

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

المدرسة العليا للأساتذة

القبة القديمة (الجزائر)

قسم الإعلام الآلي

تأمين البيانات في الشبكة المعلوماتية

مذكرة لنيل شهادة أستاذ التعليم الثانوي

تحت إشراف الأستاذة:

- بوعيسى جميلة

إعداد الطالبات:

- جبريط حبيبة

- حمدوش سالمة

- عبدون زهية

لجنة المناقشة:

الأستاذة(ة): بويحي كريمة..... رئيسا.

الأستاذة: بوعيسى جميلة مشرفا.

الأستاذ: بلبزة حمزة ممتحنا.

السنة الجامعية 2015/2014

أ	قائمة الأشكال
ت	قائمة المعادلات الرياضية
ث	قائمة الكلمات الدلالية
ح	الملخص
1	مدخل

الفصل الأول: عموميات حول الشبكات

5	1.I المقدمة
5	2.I فوائد و أهمية الشبكات
6	3.I أنواع الشبكات
6	3.1.I حسب التغطية الجغرافية
8	3.2.I حسب علاقة التحكم
9	3.3.I حسب البنية
12	4.3.I حسب الربط المنطقي
13	4.I أجهزة الشبكات
14	5.I النموذج OSI
14	5.1.I وصف النموذج OSI
16	5.2.I طريقة نقل البيانات بين جهازين حسب النموذج OSI
17	6.I شبكة الانترنت
18	1.6.I بروتوكول الإنترنت
18	1.1.6.I النموذج TCP/IP
20	1.2.6.I نقل البيانات حسب النموذج TCP/IP
21	7.I الخاتمة

الفصل الثاني: أساسيات تأمين البيانات

23	1.II المقدمة
23	2.II تعريف تأمين البيانات
23	3.II بيئة التأمين
23	1.3.II ضعف الأنظمة
24	2.3.II التهديدات
25	3.3.II الهجمات الرئيسية

25	1.3.3.II الهجمات عن طريق البرامج الخبيثة.....
26	2.3.3.II هجمات عن طريق البريد الإلكتروني.....
27	3.3.3.II هجمات عن طريق الشبكة.....
28	4.3.3.II هجمات عن طريق كلمة المرور.....
28	4.II أهم طرق الإصابة بالبرامج الخبيثة.....
29	5.II معايير التأمين المعطيات.....
30	6.II مراحل تأمين المعطيات.....
30	1.6.II وضع نهج شامل.....
31	2.6.II تحليل الإحتياجات.....
31	7.II سياسة الأمن.....
32	8.II تقنيات تأمين المعطيات.....
32	1.8.II الأمن الفيزيائي.....
33	2.8.II الأمن البرمجي.....
33	1.2.8.II التوثيق.....
34	2.2.8.II جدار الحماية (Firewall).....
36	3.2.8.II خادم الوكيل (Serveur proxy).....
37	4.2.8.II الشبكات الافتراضية الخاصة (VPN).....
40	5.2.8.II مضادات الفيروسات.....
42	6.2.8.II نظام كشف الاختراقات.....
42	1.6.2.8.II مراجعة الأمن.....
43	2.6.2.8.II أنواع أنظمة كشف الاختراقات (ID).....
44	3.6.2.8.II طرق كشف الاختراقات.....
44	10.II الخاتمة.....

الفصل الثالث: التشفير

46	1.III المقدمة.....
46	2.III نبذة تاريخية عن التشفير.....
47	3.III تعريف التشفير (cryptage).....
47	4.III تعريف فك التشفير (décryptage).....
48	5.III تعريف خوارزمية التشفير.....

الفهرس

48 مفهوم المفتاح.....6.III
48 أهداف التشفير.....7.III
48 أنواع التشفير.....8.III
49 التشفير المتمائل.....1.8.III
51 التشفير اللامتائل.....2.8.III
52 مزايا وعيوب التشفير المتمائل و اللامتائل.....9.III
52 قياس قوة التشفير.....10.III
52 الخاتمة.....11.III

الفصل الرابع: التحليل و التصميم

54 المقدمة.....1.IV
54 وصف المشروع.....2.IV
54 مبادئ العمل.....3.IV
55 طريقة معالجة المعطيات.....4.IV
55 معالجة الملفات.....1.4.IV
56 معالجة النصوص.....2.4.IV
57 وصف مفتاح التشفير المقترح.....5.IV
57 الصيغة التشفير المقترحة.....1.5.IV
58 وصف الخوارزمية.....6.IV
58 خوارزمية التشفير المقترحة.....1.6.IV
59 خوارزمية فك التشفير المقترحة.....2.6.IV
61 الخاتمة.....7.IV

الفصل الخامس: التطوير و الإنجاز

63 المقدمة.....1.V
63 بيئة التطوير.....2.V
63 العتاد المستعمل.....1.2.V
63 لغة البرمجة المستعملة.....2.2.V
64 تقديم اكلبيس Eclipse.....1.2.2.V
65 تقديم البرنامج.....3.V
65 لماذا LéNigma؟.....3.1.V

الفهرس

663.2.V تقديم واجهات التطبيق
661.2.3.V واجهة التحميل
672.2.3.V واجهة التوثيق
673.2.3.V الواجهة الرئيسية
684.2.3.V واجهات التشفير
715.2.3.V واجهات فك التشفير
746.2.3.V واجهة لتغيير كلمة المرور
747.2.3.V واجهة المساعدة
758.2.3.V واجهة المعلومات (interface à propos)
753.3.V عرض القائمة الرئيسية (présentation de menu général)
764.V الخاتمة
78الخاتمة العامة
80قائمة المراجع

المخلص

أصبح أمن المعلومات أمر ضروري لا غنى عنه، سواء كان ذلك للأفراد أو للشركات فالיום، نحن ندخل عصر تطور الشبكات بشكل متسارع، مما يستوجب الحفاظ على كفاءات نظام الكمبيوتر.

دون ان ننسى وجود تهديدات كثيرة و متنوعة، التي تصيب الحاسوب أو تلك التي تنتقل في الشبكة.

و الهدف من هذه المذكرة هو إنشاء تطبيق تشفير وفك تشفير البيانات استنادا إلى خوارزمية متماثلة.

بحيث هذا البرنامج يضمن معايير أمن المعلومات، وهي:

- سرية البيانات المشفرة.
- سلامة البيانات بعد فك التشفير.
- المصادقة على المستخدم.

الكلمات المفتاحية:

الأمن - التشفير - فك التشفير - الشبكة - خوارزمية - المتماثلة - مفتاح.