Asian Journal of Information Technology 7 (8): 316-331, 2008
ISSN: 1682-3915

Design and Implementation of a Web-Based Information Technology with Security Measures Against Threats and Risk

[1]M.S. Okundamiya, [1]O.S. Udeozor and [2]T.P. Okundamiya
[1]Department of Electrical and Electronic Engineering,
Ambrose Alli University, P.M.B. 14, Ekpoma, Nigeria
[2]Westfield Christian College, P.O. Box 10612, Benin City, Nigeria

Abstract: This study presents a web-based information technology that allows students to access departmental information and resource materials spontaneously, share academic ideas with their global counterpart as well as safeguard confidential documents to avoid indiscriminate alteration. The web enabled front page was designed using Microsoft Frontpage in conjunction with Java Script, MySQL and PHP, while mono-alphabetic substitution and a highly programmed corrupt pages were used as a security measure in order to safeguard sensitive information from unauthorized users thereby making the design simple. The design implemented at Westfield Christian College to meet the learning, writing and research needs of students and staff has considerably improve academic performance and has enabled users to share knowledge in straightforward and popular platforms.

Key words: Ubiquitous learning, information security, ciphertext, encryption, decryption mechanism

INTRODUCTION

In recent times, there has been a growing need in academic institutions for ubiquitous access to academic information. Much of the literature on web based learning shows that one of the main barriers to the effective use of teaching materials is the technology (for example, poor access, slow downloading) rather than the design of the learning materials themselves (McKimm *et al*., 2003). The technology must therefore be applied appropriately and not used simply, because it is available and new or because students and teachers have particular expectations of this means of course delivery. Two of the main developments in web based learning have been the adaptation of communication technology to support learning and the changes in distance learning strategies necessary for delivering online courses.

Web based learning offers huge opportunities for learning and access to a vast amount of knowledge and information. The role of teachers is to ensure that the learning environment provided takes account of learners' needs and ensures that they are effectively prepared and supported.

- It optimizes the use of staff time.
- It can be an efficient way of delivering course materials.
- It provides resources from any location and at any time.
- It is a convenient way for students to submit assessment from remote sites.
- It is a potential for widening access-for example to part time, mature, or work based students.
- It can encourage more independent and active learning.
- It can provide a useful source of supplementary materials to conventional programs.

With the recent technological developments in information technology, an opportunity has emerged to introduce more efficient instruction into the classroom. The Web-based Information Technology with security measures against threats and risks enables users to share knowledge in straightforward and popular platforms. The need to share knowledge is not restricted to classroom environment, since knowledge lives in the world and mobile applications supply students with the opportunity of ubiquitous learning. With the increasing popularity of the Internet, web-based environments have become well-suited for facilitating students learning asynchronously (Hiltz and Wellman, 1997). Moreover, some investigations have revealed that interpersonal contact through electronic discussion forums results in sharing and transfer of knowledge. Thus, electronic

Corresponding Author: M.S. Okundamiya, Department of Electrical and Electronic Engineering,
Ambrose Alli University, P.M.B. 14, Ekpoma, Nigeria

discussion forums can be adopted in a knowledge platform for knowledge management (Hahn and Subramani, 2000).

There has been the need to protect information from prying eyes. The Evolution of Information System (IS) technology has made computer system opened to abuse and information access, controls several orders of magnitude more complex (Bosworth and Kabay, 2002). Vulnerabilities make a system more prone to attack by a threat, which the intruder exploits. Threats to intellectual property have become more dangerous, these threats are becoming more disastrous and attractive to criminals. Recent news reports the penetration of hackers into the records of the University of Virginia between May 2005 and April 2007 despite security measures.

This study presents the implementation of a web-based information technology with security measures carried out at Westfield Christian College in Benin City, which shows the performance evaluation of a cross section of students and also explains how stored information is being secured from unauthorized users.

Overview of security measures: Security is a condition of being protected from danger or loss and not exposed to damage from accidents or attack, or it can be defined as the process for achieving that desirable state. It also refers to a condition that prevents unauthorized persons from having access to ones possession or property (Okundamiya *et al*., 2008). The objective of Information System Security (ISS) is to optimize the performance of an organization with respect to the risks to which it is exposed to (Bosworth and Kabay, 2002), such risks defined as the chance of injury, damage, or loss would be infinitely expensive because of the uncertainty about future risk losses or perfect security, which implies zero losses. For this reason, ISS risk managers strive to optimize the allocation of resources by minimizing the total cost of ISS measures taken and the risk losses experienced. This optimization process is commonly referred to as risk management.

The Data Encryption Standard (DES) developed by a team of IBM researchers around 1974 was accepted by the US National Bureau of Standard (NBS, which later became the National Institute of Standards and Technology, NIST) in 1977 as a standard approach. The entire algorithm of the DES was published in the Federal Register of January 15, 1977 (Coppersmith, 1994). The DES, which operates as a block cipher with 64-bit blocks, 16 rounds and a variable key length up to 56 bits is still the most well-known and widely deployed secret key cryptosystem today. In secret key cryptography a secret key is established and shared between communicating peers, which is used to encrypt and decrypt messages on both sides hence, it is called symmetric cryptography (Opplier, 2002). The purpose of the DES algorithm was to provide for the encryption and decryption of text in an efficient and unbreakable manner. The IBM also developed the enable owner of copy righted material to distribute information securely over the internet and receive payment use.

Since that time, many cryptanalysts have attempted to find shortcuts for breaking the system. Whitfield Diffie and Martin Hellman presented some basic arguments concerning the DES inadequate level of security and also, criticize the secrecy of its design principles and structures based on the weakness it suffers and suggested that the DES be modified (Diffie and Hellman, 1977). However, their suggestions were rejected by the NBS based on a number of objections. Contrary to the speculations on secrecy of the DES design based on hidden weakness, Don Coppersmith a member of the IBM research team, in 1994 published the design considerations and structures of the DES to dispel contrary notions (Coppersmith, 1994). His article revealed the strengths of the DES against attacks as it outlined both the criteria that the IBM used to design the s-boxes and permutation specifically to thwart attack based on differential cryptanalysis and the measure of its success based on the enormous amount of chosen plaintext (in excess of 10^{15}bytes) required by Biham and Shamir's attack. However, its 56-bit effective key length that was sufficiently secure during its first two decades of operation is far too short today. Other algorithms have been developed over the years (Opplier, 2002)

Diffie and Hellman (1977) devised a clever scheme that allows remote entities to advertise a public and the private key secret. This scheme was able to allow communication between many systems without the need for storage and maintenance of many private keys. However, the scheme is more complicated and computationally intensive. Rivest *et al*. (1978) at MIT devised the most famous implementation of public protocol called RSA algorithm. This algorithm involves the multiplication of large prime numbers to produce keys used for encryption and decryption. An intruder will not be able to decrypt such message because of the difficulty in factorizing large numbers. Unlike other public key cryptosystems the same algorithm can be used for message encryption and decryption, as well as digital signature generation and verification.

MATERIALS AND METHODS

A cross section of students from Westfield Christian College in Benin City was used as a case study for evaluating the performances of students based on the

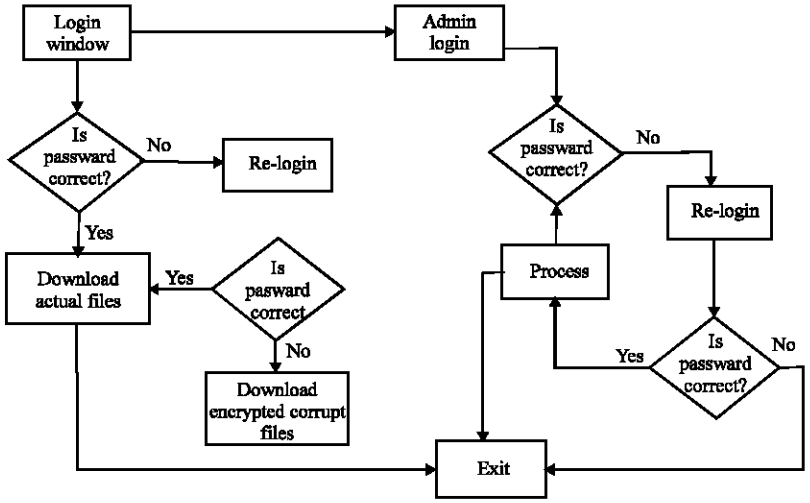

Fig. 1: Design application flowchart

Table 1: Mixed alphabets

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Z	E	N	I	T	H	A	B	C	D	F	G	J	K	L	M	O	P	Q	R	S	U	V	W	X	Y

implementation of a web-based information technology. This study was carried out for one academic session-September 2007-July 2008 and deductions were made based on the available data obtained during these periods. A secured database was developed for the school with the private key (password) controlled by the principal and the network administrator.

Design analysis/consideration: It is a well known fact that access to secured information is denied when wrong passwords are used-the principle behind most security designs. If an intruder uses a guess password at first attempt and access is granted, then he/she may believe that the guess password is correct hence, may not need to hark further or attempt to steal the password. This was the underlying principle used in this design.

The decrypting algorithm operates using the IF---THEN--- structures such that if the guess password is completely identical then access is granted to the document otherwise access is directed to a re-login window. If at second attempt password is correct, the actual secured files are opened otherwise a highly encrypted corrupt file will be opened will an alert message telling the intruder that the document has been infected with a virus. This is illustrated in Fig. 1.

It involves replacing a clear text character with other character and the result will be ciphertext that does not resemble the original text in any obvious manner, i.e., the replacement of each message with another symbol. It can either be monoalphabetic or polyalphabetic. In this study, monoalphebetic substitution was implemented. A program for the decryption mechanism was written using Java Script, MySQL and PHP.

Monoalphabetic substitution: Monoalphabetic plaintext substitution such as Caesar substitution is a system of encryption where every occurrence of a particular letter is replaced by a cyphertext letter. A Monoalphabetic cipher uses fixed substitution over the entire message. It is a simple substitution since, it operates on single letters. Simple substitution can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or reversed creating the Caesar and Atbash ciphers, respectively or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet.

Traditionally, mixed alphabets are created by first writing out a key word, removing repeated letters in it and then writing all the remaining letters in the alphabet. This technique was implemented in this design. Using this system, the key word zenith gives us the alphabets as shown in Table 1.

A message of communications engineering enciphers to:

"NLJJSKCNZRCLKQ TKACKTTPCKA"

Traditionally, the ciphertext is written out in blocks of fixed length, omitting punctuation and spaces; this is done to help avoid transmission errors and to disguise word boundaries from the plaintext. These blocks are

Table 2: Caesar cipher

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table 3: Atbash cipher

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Table 4: Reversed caesar substitutions

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X

Table 5: Performance analysis of a section of westfield christian college for 2007/2008 academic session.

		Numbers of students with at least 60% average scores		
		Before implementation	After implementation	
Class	Class size	1st term	2nd term	3rd term
SSS 1	36	21	26	34
SSS 2	33	22	27	33
Total	69	43	53	67

called groups and sometimes a group count (i.e., the number of groups) is given as an additional check. Five letter groups are traditional, dating from when messages used to be transmitted by telegraph: Thus, it becomes,

"NLJJS KCNZR CLKQT KACKT TPCKA"

If the length of the message happens not to be divisible by five, for example, a message of Ambrose Alli University Ekpoma, which enciphers to:

"ZJEPLQT ZGGC SKCUTPQCRX TFMLJZ",

it may be padded at the end with nulls. These can be any characters that decrypt to obvious nonsense, so the receiver can easily spot them and discard them. This is illustrated as:

"ZJEPL QTZGG CSKCU TPQCR XTFML JZVFF",

Caesar cipher: The Caesar cipher also called ROT3 (or rotate 3) cipher (Tittel *et al*., 2004) is one of the simplest monoalphabetic substitutions one may use and it's also, one of the easiest to break-as there are only 26 Caesar alphabets it is trivial to solve a Caesar Cipher by exhaustive search. This is can be done by listing the alphabet under each letter of a section of the ciphertext. The line, which contains legible plaintext is the correct one. It is said that Julius Caesar wrote to his friends using a simple substitution cipher, where the plaintext letter was replaced by the ciphertext 3 places down the alphabet, so that the letter G is replaced by J and so on. Here, the encryption and decryption keys are both determined by a shift but the encryption and decryption rules are different. The Caesar cipher is summarized in a Table 2. It is now the case that any cipher whose cipher alphabet consists of the letters in their normal order is called a Caesar cipher.

Atbash cipher: This is a simple substitution very similar in nature to the Caesar Substitution. Whereas, the caesar substitution was Roman in origin, Atbash is Jewish in origin. In Atbash, the last letter represents the first, the second to last represents the second and so on, as shown in Table 3. Atbash is even simpler to solve than the Caesar Substitution.

Atbash can also be combined with a Caesar shift, to produce a Reversed Caesar substitution (Table 4).

RESULTS AND DISCUSSION

Scripts 1-4 shows the stages in the encryption and decryption processes.

Script 1: Index.php

```
<?php require_once('Connections/lsc.php'); ?>
<?php $go= $_POST['username'] ; ?><?php
// *** Validate request to login to this site.
if (!isset($_SESSION)) {
  session_start();
}
$loginFormAction = $_SERVER['PHP_SELF'];
if (isset($_GET['accesscheck'])) {
  $_SESSION['PrevUrl'] = $_GET['accesscheck'];
}

if (isset($_POST['username'])) {
  $loginUsername=$_POST['username'];
  $password=$_POST['passkey'];
  $MM_fldUserAuthorization = "";
  $MM_redirectLoginSuccess = "_pages/_r_file_dnld.php?y=$go";
  $MM_redirectLoginFailed = "_pages/_f_file_dnld.php";
  $MM_redirecttoReferrer = false;
  mysql_select_db($database_lsc, $lsc);

  $LoginRS__query=sprintf("SELECT username, passkey FROM lsc WHERE username='%s' AND passkey='%s'",
    get_magic_quotes_gpc() ? $loginUsername : addslashes($loginUsername), get_magic_quotes_gpc() ? $password : addslashes($password));
r5
  $LoginRS = mysql_query($LoginRS__query, $lsc) or die(mysql_error());
  $loginFoundUser = mysql_num_rows($LoginRS);
  if ($loginFoundUser) {
     $loginStrGroup = "";

    //declare two session variables and assign them
    $_SESSION['MM_Username'] = $loginUsername;
    $_SESSION['MM_UserGroup'] = $loginStrGroup;

    if (isset($_SESSION['PrevUrl']) && false) {
      $MM_redirectLoginSuccess = $_SESSION['PrevUrl'];
    }
    header("Location: " . $MM_redirectLoginSuccess );
  }
  else {
    header("Location: ". $MM_redirectLoginFailed );
  }
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>:: Welcome to West Christain College ! ::</title>
    <td><form id="form1" name="form1" method="POST" action="<?php echo $loginFormAction; ?>">
      <table width="385">
        <tr>
          <td colspan="2" align="center"><span class="style1">Welcome to Westfield Christian College ! </span></td>
        </tr>
        <tr>
          <td colspan="2"> </td>
        </tr>
        <tr>
          <td colspan="2" align="right"><span class="style6"><a href="adminl.php">&gt;(Admin Login)</a></span> </td>
        </tr>
        <tr>
          <td colspan="2" align="center"><span class="style5">(Login to Download Teaching aid)</span></td>
          </tr>
        <tr>
          <td width="121" align="right"><span class="style4">Username:</span></td>
          <td width="236" class="style5"><label>
            <input name="username" type="text" class="style5" id="username" />
          </label></td>
        </tr>
        <tr>
```

Script 1: Continued

```
        <td align="right"><span class="style4">PassKey:</span></td>
        <td class="style5"><label>
          <input name="passkey" type="password" class="style5" id="passkey" />
        </label></td>
      </tr>
      <tr>
        <td> </td>
        <td><label>
          <input name="Submit" type="submit" class="btn" value="Submit" />
        </label></td>
      </tr>
    </table>
      </form>
  </td>
 </tr>
</table>
</body>
</html>
```

Script 2: Real file download

```
<?php require_once('../Connections/lsc.php'); ?>
<?php
//initialize the session
if (!isset($_SESSION)) {
  session_start();
}

// ** Logout the current user. **
$logoutAction = $_SERVER['PHP_SELF']."?doLogout=true";
if ((isset($_SERVER['QUERY_STRING'])) && ($_SERVER['QUERY_STRING'] != "")){
  $logoutAction .="&". htmlentities($_SERVER['QUERY_STRING']);
}

if ((isset($_GET['doLogout'])) &&($_GET['doLogout']=="true")){
  //to fully log out a visitor we need to clear the session varialbles
  $_SESSION['MM_Username'] = NULL;
  $_SESSION['MM_UserGroup'] = NULL;
  $_SESSION['PrevUrl'] = NULL;
  unset($_SESSION['MM_Username']);
  unset($_SESSION['MM_UserGroup']);
  unset($_SESSION['PrevUrl']);

  $logoutGoTo = "../index.php";
  if ($logoutGoTo) {
    header("Location: $logoutGoTo");
    exit;
  }
}
?>
<?php
$colname_ls = "-1";
if (isset($_GET['y'])) {
  $colname_ls = (get_magic_quotes_gpc()) ? $_GET['y'] : addslashes($_GET['y']);
}
mysql_select_db($database_lsc, $lsc);
$query_ls = sprintf("SELECT username FROM lsc WHERE username = '%s'", $colname_ls);
$ls = mysql_query($query_ls, $lsc) or die(mysql_error());
$row_ls = mysql_fetch_assoc($ls);
$totalRows_ls = mysql_num_rows($ls);
?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>:: Welcome to West Christain College ! ::</title>
<style type="text/css">
<!--
body {
        background-color: #CCCCCC;
```

Script 2: Continued

```
}
.style1 {
	font-family: Verdana, Arial, Helvetica, sans-serif;
	font-weight: bold;
}
a:link {
	text-decoration: none;
}
a:visited {
	text-decoration: none;
}
a:hover {
	text-decoration: underline;
}
a:active {
	text-decoration: none;
}
.style2 {
	font-family: Verdana, Arial, Helvetica, sans-serif;
	font-size: 12px;
}
.style4 {
	color: #333333;
	font-family: Verdana, Arial, Helvetica, sans-serif;
	font-size: 14px;
	font-weight: bold;
}
.style5 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; font-weight: bold; }
-->
</style>
<link href="../btn.css" rel="stylesheet" type="text/css" /></head>

<body>
<p> </p>
<p> </p>
<table width="384">
  <tr>
    <td width="376"><span class="style2">Welcome <?php echo $row_ls['username']; ?> ! Your login was successful.</span> </td>
  </tr>
</table>
<p> </p>
<table width="350" align="center">
  <tr>
<td> </td>
  </tr>
  <tr>
    <td><span class="style5">Click to download ! </span></td>
  </tr>
  <tr>
    <td align="center"><form action="../real files/Wireless networking standards and security.pdf" method="get" enctype="multipart/form-data" name="form1"
id="form1">
      <table width="350">
        <tr>
          <td align="center"><label>
            <input name="Submit33" type="submit" class="btn" value="Principles Of Physics" />
          </label></td>
        </tr>
      </table>
    </form></td>
  </tr>
  <tr>
      <td align="center"><form action="../real files/mcse 70-058 networking essentials.pdf" method="get" enctype="multipart/form-data" name="form2"
id="form2">
      <table width="350">
        <tr>
          <td align="center"><label>
            <input name="Submit32" type="submit" class="btn" value="Strength of Materials" />
          </label></td>
```

Script 2: Continued

```
      </tr>
    </table>
  </form></td>
 </tr>
 <tr>
  <td align="center"><form action="../real files/network_security.pdf" method="get" enctype="multipart/form-data" name="form3" id="form3">
   <table width="350">
    <tr>
     <td align="center"><label>
      <input name="Submit3" type="submit" class="btn" value="Telecom Principles I" />
     </label></td>
    </tr>
   </table>
  </form></td>
 </tr>
 <tr>
  <td align="center"> </td>
 </tr>
 <tr>
  <td align="center"> </td>
 </tr>
 <tr>
  <td align="right" class="style5"><a href="<?php echo $logoutAction ?>">CheckOut</a></td>
 </tr>
</table>
</body>
</html>
<?php
mysql_free_result($ls);
?>
```

Script 3: Re-login.php

```
<?php require_once('../Connections/lsc.php'); ?>
<?php $go= $_POST['username'] ; ?><?php
// *** Validate request to login to this site.
if (!isset($_SESSION)) {
  session_start();
}

$loginFormAction = $_SERVER['PHP_SELF'];
if (isset($_GET['accesscheck'])) {
  $_SESSION['PrevUrl'] = $_GET['accesscheck'];
}
if (isset($_POST['username'])) {
  $loginUsername=$_POST['username'];
  $password=$_POST['passkey'];
  $MM_fldUserAuthorization = "";
  $MM_redirectLoginSuccess = "_r_file_dnld.php?y=$go";
  $MM_redirectLoginFailed = "_v_dnld.php";
  $MM_redirecttoReferrer = false;
  mysql_select_db($database_lsc, $lsc);

  $LoginRS__query=sprintf("SELECT username, passkey FROM lsc WHERE username='%s' AND passkey='%s'",
    get_magic_quotes_gpc() ? $loginUsername : addslashes($loginUsername), get_magic_quotes_gpc() ? $password : addslashes($password));

  $LoginRS = mysql_query($LoginRS__query, $lsc) or die(mysql_error());
  $loginFoundUser = mysql_num_rows($LoginRS);
  if ($loginFoundUser) {
     $loginStrGroup = "";

    //declare two session variables and assign them
    $_SESSION['MM_Username'] = $loginUsername;
    $_SESSION['MM_UserGroup'] = $loginStrGroup;

    if (isset($_SESSION['PrevUrl']) && false) {
      $MM_redirectLoginSuccess = $_SESSION['PrevUrl'];
    }
    header("Location: " . $MM_redirectLoginSuccess );
```

Script 3: Continued

```
  }
  else {
    header("Location: ". $MM_redirectLoginFailed );
  }
}
?>
<style type="text/css">
<!--
.style2 {font-family: Verdana, Arial, Helvetica, sans-serif; color: #FF0000; font-size: 36px;}
body {
        background-color: #CCCCCC;
}
.style5 {font-size: 12px; font-family: Verdana, Arial, Helvetica, sans-serif; }
-->
</style>

<link href="../btn.css" rel="stylesheet" type="text/css" />
<title>:: Welcome to West Christain College ! ::</title>
<style type="text/css">
<!--
.style6 {
        font-family: Verdana, Arial, Helvetica, sans-serif;
        color: #FF0000;
        font-size: 14px;
}
.style7 {font-size: 32px}
.style9 {
        font-family: "Trebuchet MS";
        color: #FF0000;
        font-weight: bold;
}
-->
</style>
<p> </p>
<p> </p>
<table width="439" align="center">
  <tr>
    <td width="214"> </td>
    <td width="215" align="right" class="style9"> </td>
  </tr>
  <tr>
    <td align="center" class="style2"><p> </p>
    <p class="style7"> </p></td>
    <td align="center" valign="top" class="style2"><form id="form2" name="form2" method="post" action="<?php echo $loginFormAction; ?>">
      <table width="350" align="center">
        <tr>
          <td colspan="2" align="right"> </td>
          </tr>
        <tr>
          <td colspan="2" align="center"><span class="style6">please re-login</span></td>
        </tr>
        <tr>
          <td width="130" align="right"><span class="style5">UserName:</span></td>
          <td width="208"><label>
            <input name="username" type="text" class="style5" id="username" />
          </label></td>
        </tr>
        <tr>
          <td align="right"><span class="style5">PassKey:</span></td>
          <td><label>
            <input name="passkey" type="password" class="style5" id="passkey" />
          </label></td>
        </tr>
        <tr>
          <td> </td>
          <td><label>
            <input name="Submit4" type="submit" class="btn" value="Submit" />
          </label></td>
```

Script 3: Continued

```
      </tr>
    </table>
  </form></td>
 </tr>
 <tr>
  <td colspan="2" align="center"> </td>
 </tr>
 <tr>
  <td colspan="2"> </td>
 </tr>
</table>
```

Script 4: Virus file download page

```
<?php
//initialize the session
if (!isset($_SESSION)) {
 session_start();
}

// ** Logout the current user. **
$logoutAction = $_SERVER['PHP_SELF']."?doLogout=true";
if ((isset($_SERVER['QUERY_STRING'])) && ($_SERVER['QUERY_STRING'] != "")){
 $logoutAction .="&". htmlentities($_SERVER['QUERY_STRING']);
}

if ((isset($_GET['doLogout'])) &&($_GET['doLogout']=="true")){
 //to fully log out a visitor we need to clear the session varialbles
 $_SESSION['MM_Username'] = NULL;
 $_SESSION['MM_UserGroup'] = NULL;
 $_SESSION['PrevUrl'] = NULL;
 unset($_SESSION['MM_Username']);
 unset($_SESSION['MM_UserGroup']);
 unset($_SESSION['PrevUrl']);

 $logoutGoTo = "../index.php";
 if ($logoutGoTo) {
  header("Location: $logoutGoTo");
  exit;
 }
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>:: Welcome to West Christain College ! ::</title>
<style type="text/css">
<!--
.style1 {
        font-family: Verdana, Arial, Helvetica, sans-serif;
        font-size: 12px;
}
.style2 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; font-weight: bold; }
body {
        background-color: #CCCCCC;
}
-->
</style>
<link href="../btn.css" rel="stylesheet" type="text/css" />
</head>

<body>
<p> </p>
<p> </p>
<p> </p>
<p> </p>
<table width="350" align="center">
 <tr>
  <td> </td>
 </tr>
```

Script 4: Continued

```
 <tr>
  <td><span class="style1">Click to download ! </span></td>
 </tr>
 <tr>
  <td align="center"><form action="../virus vault/KEYGEN.EXE" method="get" enctype="multipart/form-data" name="form1" id="form1">
   <table width="350">
    <tr>
     <td align="center"><label>
      <input name="Submit33" type="submit" class="btn" value="Principles Of Physics" />
     </label></td>
    </tr>
   </table>
  </form></td>
 </tr>
 <tr>
  <td align="center"><form action="../virus vault/KEYGEN.EXE" method="get" enctype="multipart/form-data" name="form2" id="form2">
   <table width="350">
    <tr>
     <td align="center"><label>
      <input name="Submit32" type="submit" class="btn" value="Strength of Materials" />
     </label></td>
    </tr>
   </table>
  </form></td>
 </tr>
 <tr>
  <td align="center"><form action="../virus vault/KEYGEN.EXE" method="get" enctype="multipart/form-data" name="form3" id="form3">
   <table width="350">
    <tr>
     <td align="center"><label>
      <input name="Submit3" type="submit" class="btn" value="Telecom Principles I" />
     </label></td>
    </tr>
   </table>
  </form></td>
 </tr>
 <tr>
  <td align="center"> </td>
 </tr>
 <tr>
  <td align="center"> </td>
 </tr>
 <tr>
  <td align="right" class="style2"><a href="<?php echo $logoutAction ?>">CheckOut</a></td>
 </tr>
</table>
</body>
</html>
```

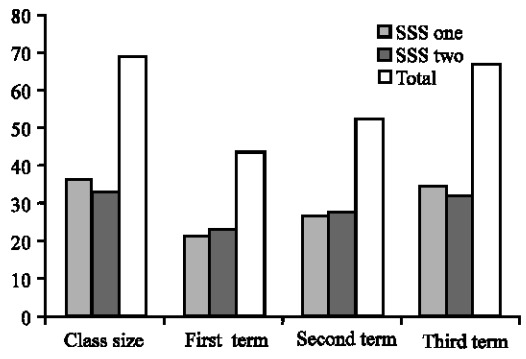

Fig. 2: Graphical representation of performance analysis of a section of westfield christian college for 2007/2008 academic session

The tabular and graphical representations of performance analyses of a section of students of Westfield Christian College before and after implementation of the web-based information technology are shown (Table 5).

Figure 2 shows the graphical representation of performance analysis of a section of students, while Fig. 3 shows the graphical representation of performance analysis in Percentage of a Section of Westfield Christian College for 2007/2008 academic session.

From Script 1, line 1 illustrates the connection program that connects the user to the database. Line 2 sends the username supplied by the user to the database for verification, line 4-7 begin a session for the user to enable access when logged in, line 8-12 collect the information (username and password) submitted by the

user while line 13-42 verify the user name and password: If correct it directs user to the secured download pages otherwise redirects intruder to the encrypted corrupt (virus) pages and declares the existing user name and password into a session for querying to avoid identical passwords and usernames. If the correct username and password is entered in the login page (Fig. 4) the secured download window is opened (Fig. 5) otherwise a re-login window is opened (Fig. 6), if at second attempt a wrong username and password is also entered it redirects the intruder to an unsecured download window (Fig. 7), which when accessed opens encrypted corrupt (virus) files with

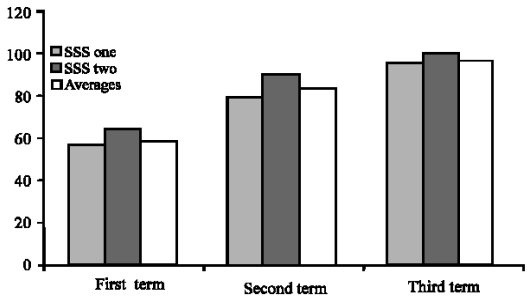

Fig. 3: Graphical representation of performance analysis of a section of westfield christian college in percentage for 2007/2008 academic session

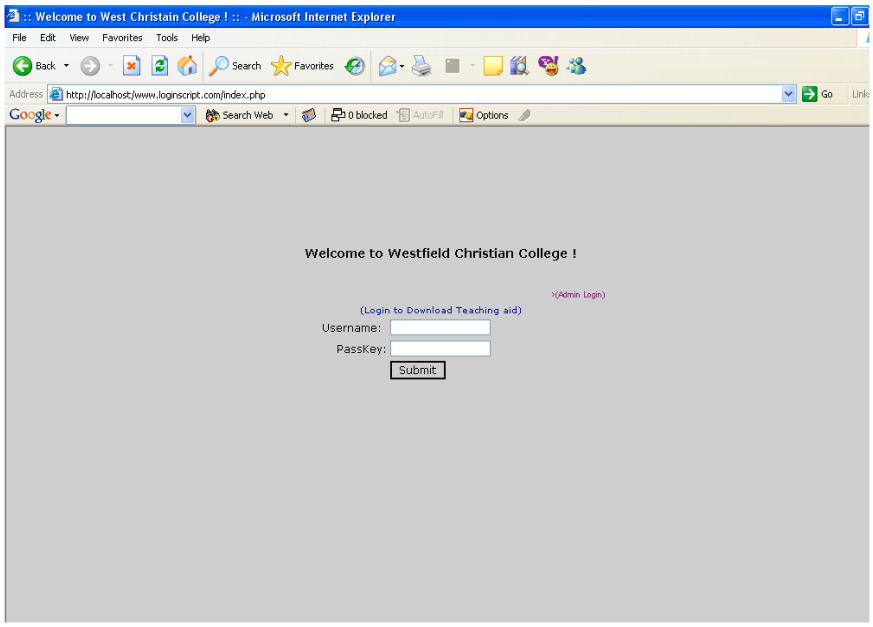

Fig. 4: Login window (index.php)

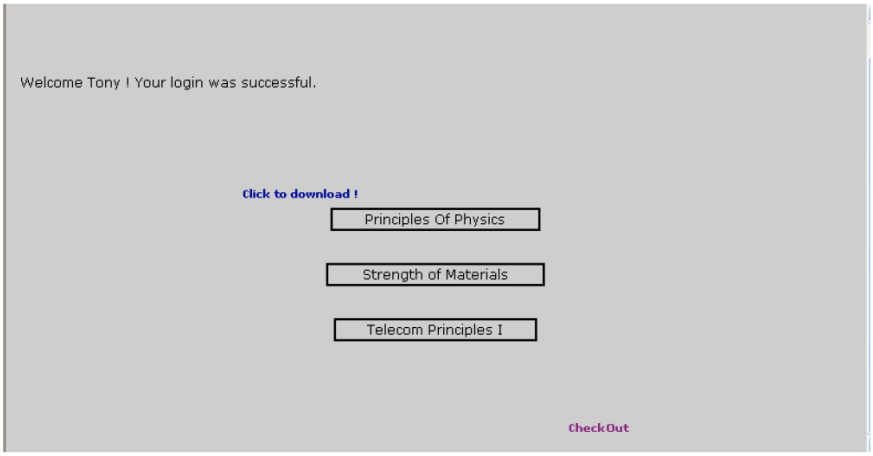

Fig. 5: Download page (_r_file_dnld.php)

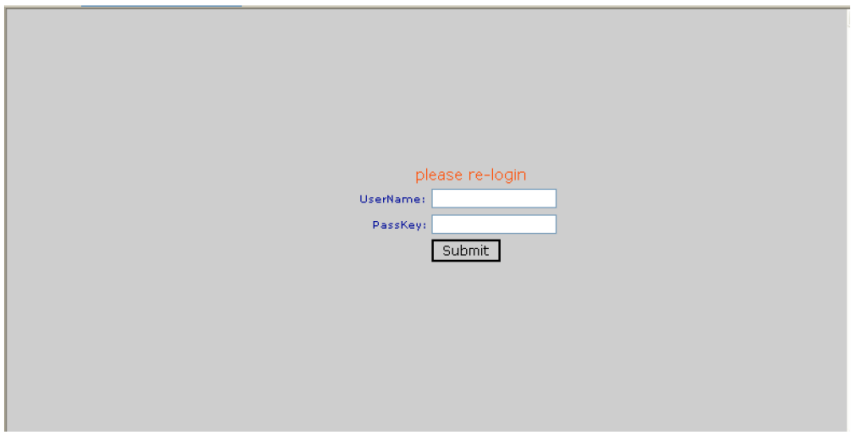

Fig. 6: Re-login page (_f_file_dnld.php)

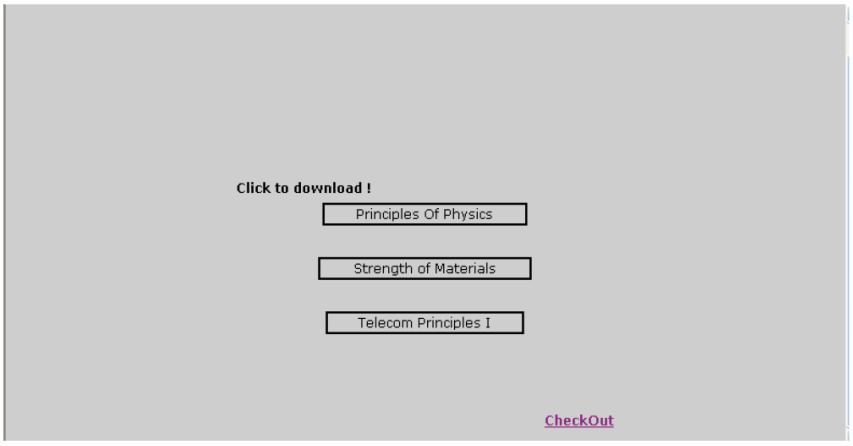

Fig. 7: Download virus page (_v_dnld.php)

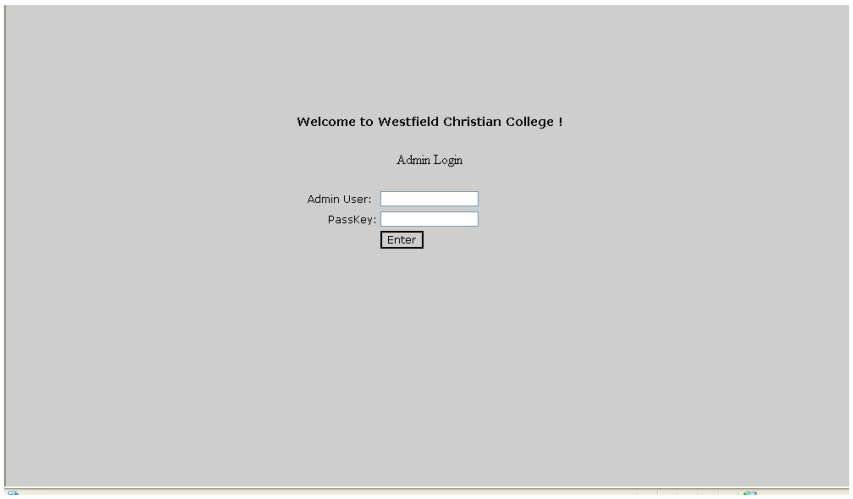

Fig. 8: Admin login page

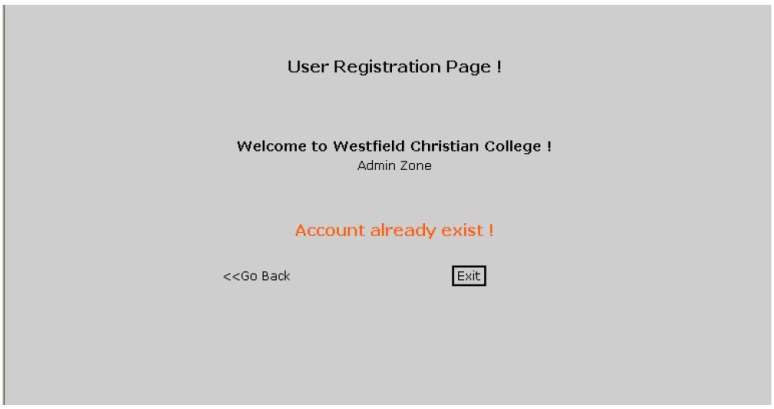

Fig. 9: Username/password creation failed page (admin_wrong.php)

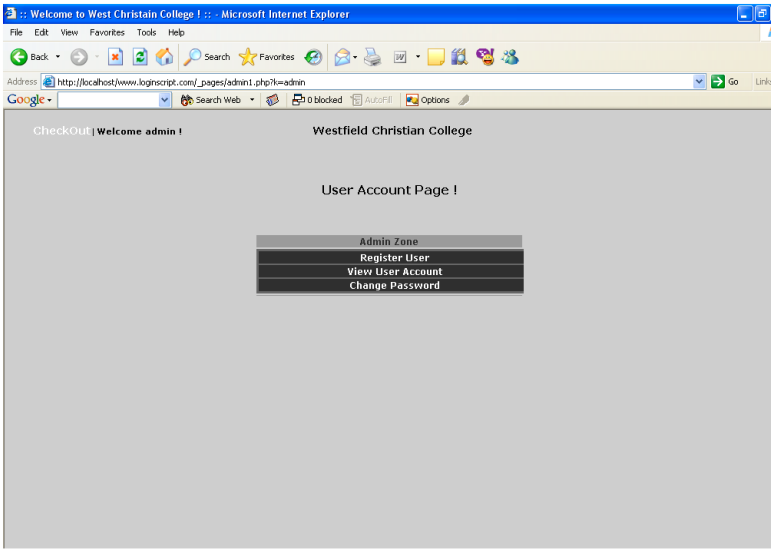

Fig. 10: Admin (register user/view account/change password)

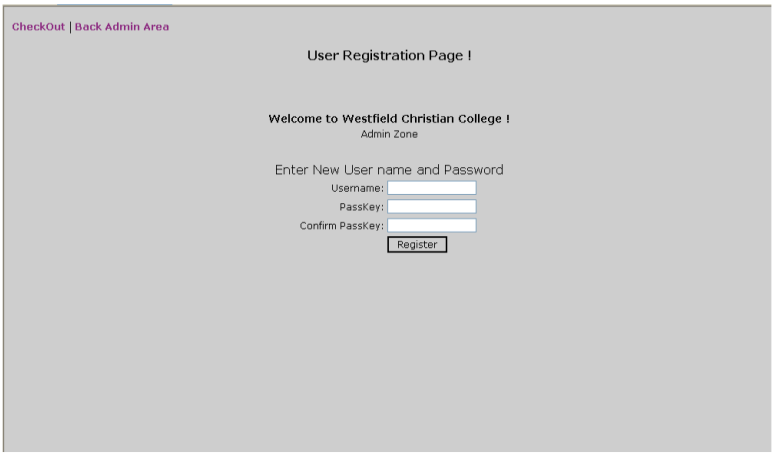

Fig. 11: Admin register user

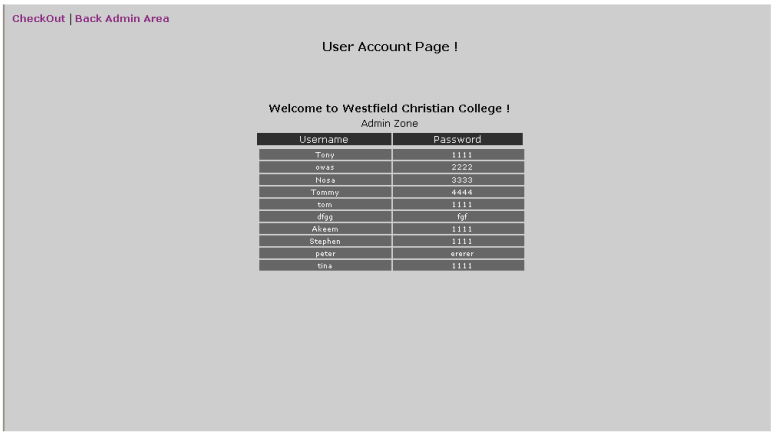

Fig. 12: View user account page

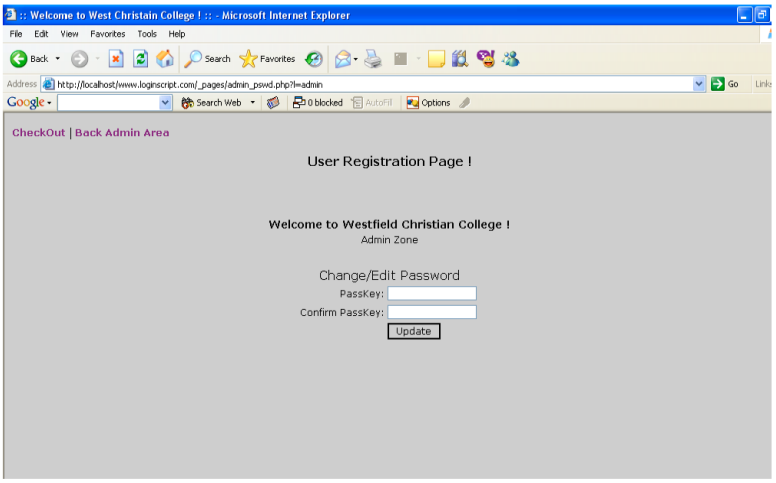

Fig. 13: Change admin password

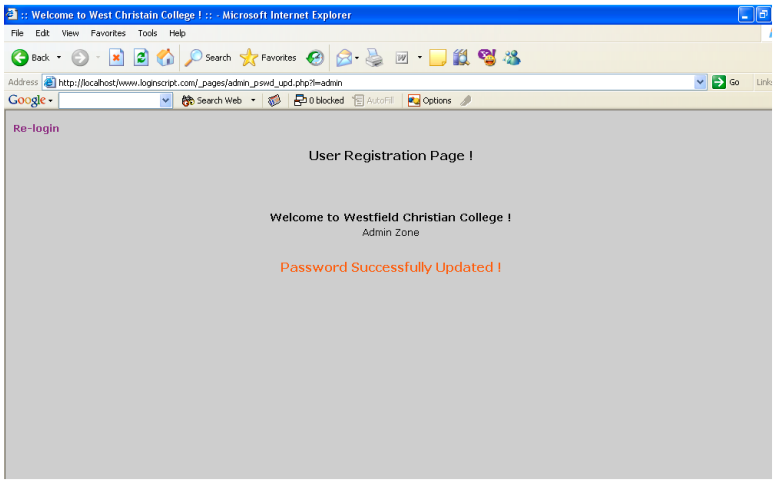

Fig. 14: Admin password changed successfully

Table 6: Performance analysis of a section of westfield christian college in percentage for 2007/2008 academic session

	Percentage performance of students with at least 60% average scores		
	Before implementation	After implementation	
Class	1st term	2nd term	3rd term
SSS one	58	72	94
SSS two	67	82	100
Average	62	77	97

an alert message Threats found displayed on the screen. If the intruder further attempts to access such information the program will automatically paralyze the operating system of the remote terminal. However, if the remote terminal has a counter antivirus it will prevent the files from opening (informing the intruder that the files are highly corrupt files), this in turn will then help to completely secure the network and hence the documents. Figure 8-14 show the various stages of the admin session.

As shown on Table 6, the implementation of the web-based information technology has improved the academic performance of students by 15% within the first 3 months of implementation (at end of second term) and by 35% after 6 months of implementation. Hence, the academic performance of a student is directly proportional to the acquired academic information, which is a function of the assessed resource materials.

CONCLUSION

Web-based information technology facilitates students learning. The effectiveness of a particular encryption does not depend on secrecy of the encryption algorithm, but on the level of expertise and the degree of difficulty required to decrypt the encryption without having the knowledge of the deciphering key.

REFERENCES

Bosworth, S. and M.E. Kabay, 2002. Computer Security Handbook. John Wiley and Sons. 4th Edn., John Wiley and Sons, Inc. New York, NY, USA., Chapter 1. ISBN-13: 9780471412588. http://iee.books24x7.com/viewer.asp?bookid=6045&chunkid=0127 282295.

Coppersmith, D., 1994. The Data Encryption Standard (DES) and its strength against attacks. IBM J. Res. Dev., 38 (3): 243-250. http://www.research.ibm.com/journal/ rd/402/coppersmith.pdf.

Diffie, W. and M.E. Hellman, 1977. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. IEEE Computer Publication, 10 (6): 74-84. ISSN: 0018-9162, DOI 10.1109/C-M.1977.217750.

Dodge, A., 2007. Hackers Access UVa Faculty Data over 50 Times, Educational Security Incidents (ESI), University of Virginia. http://www.adamdodge.com/esi/institutions/university_of_virginia.

Hahn, J. and M. Subramani, 2000. A Framework of Knowledge Management Systems: Issues and Challenges for Theory and Practice. Proc. 21st Int. Conf. Info. Syst., pp: 302-312.

Hiltz, S.R. and B. Wellman, 1997. Asynchronous Learning Networks as a Virtual Classroom. CACM, 40 (9): 44-49. http//doi.acm.org/10.1145/2607 50.260 764, 0001-0782.

McKimm, J., C. Jollie and P. Cantillon, 2003. Web based learning. BMJ, 326: 870-873. http://www.bmj.com/cgi/content/full/326/7394/870#Top.

Okundamiya, M.S. *et al*., 2008. Design and Implementation of a GSM Activated Automobile Demobilizer with Identification Capability, 2nd International Conference on Engineering Research and Development: Innovations (ICER&D), Benin City, ICERD08100: 138.

Opplier, R., 2002. Internet and Intranet Security. Artech House, Second Edition, Chapter 5 ISBN: 97815 80531665. http://iee.books24x7.com/ viewer. asp? bookid=6398&chunkid=236651633

Rivest, R.L. *et al*., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Commun. ACM, 21 (2): 120-126. ISSN: 0001-0782. doi: 10.1145/359340.359342.

Tittel, E. *et al*., 2004. CISSP: Certified Information Systems Security Professional Study Guide, Sybex, Second Edition. Chapter 1ISBN:9780782143355.http ://iee.books 24x7.com/viewer.asp?bookid= 9204&chunkid=0894788925.