

العنوان:	تصميم بريد إلكتروني آمن
المؤلف الرئيسي:	أبو يوسف، مها
مؤلفين آخرين:	أحمد، عوض حاج علي(مشرف)
التاريخ الميلادي:	2015
موقع:	الخرطوم
الصفحات:	1 - 378
رقم MD:	831143
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة النيلين
الكلية:	كلية الدراسات العليا
الدولة:	السودان
قواعد المعلومات:	Dissertations
مواضيع:	البريد الإلكتروني
رابط:	<a href="http://search.mandumah.com/Record/831143">http://search.mandumah.com/Record/831143</a>



جامعة المنيا

كلية الدراسات العليا

بحث لنيل درجة الدكتوراة في علوم الحاسوب

بعنوان :

# تصميم بريد الكترونى آمن

إشراف :

إعداد:

البروفيسور : عوض حاج علي احمد

مها أبو يوسف أبو

ديسمبر 2015م

# الآية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

أَقْرَأُ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ (1) خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ (2)  
أَقْرَأُ وَرَبُّكَ الْأَكْرَمُ (3) الَّذِي عَلَّمَ بِالْقَلَمِ (4) عَلَّمَ الْإِنْسَانَ مَا  
لَمْ يَعْلَمْ (5)

صَدَقَ اللَّهُ الْعَظِيمُ

سورة العلق الآيات (1-5)

# الإهداء

إلهى لا يطيب الليل الا بذكرك ... ولا يطيب النهار الا بطاعتك ... ولا تطيب الآخرة الا بعفوك ... ولا تطيب الجنة الا برويتك.... الله جل جلالك

إلى من بلغ الرسالة ... وأدى الامانة ... ونصح الامة ... الى نبي الرحمة ونور العالمين .... سيدنا محمد صلى الله عليه وسلم

إلى من كلفه الله بالهبة والوقار ... إلى من علمنى العطاء بدون إنتظار ... إلى من أحمل اسمه بكل افتخار... والدى العزيز

إلى من بها اكبر وعليها اعتمد ... إلى الشمعة المتقدة التى تثير ظلمة حياتى ... إلى من بوجودها أكتسب قوة ومحبة لا حدود لها ... إلى من عرفت معها معنى الحياة ... امى الحبيبة

إلى من تميزوا بالعطاء والوفاء ... إلى ينابيع الصدق الصافى .... إلى من كانوا معى على دروب الحياة الحلوة والمرة ... أخوانى وأخواتى

إلى من وقفوا بجانبى وتحلوا بالصبر معى .... إلى من كانوا بجانبى على طريق النجاح والخير.... زوجى وأبنائى

إلى من عرفت كيف اجدهم .... وجمعتنى بهم الحياة .... وعلمونى الا أضيعهم .... زملائى وزميلاتى بجامعة النيلين

الباحث

# الشكر والعرفان

أولاً أشكر الله تعالى أن مدنى بالقوة والعزيمة لإكمال هذه الرسالة . ثانياً

الشكر للبروفسيور عوض حاج علي على إشرافه على رسالتى.

الشكر كل الشكر لزملائى بجامعة النيلين كلية علوم الحاسوب وتقانة

المعلومات.

ومن الشكر أجزله وأعمقه لأسرتى الصغيرة زوجى وأبنائى وأسرتى الكبيرة

أمى وأبى وإخوتى لتشجيعهم الدائم لى ومساندتهم لى لإنجاز هذا العمل.

الباحث

# مستخلص الدراسة

ان البريد الالكتروني كخدمة من الخدمات التي توفرها شبكة الانترنت صار من وسائل الاتصال السريعة والسهلة بين مستخدمي الحاسوب، ونجد ان بعض الرسائل المرسله عبر البريد الالكتروني تحتاج الى درجة خاصة من السرية ولاسيما ان شبكة الانترنت مع انتشار الوسائل التقنية الحديثة تعتبر ثرية بالماهجين و المتلصين.

تهدف الدراسة الى انشاء بريد الكتروني وتزويده بالامان. اذ يمكن للمستخدم فتح حساب كعضو في النظام وبعد ذلك يمكن للمرسل من خلال النظام انشاء بريد الكتروني ثم تشفيره وارساله الى المستقبل، كما يمكن للمستقبل اختيار الرسالة وفتحها وهي مشفرة ثم فك تشفيرها.

وقد استخدمنا خوارزمية الجودة العالية المستوى كاداة للسرية والأمن. تمتلك هذه الخوارزمية مناعة عالية ضد المهاجمين. إذ تتكون من اربعة خوارزميات هي: دالة تمويه لانشاء التوقيع الالكتروني، خوارزمية تشفير غير متماثل لانشاء المفاتيح، خوارزمية تشفير متماثل لتشفير الرسالة بمفتاح الجلسة، وخوارزمية لضغط الرسائل. تم استخدام خوارزميات محددة لما بها من مزايا في مجال علم التشفير وهي MD5 كدالة تمويه ، RSA في التشفير الغير متماثل، AES في التشفير المتماثل، و (Lempel-Ziv 1977 (LZ77 كخوارزمية ضغط . وذلك بعد ان تمت مقارنة الخوارزميات اعلاه مع مجموعة من الخوارزميات واثبتت سرعتها وقوتها.

ومن اهم التوصيات التي خرج بها الباحث يوصى الباحث باضافة ملصقات (Attachment) تشفير وترسل مع الرسالة في جانب المرسل ، ويفك تشفيرها في جانب المستقبل وان كانت ملفات صوت او صور او

ففيديو. وكذلك تقوية بروتوكول توزيع المفاتيح العامة بسبب تزايد عددها و حل مشكلة الـ (spam) والتي  
يعانى منها البريد الالكترونى بجامعة النيلين.

وقد تم بناء النظام بلغة PHP و Bootstrap و MySQL .

# Abstract

An E-mail as an internet service become easy and quick way around computer users. Some E-mails needs more security against hackers.

The aim of this study construct a secure E-mail system protected with pretty good privacy algorithm.

In this study, we have constructed a secure mailing system. The user can create a count create account in the system after that he can make a message, encrypt then transmit it to the receiver. The receiver can select the message, decrypt it.

The Pretty Good Privacy (PGP) algorithm is used as a tool to provide secrecy. This algorithm possesses high quality against hackers. It contains four cryptographic functions which they are hash function to create the digital signature, asymmetric coding algorithm for constructing the keys, symmetric coding algorithm to encode the message with the session key, and a file compression algorithm to compress the size of the message.

We have used algorithms that has special function in the science of cryptography such as Sevure Hash Algorithm (SHA-1) as hash function, RSA for Asymmetric encryption, AES for Symmetric encryption, and Lempel-Ziv 1977 (LZ77) for Compression after comparing them with another algorithm and they proved their speed and strength.



We construct the system using PHP language, bootstrap and MySQL.

## فهرس الموضوعات

الصفحة	الموضوع	الرقم
أ	الآية	
ب	الإهداء	
ج	الشكر والعرفان	
د	ملخص الرسالة	
و	Abstract	
ز	فهرس الموضوعات	
ف	فهرس الأشكال	
ض	فهرس الجداول	
ظ	فهرس الاختصارات	
أأ	فهرس الرموز	
<b>الفصل الأول : المقدمة</b>		
1	مقدمة	1-1
2	مشكلة الدراسة	2-1
3	أهداف الدراسة	3-1
3	الدراسات السابقة	4-1

3	الهيكل العام للدراسة	5-1
<b>الفصل الثاني : أمن المعلومات والتشفير</b>		
6	امن المعلومات	1-2
6	مقدمة عن أمن المعلومات	1-1-2
7	تعريف أمن المعلومات	2-1-2
8	المخاطر و الإعتداءات في بيئة المعلومات	3-1-2
8	تحليل العوامل المهددة لأمن الأنظمة الآلية للمعلومات	4-1-2
9	خطط أمن البيانات	5-1-2
10	مكونات أمن المعلومات	6-1-2
12	التشفير	2-2
12	نبذة تاريخية	1-2-2
12	تعريف	2-2-2
13	الأخطار التي يجب التغلب عليها بواسطة التشفير	3-2-2
14	أهداف التشفير	4-2-2
15	أنظمة التشفير	5-2-2
15	التشفير بالطرق الكلاسيكية	1-5-2-2
15	شفرات الاحلال	1-1-5-2-2

16	شفرات الابدال	2-1-5-2-2
16	طرق التشفير الحديثة	2-5-2-2
17	التشفير بالمفتاح المتناظر	1-2-5-2-2
18	شفرات الكتل	1-1-2-5-2-2
18	شفرات التدفق	2-1-2-5-2-2
19	فوائد انظمة التشفير التناظري	3-1-2-5-2-2
19	مساوى انظمة التشفير التناظري	4-1-2-5-2-2
20	التشفير بالمفتاح الغير متناظر (العام)	2-2-5-2-2
22	فوائد انظمة تشفير المفتاح العام	1-2-2-5-2-2
22	مساوى انظمة تشفير المفتاح العام	2-2-2-5-2-2
23	خوارزمية معيار التشفير المتقدم AES	6-2-2
23	طريقة عمل خوارزمية معيار التشفير المتقدم AES	1-5-2-2
28	مميزات وعيوب خوارزمية معيار التشفير المتقدم AES	2-6-2-2
29	خوارزمية تشفير البيانات المعيارية DES	7-2-2
29	طريقة عمل خوارزمية تشفير البيانات المعيارية DES	1-7-2-2
42	مميزات وعيوب خوارزمية تشفير البيانات المعيارية DES	2-7-2-2
43	خوارزمية تشفير البيانات المعيارية الثلاثية 3DES	8-2-2

43	طريقة عمل خوارزمية تشفير البيانات المعيارية الثلاثية 3DES	1-8-2-2
44	مميزات وعيوب خوارزمية تشفير البيانات المعيارية الثلاثية 3DES	2-8-2-2
45	خوارزمية Rivets Cipher 4 (RC4)	9-2-2
46	طريقة عمل خوارزمية RC4	1-9-2-2
48	مميزات وعيوب خوارزمية RC4	2-9-2-2
48	المقارنة بين الخوارزميات التناظرية AES, DES, 3DES, RC4	10-2-2
49	خوارزمية RSA	11-2-2
50	طريقة عمل خوارزمية RSA	1-11-2-2
53	مميزات وعيوب خوارزمية RSA	2-11-2-2
54	خوارزمية الجمال Elgamal	12-2-2
54	طريقة عمل خوارزمية الجمال Elgamal	1-12-2-2
56	مميزات وعيوب خوارزمية Elgamal	3-12-2-2
56	المقارنة بين خوارزميتي RSA و Elgamal	13-2-2
57	تحليل الشفرات	14-2-2
59	متطلبات السرية	1-14-2-2
60	طول المفتاح وقوة الشفرة	2-14-2-2
60	أمنية الخوارزميات	15-2-2

61	ضغط البيانات	3-2
61	تعريف	1-3-2
63	أهداف ضغط البيانات	2-3-2
64	مشاكل ضغط البيانات	3-3-2
64	تصنيف طرق الضغط	4-3-2
64	خوارزميات الضغط الفاقدة	1-4-3-2
65	خوارزميات الضغط الغير فاقدة	2-4-3-2
66	مقياس جودة الضغط	5-3-2
68	خوارزمية LZ77	6-3-2
68	طريقة عمل خوارزمية LZ77	1-6-3-2
70	مميزات وعيوب خوارزمية LZ77	2-6-3-2
70	خوارزمية هوفمان Huffman	7-3-2
71	طريقة عمل خوارزمية Huffman	1-7-3-2
74	مميزات وعيوب خوارزمية هوفمان Huffman	2-7-3-2
75	الدوال الهاشمية	4-2
75	تعريف	1-4-2
76	خواص الدالة الهاشمية	2-4-2

77	استخدامات الدالة الهاشمية	3-4-2
79	خوارزمية (MD5) Message Digest	4-4-2
79	طريقة عمل خوارزمية MD5	1-4-4-2
83	مميزات وعيوب خوارزمية MD5	2-4-4-2
83	خوارزمية (SHA-1) Secure Hash Algorithm	5-4-2
84	طريقة عمل خوارزمية SHA-1	1-5-4-2
87	مميزات وعيوب خوارزمية SHA-1	2-5-4-2
88	المقارنة بين الدوال الهاشمية MD5 , SHA-1	6-4-2
88	خوارزمية الجودة عالية المستوى	5-2
88	لمحة تاريخية	1-5-2
89	تعريف	2-5-2
90	تحليل مكونات خوارزمية الجودة عالية المستوى	3-5-2
90	السرية فى خوارزمية الجودة عالية المستوى	1-3-5-2
92	التحقق من صحة المصدر فى خوارزمية الجودة عالية المستوى	2-3-5-2
93	ضغط البيانات فى خوارزمية الجودة عالية المستوى	3-3-5-2
94	عملية الارسال	4-5-2
96	عملية الاستقبال	5-5-2

الفصل الثالث : تحليل اختراقات البريد الإلكتروني وطرق تأمينه

99	القرصنة الالكترونية	1-3
99	مقدمة	1-1-3
99	تاريخ القرصنة	2-1-3
101	تصنيف قرصنة المعلومات	3-1-3
102	أشكال القرصنة	4-1-3
103	الأسباب التي تدفع إلى ارتكاب جرائم القرصنة المعلوماتية	5-1-3
104	طرق اختراق الحاسوب	6-1-3
106	جرائم الاختراقات عبر الانترنت	7-1-3
109	ضعف شبكة الانترنت فى حماية اجهزة المستخدمين	8-1-3
110	مخاطر الانترنت الامنية	9-1-3
112	الوسائل المتبعة للحد من مخاطر الانترنت	10-1-3
113	البريد الالكترونى	2-3
113	مقدمة	1-2-3
113	تعريف	2-2-3
114	مميزات البريد الالكترونى	3-2-3



115	طريقة عمل البريد الالكتروني	4-2-3
117	تكاملية البريد الالكتروني	1-4-2-3
118	تجزئة رسالة البريد الالكتروني	2-4-2-3
118	أنواع البريد الالكتروني	5-2-3
120	الأخطار التي تكتنف استعمال البريد الالكتروني	6-2-3
122	أساليب وطرق اختراق البريد الإلكتروني	7-2-3
124	أمن وحماية البريد الالكتروني	8-2-3
125	حماية البريد الإلكتروني من الاختراق أو السرقة	1-8-2-3
125	حماية البريد الالكتروني من التنصت	2-8-2-3
128	إستخدام حساب بريد الكتروني آمن	3-8-2-3
130	زيادة خصوصية التراسل بالبريد الإلكتروني	9-2-3
132	خوارزميات التشفير المستخدمة لحماية البريد الالكتروني	10-2-3
134	شركة Microsoft وأمن البريد الالكتروني	11-2-3
136	نظام البريد الالكتروني الحالي	3-3
136	طريقة حماية البريد الالكتروني الحالي	1-3-3
136	طريقة عمل خوارزمية الـ PGP التجارية	2-3-3

137	مميزات خوارزمية او نظام ال PGP	3-3-3
138	عيوب وثغرات خوارزمية او نظام ال PGP	4-3-3
139	الحل المقترح	4-3
139	تطوير خوارزمية ال PGP	1-4-3
140	الخوارزمية التناظرية المستخدمة فى بناء ال PGP	1-1-4-3
143	الخوارزمية العامة المستخدمة فى بناء ال PGP	2-1-4-3
146	الدالة الهاشية المستخدمة فى بناء ال PGP	3-1-4-3
149	خوارزمية الضغط المستخدمة فى بناء ال PGP	4-1-4-3
153	خطوات تطوير خوارزمية PGP للتشفير	2-4-3
154	خطوات تطوير خوارزمية PGP لفك التشفير	3-4-3
155	أمنية النظام المقترح	4-4-3
<b>الفصل الرابع : التصميم</b>		
156	وصف تصميم النظام	1-4
157	تصميم الشاشات	2-4
157	تصميم الشاشات باللغة الانجليزية	1-2-4
161	تصميم شاشات المدير	1-1-2-4
184	تصميم شاشات المستخدم	2-1-2-4

203	تصميم الشاشات باللغة العربية	2-2-4
207	تصميم شاشات المدير	1-2-2-4
230	تصميم شاشات المستخدم	2-2-2-4
<b>الفصل الخامس : التنفيذ</b>		
249	وصف تنفيذ النظام	1-5
250	تنفيذ الشاشات	2-5
250	تنفيذ الشاشات باللغة الانجليزية	1-2-5
259	تنفيذ شاشات المدير	1-1-2-5
273	تنفيذ شاشات المستخدم	2-1-2-5
285	تنفيذ الشاشات باللغة العربية	2-2-5
294	تنفيذ شاشات المدير	1-2-2-5
308	تنفيذ شاشات المستخدم	2-2-2-5
<b>الفصل السادس : الخاتمة والنتائج والتوصيات</b>		
320	الخاتمة	1-6
321	النتائج	1-6
323	التوصيات	3-6

324	المصادر والمراجع	4-6
-----	------------------	-----

## فهرس الأشكال

17	الشكل (1-2) يوضح التشفير وفك التشفير بالمفتاح المتناظر
21	الشكل (2-2) يوضح التشفير و فك التشفير بالمفتاح غير المتناظر
24	الشكل (3-2) يوضع الشكل العام لخوارزمية معيار التشفير المتقدم AES
26	الشكل (4-2) يوضع عملية الاستبدال في خوارزمية معيار التشفير المتقدم AES
27	الشكل (5-2) يوضع عملية ازاحة الصفوف في خوارزمية معيار التشفير المتقدم AES
27	الشكل (6-2) يوضع عملية خلط الاعمدة في خوارزمية معيار التشفير المتقدم AES
28	الشكل (7-2) يوضع عملية اضافة المفتاح في خوارزمية معيار التشفير المتقدم AES
30	الشكل (8-2) يوضح دوال توليد المفتاح لخوارزمية DES
31	الشكل (9-2) يوضح عملية الازاحة لتوليد المفتاح في خوارزمية DES
33	الشكل (10-2) يوضح دوال التشفير في خوارزمية DES
44	الشكل (11-2) يوضح الشكل العام لخوارزمية 3DES
47	الشكل (12-2) يوضح خوارزمية (PRGA) المستخدمة في خوارزمية RC4
52	الشكل (13-2) يوضح المخطط الانسيابي لعملية التشفير في خوارزمية RSA
53	الشكل (14-2) يوضح المخطط الانسيابي لعملية فك التشفير في خوارزمية RSA
65	الشكل (15-2) يوضح خوارزميات الضغط الفاقدة

66	الشكل (2-16) يوضح خوارزميات الضغط الغير الفاعلة
68	الشكل ( 2-17) يوضح الشكل العام لخوارزمية LZ77
73	الشكل ( 2-18) يوضح شجرة هوفمان
80	الشكل (2-19) يوضح الهيكل العام لخوارزمية MD5
82	الشكل (2-20) يوضح معالجة كتل الرسالة لخوارزمية MD5
84	الشكل (2-21) يوضح الهيكل العام لخوارزمية SHA-1
87	الشكل (2-22) يوضح معالجة كتل الرسالة لخوارزمية SHA-1
91	شكل (2-23) يوضح السرية فى خوارزمية الجودة عالية المستوى
93	الشكل (2-24) يوضح عملية التحقق فى خوارزمية الجودة عالية المستوى
95	الشكل (2-25) يمثل مخطط انسيابى لتوضيح عملية الارسال فى خوارزمية الجودة عالية المستوى
97	الشكل (2-26) يمثل مخطط انسيابى لتوضيح عملية الاستقبال فى خوارزمية الجودة عالية المستوى
117	شكل (3-1) يوضح طريقة عمل البريد الالكترونى
142	الشكل (3-2) يوضح المقارنة بين زمن التنفيذ فى خوارزميات RC4 و DES و 3DES و AES
145	الشكل (3-3) يوضح المقارنة بين زمن التنفيذ فى خوارزميات RSA و Elgamal
148	الشكل (3-4) يوضح المقارنة بين زمن التنفيذ فى دالتى MD5 و SHA-1

151	الشكل (3-5) يوضح المقارنة بين حجم الملف بعد الضغط في خوارزميات Huffman و LZ77
152	الشكل (3-6) يوضح المقارنة بين نسبة الضغط في خوارزميات الضغط Huffman و LZ77
157	الشكل (4-1) يوضح تصميم الشاشة الرئيسية باللغة الانجليزية
159	الشكل (4-2) يوضح تصميم شاشة تسجيل مستخدم جديد
161	الشكل (4-3) يوضح تصميم الشاشة الرئيسية للمدير
163	الشكل (4-4) يوضح تصميم شاشة انشاء رسالة جديدة
165	الشكل (4-5) يوضح تصميم الرسالة المشفرة قبل ارسالها
167	الشكل (4-6) يوضح تصميم شاشة ارسال الرسالة المشفرة
168	الشكل (4-7) يوضح تصميم شاشة البريد الوارد
170	الشكل (4-8) يوضح تصميم الرسالة الواردة المشفرة
172	الشكل (4-9) يوضح تصميم شاشة الرسالة الواردة بعد فك تشفيرها
174	الشكل (4-10) يوضح تصميم شاشة الرسائل المحذوفة للمدير
176	الشكل (4-11) يوضح تصميم شاشة الاعضاء فى النظام
178	الشكل (4-12) يوضح تصميم شاشة حذف مستخدم من النظام
180	الشكل (4-13) يوضح تصميم شاشة الخصوصية
182	الشكل (4-14) يوضح تصميم شاشة المعلومات عن المالك للنظام
184	الشكل (4-15) يوضح تصميم الشاشة الرئيسية للمستخدم

186	الشكل (4-16) يوضح تصميم شاشة انشاء رسالة جديدة
188	الشكل (4-17) يوضح تصميم شاشة الرسالة المشفرة قبل ارسالها
190	الشكل (4-18) يوضح تصميم شاشة ارسال الرسالة المشفرة
191	الشكل (4-19) يوضح تصميم شاشة البريد الوارد
193	الشكل (4-20) يوضح تصميم شاشة الرسالة الواردة قبل فك تشفيرها
195	الشكل (4-21) يوضح تصميم شاشة الرسالة الواردة بعد فك تشفيرها
197	الشكل (4-22) يوضح تصميم شاشة الرسائل المحذوفة
199	الشكل (4-23) يوضح تصميم شاشة الخصوصية
201	الشكل (4-24) يوضح تصميم شاشة المعلومات عن المالك للنظام
203	الشكل (4-25) يوضح تصميم الشاشة الرئيسية باللغة العربية
205	الشكل (4-26) يوضح تصميم شاشة تسجيل مستخدم جديد
207	الشكل (4-27) يوضح تصميم الشاشة الرئيسية للمدير
209	الشكل (4-28) يوضح تصميم شاشة انشاء رسالة جديدة
211	الشكل (4-29) يوضح تصميم الرسالة المشفرة قبل ارسالها
213	الشكل (4-30) يوضح تصميم شاشة ارسال الرسالة المشفرة
214	الشكل (4-31) يوضح تصميم شاشة البريد الوارد
216	الشكل (4-32) يوضح تصميم الرسالة الواردة المشفرة



218	الشكل (4-33) يوضح تصميم شاشة الرسالة الواردة بعد فك تشفيرها
220	الشكل (4-34) يوضح تصميم شاشة الرسائل المحذوفة
222	الشكل (4-35) يوضح تصميم شاشة الاعضاء فى النظام
224	الشكل (4-36) يوضح تصميم شاشة حذف مستخدم من النظام
226	الشكل (4-37) يوضح تصميم شاشة الخصوصية
228	الشكل (4-38) يوضح تصميم شاشة المعلومات عن المالك للنظام
230	الشكل (4-39) يوضح تصميم الشاشة الرئيسية للمستخدم
232	الشكل (4-40) يوضح تصميم شاشة انشاء رسالة جديدة
234	الشكل (4-41) يوضح تصميم شاشة الرسالة المشفرة قبل ارسالها
236	الشكل (4-42) يوضح تصميم شاشة ارسال الرسالة المشفرة
237	الشكل (4-43) يوضح تصميم شاشة البريد الوارد
239	الشكل (4-44) يوضح تصميم شاشة الرسالة الواردة قبل فك تشفيرها
241	الشكل (4-45) يوضح تصميم شاشة الرسالة الواردة بعد فك تشفيرها
243	الشكل (4-46) يوضح تصميم شاشة الرسائل المحذوفة
245	الشكل (4-47) يوضح تصميم شاشة الخصوصية
247	الشكل (4-48) يوضح تصميم شاشة المعلومات عن المالك للنظام
250	الشكل (5-1) يوضح تنفيذ شاشة الدخول الرئيسية