does not affected because there is no change of letter frequencies just replacing A with E, but the bits information changed from (0110111**0**000) to (0110111**1**000), so a change has been detected.

There is another example showing how the key information works:

Consider the third paragraph had a change in the first line by changing the word comes with goes, now:

Table 10: Key Information

Key Length	Key Value
10	THWRCYMUFG

Table 11: Bit Information

Total Letters	Total Bits	Nearest 2^x	Bits Length Used	Bits Value
298	2384	2048=2^{11}	11	11100001101

The above tables are very clear showing that the key value is changed from (THEWORCYAUFG with length 12) to (THWRCYMUFG with length 10), and the bits information is changed also from (1110000**0**10**0**) to (1110000**1**10**1**) with keeping the total number of letters the same.

Conclusions:

The following conclusions are derived from the research:

the prime number 3 is used for most paragraphs to get longer key.To increase the complexity of the method , we must invent rules to select the most appropriate prime number for each paragraph.

The experimental results showed that the longer paragraph the more complex the key generated.

From (3) we can conclude that the proposed system is most appropriate for long text files with long paragraphs or for other files types like large pictures or very long wave files divided into large blocks.

The proposed system can be implemented for several types of text files to prevent intruders from modifying the text even the can read they text. This may be useful in solving the original text uncorrupted or unchanged by the intruder for commercial, political, diplomatic, and security files that exchanged over the internet.

Future Works:

For future work, one can increase the complexity of the system by generating a general key for several text files also it is possible to work on different types of files like video , image , or audio files.

References:

1. نوفل ، عبد الرزاق، 1982، "معجزة الارقام والترقيم في القرآن الكريم"، دار الكتاب العربي،
2. David J.C. MacKay, 2003,*Information Theory*, Inference, and Learning Algorithms, Copyright Cambridge University Press.
3. Moon, Todd K., Publish Date: 06/06/2005, *Error Correction Coding* , ISBN: 9780471648000 , Format: Hardcover Pages: 756 , Publisher: Wiley-Interscience ,Language: English.
4. David A. Patterson & John L. Hennessy. , 1998, *Computer Organization & Design*. Morgan Kaufmann Publishers, Inc: B34-B35.

   A concise description of Hamming Codes and other error detection mechanisms

5. Verman L. R., 1996, *Elements of Algebraic Coding Theory*. Chapman & Hall,: Ch3. Description and examples of forming Hamming codewords.
6. Houghton A. D. , 1997, *The Engineer's Error Coding Handbook*. Chapman & Hall,: 35-38, 53-60.Description of various error detecting/correcting codes.
7. Rivest, R.; A. Shamir; L. Adleman 1978. "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*". Communications of the ACM 21 (2): 120–126.doi:10.1145/359340.359342. http://theory.lcs.mit.edu/~rivest/rsapaper.pdf.
8. Cormen, Thomas H.; Charles E. Leiserson; Ronald L. Rivest; Clifford Stein 2001. *Introduction to Algorithms*, MIT Press and McGraw-Hill., (2nd ed.). pp. 881–887. ISBN 0-262-03293-7.
9. Ferguson;N. Schneier, B. 2003. *Practical Cryptography*. Wiley. ISBN 0-471-22357-3.
10. Katz, J. Lindell,Y. 2007. *Introduction to Modern Cryptography*. CRC Press. ISBN 1-58488-551-3.
11. Menezes, B. J., Oorschot, P. C. van; , Vanstone, S. A. 1997. *Handbook of Applied Cryptography*. ISBN 0-8493-8523-7.
12. Vanstone, Stott A. and Zuccherato, Robert J. Spring 1995, *Short RSA Keys and Their Generation. Journal of Cryptology*, Vol. 8, No. 2, pp. 101-114.
13. Anoop M.S. 2007. *Public key Cryptography - Applications Algorithms and Mathematical Explanations*. , Tata Elxsi , India:. http://www.infosecwriters.com/text_resources/pdf/Public_Key_Cryptography_AMS.pdf.
14. Micciancio D. and . Goldwasser, S, 2002, *Complexity of Lattice Problems: A Cryptographic Perspective*, Kluwer International Series in Engineering and Computer Science, Vol. 671, Kluwer Academic Publishers Cited, on page 284
15. Koblitz N., Menezes A. J., Y. H. Wu, and Zuccherato R., 2004, Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics, Springer-Verlag, Cited on page 284
16. Spillman R. J., 2004, *Classical and Contemporary Cryptology*, Preritice Hall, Cited on page 1.
17. Safford L. F. and Seiler D. W., January 2001, *Control circuits for electric coding machines*, United States patent number 6,175,625, Cited on page 53

حماية النص من التغيير باستعمال امنية القرآن و شفرات هامنك

مختار محمد حسن*   احمد عبد الأئمة*

*قسم الحاسبات – كلية العلوم للبنات – جامعة بغداد

الخلاصة:

إنَّ الانتشار الواسع للانترنت في جميع انحاء العالم مع تزايد العدد الهائل من المستخدمين الذين يتناقلون المعلومات المهمة عبرهُ سلط الضوء على طرائق جديدة لحماية المعلومات المتبادلة المهمة من العبث او التحريف من المتطفلين .

تقترح هذه الورقة البحثية طريقة جديدة لحماية الملفات النصية المختلفة من التحريف من المتطفلين او المخربين ولضمان أن النص الاصلي لم يتغير.

إنَّ الطريقة الجديدة هي عبارة عن خلطة من ثلاث خطوات . الخطوة الاولى تستعير بعض مفاهيم نظام الحماية في القرآن لأكتشاف نوع معين من التغيير الذي قد يحدث على النص جراء تدخل المتطفلين او المخربين اذ يتم استخراج مفتاح لكل فقرة في النص من مجموعة الاحرف الموجودة في الفقرة التي تتكرر بمضاعفات عدد اولي معين . هذه الخطوة لاتستطيع تحديد التغيير في النص الناتج من اعادة ترتيب كلمات او احرف النص الاصلي دون احداث تغيير في احرف النص. لذلك فان الخطوة التالية تستخدم احدى طرائق تحديد مكان الخطأ (أو التغيير) الا وهي طريقة هامنك Hamming Codes لاكتشاف حدوث التغيير وموقعه في النص. بعد ذلك تأتي الخطوة الثالثة اذ استخدمت طريقة التشفير باستخدام المفتاح العام RSA لتشفير المفاتيح المستخلصة من الخطوة الاولى لكل فقرة في النص وكذلك شفرات هامنك من الخطوة الثانية (لكل فقرة في النص أيضاً) لمنع المتطفلين من كسر الحماية التي توفرها الطريقة.

ان اهمية هذه الطريقة تبرز في حماية المعلومات المتبادلة المهمة من تحريف معناها الى معنى اخر او اضافة فقرات غير موجودة اصلاً او حذف فقرات من النص.ان هذه الطريقة مفيدة لحماية معلومات مثل الخطابات التجارية او الدبلوماسية اوالسياسية او حتى الامنية..الخ.