Transmitted Data Encryption Using RC4 Algorithm via Proposed Multi-tier Infrastructure Environment

Dr. Wisam Abed Shukur
Computer Science Department, College of Education For Pure Science/Ibn Al-Haitham, University of Baghdad, Iraq
Wisam_shukur@yahoo.com

Abstract:-

In this paper, the goal is to design and implement secure web site via two stages. The first stage is selecting the multi-tier architecture in infrastructure of network designing, this stage leads to prevent the direct access to database and increase the level of security since the middle tier (application server) will be receive the client's requests then interact with the last tier (database) to pass the results into client without direct accessing from client to database. The second stage is encrypting of transmitted data from the application server to client via using RC4 algorithm, this stage provides data secrecy or confidentiality to secure the transmission process of information through these tiers. This stage acts the core of this paper because all users of internet want to get secure transmission of their information. RC4 algorithm is used in this work because it has been used as the data encryption algorithm for many applications and protocols. RC4 algorithm is widely used in security software based on stream cipher including one in the encryption of traffic to and from secure web sites such as Transport Layer Security (TLS), Secure Socket Layer (SSL), and Wired Equivalent Privacy (WEP) implementations. RC4 algorithm is fast in comparison to other algorithms and it has a simple design hardware implementation. So,RC4 algorithm is five times faster than Data Encryption Standard (DES) and fifteen times faster than Triple-DES. The software requirements for this work are Windows 7, Adobe Dreamweaver CS6, Wampserver 2.2, PHP 5.2.9, Apache 2.2.22 and MySQL 5.5.24. the hardware requirements for this work are CPU (Intel(R) Celeron 1.732GHz for client, Intel(R) Dual-Core 2GHz for server and Intel(R) Core i5 2.4 GHz for database) and RAM (1GB for client, 4GB for server and 8GB for database).

Keywords: Security, Data Encryption, RC4, multi-tier architecture, server.

Introduction

Traditionally, the database applications use multi-tier architectures. The multi-tier architecture provides many advantages over client/server architecture [11]. The three-tier architecture consists of three tiers or layers that are: first tier deals with the user and system interfaces, second tier handles the business logic, being the core of the system, and third tier is representing the data storage. Enterprise applications are typically implemented as three-tier architectures that consist of clients in the front tier, servers that perform the application business logic processing in the middle tier, and databases that store the application data in the back-end tier [10]. The safety degree of data transferring between the server and the client is more interest for many web applications. Security is a continuous operation of protecting an object from unauthorized access. Fast implementation, small size, low complexity, and high security that provided by the cryptographic algorithms are imperative but the conventional cryptographic algorithms are very complex and consume significant amount of energy [13].

There are a number of cryptographic stream cipher algorithms presented to implement high performance software such as RC4. RC4 is a proprietary stream cipher which was designed in 1987 by Ron Rivest. RC4 is widely used in security software based on stream cipher including one in the encryption of traffic to and from secure web sites such as Transport Layer Security (TLS), Secure Socket Layer (SSL), and Wired Equivalent Privacy (WEP) implementations. RC4 is fast in comparison to other algorithms and it has a simple design hardware implementation [7]. For instance, RC4 is five times faster than Data Encryption Standard (DES) and fifteen times faster than Triple-DES [1]. RC4 has been used as the data encryption algorithm for many applications and protocols. Some of the protocols and applications using RC4 include the Wi-Fi, Skype, and Bit Torrent, to name a few. In this paper, the RC4 is performed to encrypt transmitted data from the application server to the client when the three tier architecture is used. This means, this proposed system is implemented at a hardware level (both nodes and network infrastructure) and at the programming level (both client and server side scripts).

Security Models

There are many models of security, These will be a computer security model that focuses on creating a secure environment for the use of computers [8], a network security model that involves creating an environment of a computer network, including all its resources, all the data in both storage and transit [17] and information security model that involves the creation of a state in which information and data are secure [8].

Security Services

There are five security services to protect resources of system from unauthorized parties such as access control, authentication, confidentiality, integrity and nonrepudiation [17].

1. Access Control

Two types of access control that are hardware access control and software access control [3]. Hardware access control is a network technology that possible to be connected to a monitoring network or remain in a stand-alone off-line mode like visual event, Access terminal, identification cards and video surveillance [4].

Software access control falls into two types that are point of access monitoring and remote monitoring [8].

2. Authentication

Authentication of user based on checking one or more of the items related to user such as user name, password, retinal images, fingerprints, physical location and identity cards [4].

3. Confidentiality

The confidentiality service protects information of system from unauthorized disclosure. This service uses encryption algorithms to ensure that nothing of the sort happened while the data was in the wild [8].

4. Integrity

The integrity service protects data against active threats such as those that may alter it[17].

5. Nonrepudiation

This is a security service that provides proof of origin and delivery of service and/or information. This service, through digital signature and encryption algorithms, ensures that digital data may not be repudiated by providing proof of origin that is difficult to deny [4].

Security Attack

Security attack defines any action that compromises the security of information owned by an organization. There are four general categories of attack that shown in **Fig. 1.**

1. Interruption

An asset of the system gets destroyed or becomes unavailable. This attack targets the source or the communication channel and prevents information from reaching its intended target.

2. Interception

An unauthorized party gets access to the information by eavesdropping into the communication channel.

3. Modification

The information is not only intercepted, but modified by an unauthorized party or to modify the content of transmitted message.

4. Fabrication

An attacker inserts counterfeit objects into the system without having the sender doing anything. When a previously intercepted object is inserted, this process is A called replaying. When the attacker pretends to be the legitimate source and inserts its desired information, the attack is called masquerading (e.g., replaying an authentication message or adding records to a file) [9].

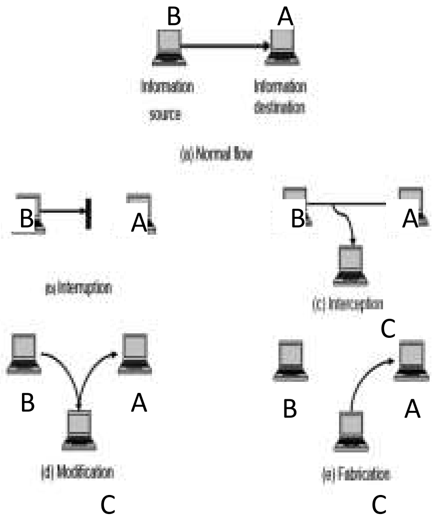


Fig. 1 Types of Security attacks

Cryptography

Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity [2]. Many cryptographic algorithms use complex transformations involving substitutions and permutations to transform the plaintext into the ciphertext. However, if quantum cryptography can be made practical, the use of one-time pads may provide truly unbreakable cryptosystems Encryption is the process of transforming plaintext data into cipher text in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data. Cryptographic algorithms can be divided into symmetric-key algorithms and public-key algorithms. Symmetric-key algorithms mangle the bits in a series of rounds parameterized by the key to turn the plaintext into the cipher text. Triple DES and Rijndael (AES) are the most popular symmetric-key algorithms at present. These algorithms can be used in electronic code book mode, cipher block chaining mode, counter mode, and others [5]. Public-key algorithms have the property that different keys are used for encryption and decryption and that the decryption key cannot be derived from the encryption key. These properties make it possible to publish the public key. The main public-key algorithm is RSA, which derives its strength from the fact that it is very difficult to factor large numbers [6]. Basically the two methods of producing cipher text are stream cipher and block cipher. The two methods are similar except for the amount of data each encrypts on each pass [14]. Another special type of encryption is the one way encryption, which is a method where the enciphering process is irreversible. The plaintext can never be recovered from the cipher text. This may seem pointless but it is probably the form of encryption that is the most familiar to computer users. Passwords on UNIX systems are encrypted by a one way algorithm [5].

RC4 Algorithm

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. The algorithm can be broken into two stages: initialization and operation. In the initialization stage the 256-bit state table, **State** is populated, using the **Key** as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The pseudo-code of initialization stage (KSA) is shown below [15];

```
x = 0;
For y = 0 to 255:
     State[y] = y;
For y= 0 to 255:
      x = (x + State[y] + Key[y]) mod
256;
Swap (State [y] and State [x]);
```

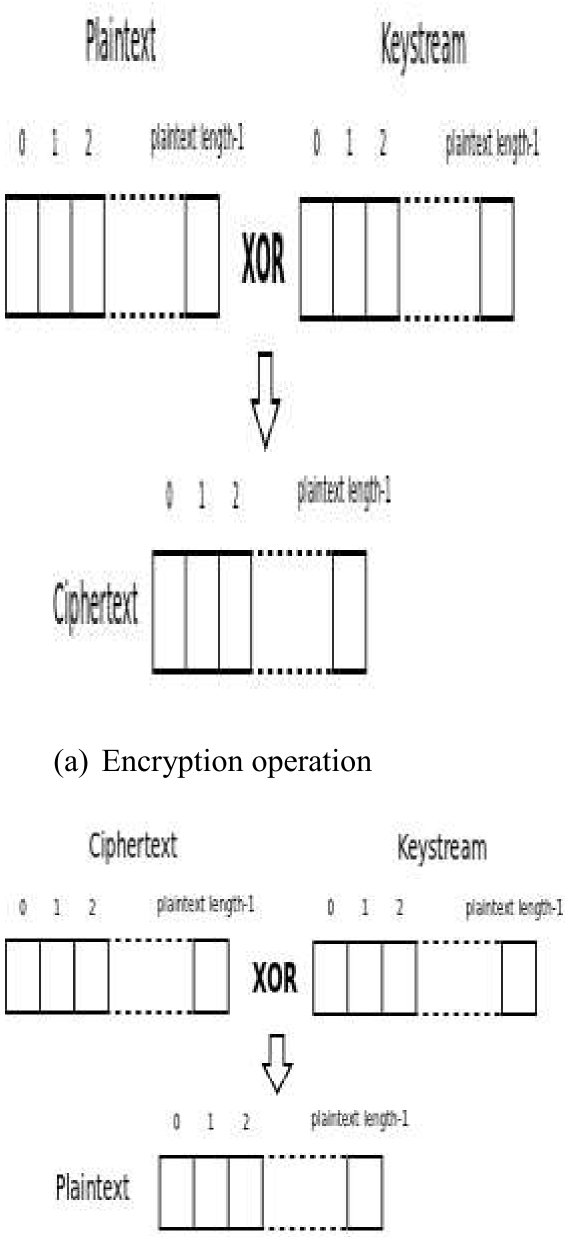
The actual example on how to attack the KSA is deriving the secret key from an early permutation; an attacker can re-derive the secret part by analyzing the initial word of the key stream with relatively little work.

The values of the state table are provided. It is important to notice here the swapping of the locations of the numbers 0 to 255 (each of which occurs only once) in the state table. The pseudo-code of operation stage (PRGA) is shown below:

```
y = x = 0;
for (k = 0 to N-1)
{
y = (y + 1) mod 256;
x = (x + State [y]) mod 256;
swap State [y] and State [x];
Result = State [ (State [y] + State
[x]) mod 256]
Cipher Message[k] XOR Result
}
```

Where Message [0..N-1] is the input message consisting of N bits.

The RC4 algorithm produces a stream of pseudo-random values. These values are XORed with the input stream in manner bit by bit. The encryption and decryption operations are the same as the data stream is simply XORed with the generated key sequence. The encryption and decryption operations are shown in **Fig. 2.**



(a) Encryption operation

(b) Decryption operation

Fig. 2 The encryption and decryption operations

The RC4 algorithm can be summarized in seven general steps that are shown as following:

1- Read the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate first array with numbers from 0 to 255.
4- Set the selected key in the second array.
5- Randomize the first array depending on the array of the key.
6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text [15].

Analysis of RC4 Algorithm

There are many basic features of RC4 algorithm such as symmetric stream cipher, variable key length, very quick in software and used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol. the RC4 algorithm is as another cipher algorithms has many advantages and disadvantages, some advantages of RC4 algorithm are faster than DES , enormous key space (average of 1700 bits), used in popular protocols such as secure socket layer (SSL) to protect internet traffic and in 802.11 WEP to secure wireless networks. In other side, the disadvantages of RC4 algorithm are large number of weak keys 1 of 256 and weak keys can be detected and exploited with a high probability. The key scheduling algorithm (KSA) can be attacked with several methods mainly because of the simple initialization permutation used [12]. In RC4 algorithm, the key has length from 1 to 256 bytes, that key is used to initialize a 256 byte state vector S (S[1],…,S[255]) which contains a permutation of all 8-bit numbers from 0 through 255. The key used in encryption and decryption processes is generated from S by selecting one of the 255 entries such as following:

```
For i=0 to 255 do
S[i]=i;
T[i]=K[i mod keylen] ;
```

To perform an initial permutation of S, the T is used such as shown in the following:

```
j=0;
 For i=0 to 255 do
j=(j+S[i]+T[i] mod 256);
Swap(S[i],S[j]);
```

Stream generation involves starting with S[0] through S[255], for each S[i], swapping S[i] with another byte in S, after S[255] is reached, the process continues then starting over again at S[0] such as shown in the following[16]:

```
i=j=0;
While (true)
i=(i+1) mod 256;
j=(j+ S[i]) mod 256;
Swap (S[i], S[j]);
T= (S[i]+S[j]) mod 256;
K=S[t];
```

RC4 Example

Encrypt the message (HI) by using RC4 algorithm if you have just 4-byte.
S = {0, 1, 2, 3}
K = {1, 7, 1, 7}
Set i = j = 0

KSA Stage

First Iteration: (i = 0, j = 0, S = {0, 1, 2, 3}):
j = (j + S[i] + K[i]) = (0 + 0 + 1) = 1
Swap S[i] with S[j]: S = {1, 0, 2, 3}

Second Iteration: (i = 1, j = 1, S = {1, 0, 2, 3}):
j = (j + S[i] + K[i]) = (1 + 0 + 7) = 0 (mod 4)
Swap S[i] with S[j]: S = {0, 1, 2, 3}

Third Iteration: (i = 2, j = 0, S = {0, 1, 2, 3}):
j = (j + S[i] + K[i]) = (0 + 2 + 1) = 3
Swap S[i] with S[j]: S = {0, 1, 3, 2}

Fourth Iteration: (i = 3, j = 3, S = {0, 1, 3, 2}):
j = (j + S[i] + K[i]) = (3 + 2 + 7) = 0 (mod 4)
Swap S[i] with S[j]: S = {2, 1, 3, 0}

PRGA Stage

Reset i = j = 0, Recall S = {2, 1, 3, 0}
i = i + 1 = 1
j = j + S[i] = 0 + 1 = 1
Swap S[i] and S[j]: S = {2, 1, 3, 0}
Output z = S[S[i] + S[j]] = S[2] = 3
Z = 3= (0000 0011), Since H=0100 1000 then :

```
    0100 1000 (H)
XOR 0000 0011 (3)
    0100 1011
```

i=1 , j=1 , S = {2, 1, 3, 0}
i = i + 1 = 2
j = j + S[i] = 1 + 3 = 4 (mod 4) = 0
Swap S[i] and S[j]: S = {3, 1, 2, 0}
Output z = S[S[i] + S[j]] = S[1] = 1
Z = 1 (0000 0001)

```
      0100 1001 (I)
XOR   0000 0001 (1)
      0100 1000
```

Result : **Plaint Text** : 0100 1000 0100 1001 (HI)
Cipher Text: 0100 1011 0100 1000

Plaintext:
SECRET DATA SECRET DATA SECRET DATA SECRET DATA SECRET DATA SECRET DATA SECRET DATA SECRET DATA
Key:

Wisam

Cipher text:

F7 57 0D CC 75 90 7E 63 43 CE F9 09 5B 33 E1 3B 84 F9 CC 73 D9 57 A5 A7 DE 96 68 26 3C 5B 29 57 CF 9A 2E C8 54 25 90 46 68 39 AB 25 87 43 8C 38 A3 A6 24 50 11 41 6A 37 79 64 B1 EB 00 E5 40 D2 5C 84 D6 AB 75 DB E6 83 A0 49 4C CC E9 C2 42 C7 6E 3F BB 1B 23 EF 98 85 2C 04 E8 69 44 5D 85 14

Time: 4 sec.

The Proposed System

The proposed system aims to secure transmission process of data from application server to client by using RC4 algorithm via designing simple website based on three-tier architecture. Therefore, the core of this work is using RC4 algorithm to encrypt transmitted data from application server tier to client tier. This work describes a method for building applications with a three-tier structure (client, server, and database) as shown in **Fig. 3**. The database server tier consists of the DBMS (the Database Management System) and the database that built it off-line to reduce unauthorized access to sensitive data. The Client tier which is usually a web browser processes and used to display HTML resources, these web browsers are HTTP clients that interact with the Web servers using standard protocols. In the middle comes the application server tier that includes most of the application logic. The input receives from the clients and interacts with the database through this tier and also the results are sent to application server then to client.

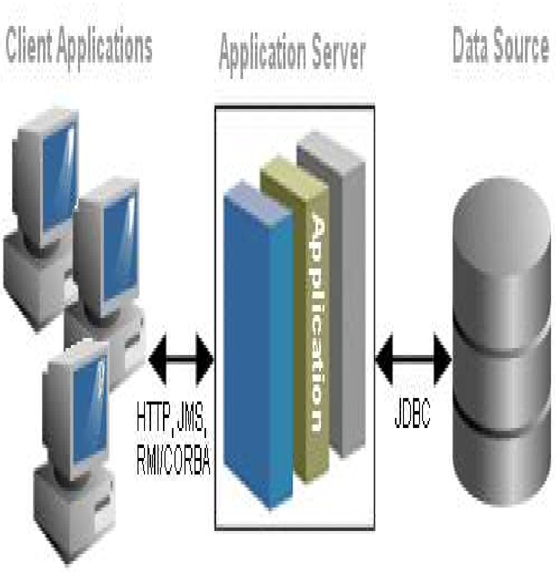


Fig. 3 Three-Tier Architecture General Structure of Proposed System

In this work, the network is designed based on multi-tier architecture, therefore, the network consists of three parts or modules that are client tier, and application server tier and database tier as shown in **Fig. 4**.

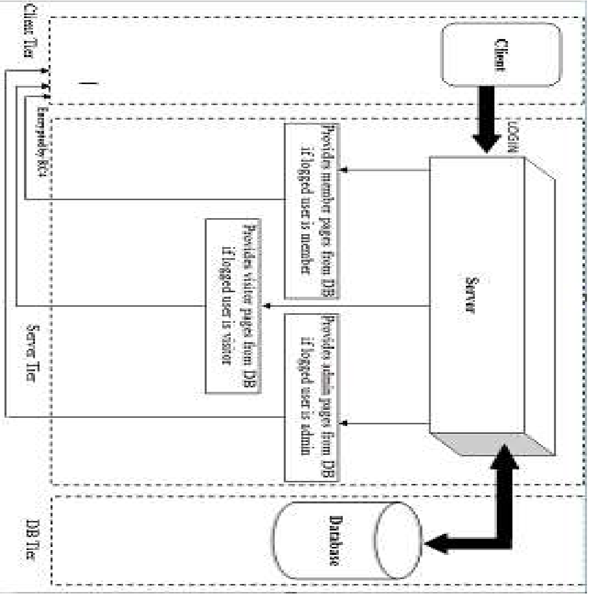

Client Tier
Client
LOGIN
Encrypted by RC4
Provides member pages from DB if logged user is member
Provides visitor pages from DB if logged user is visitor
Provides admin pages from DB if logged user is admin
Server
Server Tier
DB Tier
Database

Fig. 4 General structure of the proposed system

There are three types of users that can use a site designed in PHP, each one of them has permissions or privileges that makes them to access contents of a site correctly.

1. Visitor User: all users can enter the site and show allowable contents.
2. Members User: all members' users can view full contents of a site and download it as they want.
3. Administrator User: who has the ability to access all pages of site and manage it such as add new contents, delete contents and activate or block members' accounts.

In this work, the middle tier is usually split recursively into three tiers again. The Client applications that run inside the browser submit requests to the web server using HTTP protocol. The 'presentation layer' on the server transforms the request and passes it to the 'business layer' which will perform some computation by interacting with the 'data layer'. The results from the 'business layer' are transformed into HTML by the 'presentation layer' and returned as the response to the client. The most popular way of generating HTML responses in the middle tier is by using the server pages, the server page is a special HTML page that contains embedded scripts.

Implementation of the Proposed System

The proposed three tire system that designed using Adobe Dreamweaver for writing the programs and creating the web pages, using GUI for login screens and interacting with database PHP 5.2.9 as Programming language to write all programs, Apache server 2.2.22 as web server software, and MySQL 5.5.24 is used for creating the local and global database (server). The proposed tire site contains three types of users that are Visitor, Member and administrator.

Visitors

This is allowable for everyone, it contains information about site and the pages to registers and login and contains information about what is available in site. This consists of three pages:

1- **Home Page:** it's a window of the proposed site and the main URL address, it contains text links and thumbnails links with links for Sign-in (for login to member pages), Administration (for login to administrator pages) and registration pages as shown in **Fig. 5.**

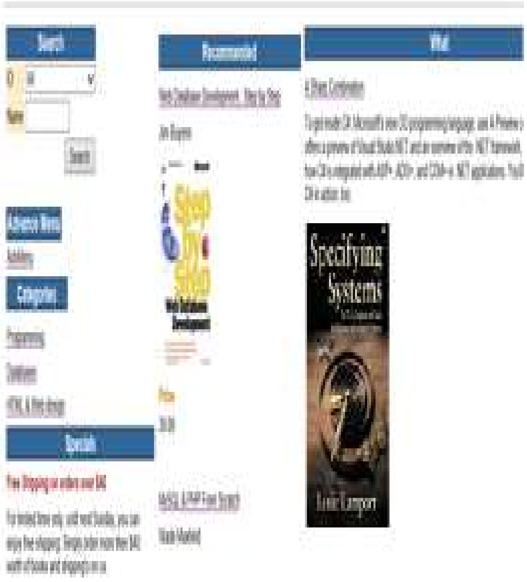
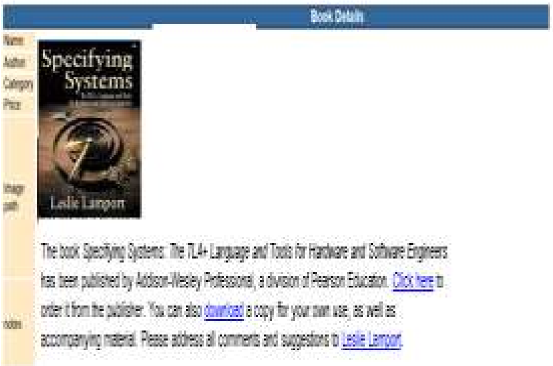


Fig. 5 Visitor Home Page

All details of book such as book name, author, category, and book cover image and descriptions are displayed when the book thumbnail was clicked by user as shown in **Fig. 6.**



The book Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers has been published by Addison-Wesley Professional, a division of Pearson Education. Click here to order it from the publisher. You can also download a copy for your own use, as well as accompanying material. Please address all comments and suggestions to Leslie Lamport.

Fig. 6 Book Details Page

2- Register Page: this page is an electronic form that user must full to have an account in the proposed bookstore site as shown in **Fig. 7.**

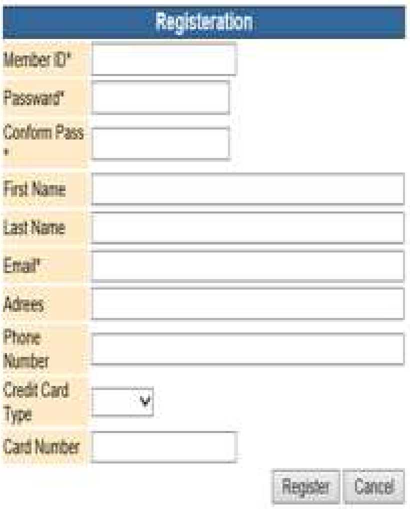


Fig. 7 Register page

3- **Sign In:** this page is the portal page to member pages that verified if the client is allowed or not allowed to enter member pages as shown in **Fig. 8.**

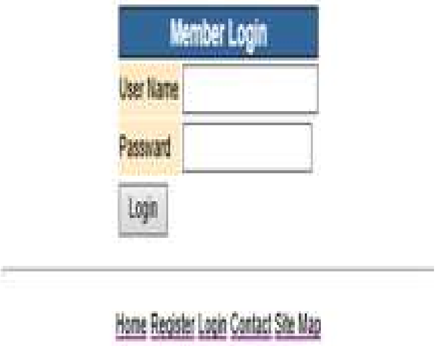
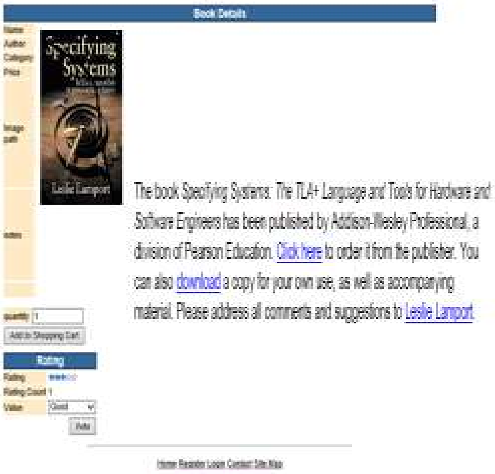


Fig. 8 Sign-in Page

Members

This level is allowable just for the activated members after passing authentication process. It contains main web pages of proposed Bookstore site, which contains books that are available just for members; also, it give the ability to members to view allowable books or buying books from site.

1- **Member Home Page:** it's the default page of member site as shown in **Fig. 9.** It contains text links and thumbnails links for books and its categories.



The book Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers has been published by Addison-Wesley Professional, a division of Pearson Education. Click here to order it from the publisher. You can also download a copy for your own use, as well as accompanying material. Please address all comments and suggestions to Leslie Lamport.

Fig. 9 Member Home Page

2- **Shopping Cart Page:** this page represents member shopping of books. It is including member information and books shopping details as shown in **Fig.10.**

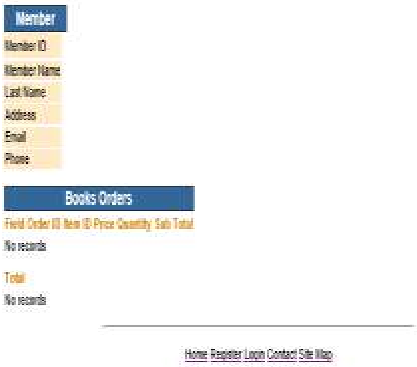


Fig. 10 Shopping Cart Page

Administrator

This is allowable just for the administrator after passing the authentication process. It manages the proposed bookstore site such as user information, user activation, deleting account, adding books and edit books categories.

1- **Administrator Home Page:** it contains links of management pages such as: member accounts, books details and information, books categories, editorials, editorials categories orders and credit card types as shown in **Fig. 11.**

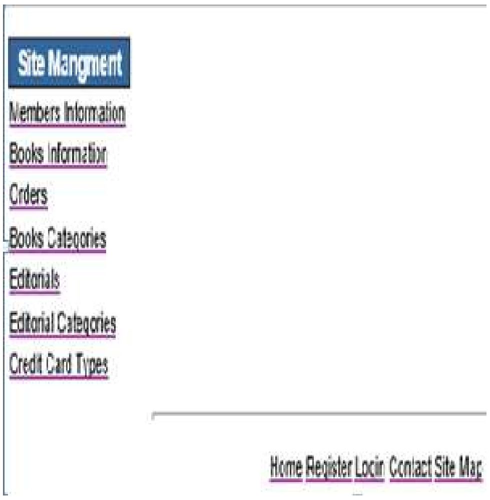


Fig. 11 Administrator Home Page

Conclusions

The multi-tier architecture is used as infrastructure environment for the proposed system. Using RC4 algorithm to secure data transmission between application server and client acts the core of the proposed system. There are many points concluded as following:

1- The three tier architecture of the proposed system plays the basic role of database security because the client does not have a direct access to the database.

2- The Application Server -to-Client provides data confidentiality by using the RC4 algorithm.
3- The time of encryption and decryption processes is related to the key length and to size of data file.
4- The text data requires less time to be processed than image data mainly due to the larger file size of image.
5- The KSA can be attacked with several methods mainly because of the simple initialization permutation used.

References

[1] Ahmad S, Beg MR, Abbas Q, Ahmad J, Atif S, " Comparative study between stream cipher and block cipher using RC4 and Hill Cipher" Int J Comput Appl (0975–8887), 1(25),2010.

[2] Andrew S. Tanenbaum, Computer Networks, Fourth Edition, Prentice Hall, 2003.

[3] Budi K., "Java for the Web with Servlets, JSP, and EJB: A Developer's Guide to J2EE Solutions", Sams Publishing; First Edition, ISBN: 073571195X, 2004.

[4] Charles P. P. and Shari L. P., "Security in Computing, Fourth Edition", Prentice Hall, Fourth Edition, ISBN: 978-0132390774, 2006.

[5] David Groth, Network+ ™, Study Guide, Third Edition, SYBEX, Inc., Alameda, CA, 2002.

[6] Glover, P. and M. Grant, Digital Communications, 2nd edition, Person Education, 2004.

[7] Gupta SS, Chattopadhyay A, Sinha K, Maitra S, Sinha B, " High-performance hardware implementation for RC4 stream cipher" IEEE Trans Comput 62(4):730–743,2013.

[8] John R. V., "Computer and Information Security Hand Book", Morgan Kaufmann, ISBN: 0123743540, 2009.

[9] Joseph M. K., "A Guide to Computer Network Security", Springer, Second Edition, ISBN: 184800916X, 2008.

[10] Mumtaz A. and Sarmad H., "Developing a Three-Tier Web Data Management Application for Higher Education Admission Environment", International Arab Journal of e-Technology, Vol. 2, No. 4, June 2012.

[11] Oracle Technology Network, http://java.sun.com/products/jsp/ JavaServer Pages.

[12] Scott Fluhrer, Itsik Mantin and Adi Shamir, Weaknesses in the key scheduling algorithm of RC4, 2008.

[13] Sharma K, Ghose MK, Kumar D, Singh RPK, Pandey VK, "A comparative study of various security approaches used in

wireless sensor networks” Int J Adv Sci Technol, 177(77), 2010.

[14] Wenbo Mao, Modern Cryptography Theory and Practice, Prentice Hall, New Jersey, 2004.

[15] William Stallings, Cryptography and network security: Principles and practice, Prentice Hall, Upper Saddle River, New Jersey, 2003.

[16] William Stallings, “ The RC4 stream encryption algorithm”, 2005.

[17] William S., “Network Security Essentials: Application and Standards”, Pearson Education, ISBN: 978027379336, 2011.

تشفير البيانات المرسلة باستخدام خوارزمية RC4 في بيئة مقترحه ذات طبقات متعددة

د. وسام عبد شكر

قسم علوم الحاسبات/كلية التربية للعلوم الصرفة - ابن الهيثم

جامعة بغداد

Wisam_shukur@yahoo.com

الخلاصة

في هذا البحث الهدف هو تصميم وتنفيذ موقع الكتروني امين من خلال مرحلتين وهما: المرحلة الاولى هي اختيار معماريه ذات طبقات متعددة (ثلاث طبقات) في البنيه التحتية عند تصميم الشبكة, وهذه المرحلة تؤدي الى منع الوصول المباشر الى قاعدة البيانات وبهذا تزيد من مستوى الأمنية والسبب هو ان الطبقة الوسطى (سيرفر التطبيق) سوف يستلم طلبات المستخدمين وبدوره يتعامل مع الطبقة الأخيرة وهي قاعدة البيانات لغرض تمرير نتائج طلبات المستخدمين الى المستخدمين بدون الوصول المباشر للمستخدمين الى قاعدة البيانات. اما المرحلة الثانية فهي تشفير البيانات المرسلة من الطبقة الوسطى (سيرفر التطبيق) الى الطبقة الأخيرة وهي قاعدة البيانات من خلال استخدام خوارزمية RC4 للتشفير, وهذه المرحلة توفر خصوصية للبيانات لغرض تامين عملية نقل البيانات خلال الطبقات الثلاثة لمعمارية الشبكة المقترحة. هذه المرحلة تمثل جوهر البحث بسبب ان جميع مستخدمي الانترنت يريدون ان يحصلوا على نقل امين لمعلوماتهم عبر الشبكة العالمية.

ان خوارزمية RC4 تستخدم بشكل واسع في برمجيات الأمنية بالاعتماد على التشفير التدفقي من والى المواقع الإلكترونية مثل WEP, SSL, TLS . خوارزمية RC4 هي سريعة مقارنة" بالخوارزميات الاخرى اضافة الى انها تمتلك تصميم مادي بسيط وكذلك انها اسرع خمس مرات تقريبا" من خوارزمية DES وبخمسة عشر مره تقريبا" من خوارزمية 3-DES.

المتطلبات البرمجية هي : Windos7, Adobe Deamweaver CS6, Wampserver 2.2, PHP5.2.9 , Apache 2.2.22, MySQL5.5.24 اما المتطلبات المادية فهي: CPU with 1.7 GHz للمستخدم, Dual-core 2GHz للسيرفر core i5 with 2.4 GHz لقاعدة البيانات , وذاكرة RAM 1GB للمستخدم, وذاكرة RAM 4GB للسيرفر, وذاكرة RAM 8GB لقاعدة البيانات.

الكلمات المفتاحية: امنية ، تشفير البيانات، RC4، معماريه متعددة الطبقات ، سيرفر.