

شرح الإختصارات

المعنى	الإختصارات
Public key Infrastructure	PKI
Certificate Authority	CA
Virtual Private Network	VPN
Confidentiality , Integrity , Availability	CIA
Registration Authority	RA
Certificate Revoked List	CRL
Hypertext Transfer Protocol	HTTP
Lightweight Directory Access Protocol	LDAP
Secure Socket Layer	SSL
International Telecommunication Union	ITU
secure/Multipurpose Internet Mail Extensions	S/MIME
Internet Protocol Security	IP SEC
Encrypting File System	EFS
Unified Modeling Language	UML
Active Server Pages	ASP
Personal Home Page	PHP
Object Oriented Programming	OOP
Extensible Markup Language	XML
Integrated Development Environment	IDE
Graphical User Interface	GUI
Hypertext Markup Language	HTML
Advanced Encryption Standard	AES
Data Encryption Standard	DES
Ron Rivest, Adi Shamir, and Len Adleman	RSA
Internet Information Services	IIS
Wide Area Network	WAN
Local Area Network	LAN
File Transfer Protocol	FTP
Network News Transfer Protocol	NNTP
Simple Mail Transfer Protocol	SMTP
Transmission Control Protocol/Internet Protocol	TCP/IP
Transport Layer Security	TLS
Online Certificate Status Protocol	OCSP
Internet Engineering task Force	IETF

فهرس الأشكال

رقم الصفحة	موضوع الشكل	رقم الشكل الباب/الشكل
12	يوضح عناصر توليد الشهادة	1.2
14	يوضح هرمية إعطاء الثقة	2.2
21	إرسال طلب شهادة والرد عليه	1.3
27	تقنية التوقيع الإلكتروني	2.3
42	طبقات بروتوكول SSL	1.5
46	خطوات المصافحة	2.5
48	عملية التشفير وفك التشفير باستخدام التشفير المُتمائل	3.5
49	عملية التشفير باستخدام التشفير غير المُتمائل	4.5
49	عملية فك التشفير باستخدام التشفير غير المُتمائل	5.5
67	نظام الصرافة	1.6
68	عملية الدخول للنظام	2.6
69	عملية إضافة عميل جديد	3.6
70	إجراء معاملة مصرفية	4.6
71	التأكد من إجراء معاملة مصرفية معينة	5.6
72	عملية إستخراج التقارير للمعاملات التي تمت	6.6
74	عمليات نظام الصرافة	7.6
77	واجهة الدخول للنظام	1.7
78	واجهة إضافة مستخدم جديد	2.7
79	مراجعة مدير النظام للعمليات والمستخدمين	3.7
80	واجهة المعاملات الصادرة	4.7
81	واجهة المعاملات الواردة	5.7
82	واجهة المعاملات اليومية	6.7
83	واجهة استخراج التقارير	7.7
84	واجهة مراجعة المستخدم للمعاملات التي تمت	8.7
85	واجهة المستخدم للمعاملات الصادرة	9.7
86	واجهة المستخدم للمعاملات الصادرة	10.7
87	واجهة المستخدم للمعاملات اليومية	11.7
88	واجهة المستخدم لاستخراج التقارير	12.7

فهرس المحتويات

رقم الصفحة	الموضوع	الباب
	مقدمة	الأول
1	1.1 مقدمة البحث
1	2.1 مشكلة البحث
2	3.1 أهداف البحث
2	4.1 أهمية البحث
2	5.1 حدود البحث
2	6.1 منهجية البحث
3	7.1 هيكلية البحث
	الأنظمة المصرفية	الثاني
5	1.2 مقدمة
5	2.2 مفهوم الصرافة
5	1.2.2 أعمال الصرافة
6	2.2.2 الشروط التي يجب الإلتزام بها في كل صرافة
6	3.2.2 شروط البدء بأعمال الصرافة
7	3.2 مفهوم أمن المعلومات
7	1.3.2 المبادئ الأساسية لأمن المعلومات
9	4.2 البنية الأساسية للمفتاح الأساسي ومكوناتها
10	1.4.2 أهداف البنية التحتية للمفتاح العام
10	2.4.2 مكونات البنية الأساسية للمفتاح العام
12	5.2 وظائف البنية التحتية للمفتاح العام
	الشهادات الرقمية	الثالث
16	1.3 مقدمة
17	2.3 الشهادات الرقمية
17	1.2.3 مكونات الشهادات الرقمية
19	2.2.3 أنواع الشهادات الرقمية
20	2.2.4 استخدام نظام الP12
20	3.3 حالات الشهادة الرقمية

21	4.3 سياسة الشهادات الرقمية
22	5.3 متطلبات الشهادات الرقمية
24	6.3 التوقيع الإلكتروني
24	1.6.3 خواص التوقيع الإلكتروني
24	2.6.3 مزايا استخدام التوقيع الإلكتروني
25	3.6.3 فوائد التوقيع الإلكتروني
25	4.6.3 متطلبات التوقيع الإلكتروني
26	5.6.3 كيفية عمل تقنية التوقيع الإلكتروني
27	7.3 التحقق من صحة التوقيع الرقمي
29	8.3 الفرق بين الشهادة الرقمية والتوقيع الرقمي
		الرابع
		الدراسات السابقة
31	1.6 تطوير البنية التحتية للمفتاح العام في المعاملات المصرفية عبر الانترنت.
31	
		Software (2010)2.6
		SecurityModule Ssm
32	3.6 نموذج لتأمين صفحات الإنترنت (2009)
33	
		4.6 البنية التحتية للمفتاح العام (2009)

35	1.5 مقدمة
35	ASP.NET(Active 2.5 Server Pages)
35	1.2.5 الاختلافات بين ال ASP.NET وال ASP
35	2.2.5 مميزات ال ASP
36	Visual Studio2010 3.5
37	4.5 لغة C#
38	1.4.5 مميزات C#
38	2.4.5 مجالات ال C#
38	SQL Server R2 2008 5.5
39	1.5.5 مميزات SQL Server
39	6.5 تعريف IIS
39	1.6.5 محتويات خدمة معلومات الانترنت
40	2.6.5 بعض البروتوكولات الداعمة لبروتوكولات ال IIS
40	3.5.6 فوائد ومميزات ال IIS
41	7.5 بروتوكول أمن الإتصال
45	Open SSL 8.5
45	1.8.5 مزايا OpenSSL
46	9.5 التشفير
46	1.9.5 أنواع التشفير
49	2.9.5 أهمية التشفير
49	10.5 خوارزمية RSA
50	11.5 دالة الهاش Hash
51	12.5 جهاز توثيق الرقم السري (Token)
51	13.5 بروتوكول التحقق من حالات الشهادة على الإنترنت
51	1.13.5 مزايا بروتوكول التحقق
52	2.13.5 تفاصيل بروتوكول (OCSP)
	السادس
	الفصل الأول
	مقارنة النظام الحالي والنظام المقترح
55	1.1.6 مقدمة
55	2.1.6 الأهداف
55	3.1.6 كيفية عمل النظام الحالي
56	4.1.6 المشاكل التي تواجه النظام

		الحالي
56	5.1.6 الحلول المقترحة
56	6.1.6 العمليات التي يقوم بها النظام المقترح
56	1.6.1.6 مايمكن النظام عمله
56	2.6.1.6 مايستفيدة الزبائن
56	3.6.1.6 ماتستفيدة الصرافة
57	7.1.6 تفصيل الإقتراح
57	8.1.6 المصادر
		الفصل الثاني
		تحليل النظام المقترح
59	1.2.6 مقدمة
59	2.2.6 لغة النمذجة الموحدة
59	1.2.2.6 أنواع مخططات ال(UML)
60	2.2.2.6 مميزات ال(UML)
60	Enterprise 3.2.6 Architecture
62	Enterprise 1.3.2.6 Architecture
62	4.2.6 مخطط العمليات
64	5.2.6 مخطط التتابع
69	6.2.6 مخطط النشاط
		السابع
		التطبيق
73	1.7 مقدمة
73	2.7 تطبيق إطار العمل المقترح
		الثامن
		النتائج والتوصيات
87	1.8 النتائج
88	2.8 التوصيات
89	3.8 الخلاصة
90	4.8 الخاتمة
92	المراجع
96	الملاحق