**بسم الله الرحمن الرحيم**



**جامعة القدس المفتوحة**

**المشروع العملي لمقرر مبادئ علم التشفير 1374**

**إعـــــــــــــــــداد :هديل فؤاد فاروق حرب**

**التخصص : أنظمة معلومات حاسوبية فرع أمن معلومات**

**الرقم الجامعي:0123012110056**

**المشــــــــــــرف :د.أسامة أمين مصطفى مرعي**

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

**الفهرس**

[**أولا: التطبيق الذي يقوم بتشفير وفك التشفير باستخدام مفتاح متناظر(Symmetric-key)** 3](#_Toc165403160)

[**نبذة مختصرة عن تطبيق :AES Crypt** 3](#_Toc165403161)

[**إمكانيات التطبيق المختلفة :** 3](#_Toc165403162)

[**ثانيا: التطبيق الذي يقوم بتشفير وفك التشفير باستخدام مفتاح غير متناظر(Asymmetric-key)** 6](#_Toc165403163)

[**نبذة مختصرة عن تطبيق GnuPG (GNU Privacy Guard) :** 6](#_Toc165403164)

[**إمكانيات التطبيق المختلفة :** 7](#_Toc165403165)

[**الإيجابيات (المميزات):** 7](#_Toc165403166)

[**السلبيات:** 7](#_Toc165403167)

تقرير لمقرر مبادئ علم التشفير 1374

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

* **أولا: التطبيق الذي يقوم بتشفير وفك التشفير باستخدام مفتاح متناظر(Symmetric-key)**
* **نبذة مختصرة عن تطبيق :AES Crypt**
* AES Crypt هو تطبيق تشفير مجاني ومفتوح المصدر و بسيط وفعال يستخدم تشفير AES (Advanced Encryption Standard) لحماية الملفات والمجلدات على أنظمة التشغيل Windows، macOS، Linux وAndroid. يهدف AES Crypt إلى توفير حماية سهلة الاستخدام وقوية للبيانات الحساسة والملفات الشخصية.
* التطبيق يتيح للمستخدمين تشفير الملفات باستخدام كلمة مرور، وبالتالي لا يتطلب البرنامج تثبيتًا معينًا أو تهيئة معقدة. كل ما يحتاجه المستخدم هو تنزيل التطبيق واستخدامه لتشفير وفك تشفير الملفات بسهولة.
* من خلال استخدام AES كخوارزمية تشفير، يوفر AES Crypt مستوى عالٍ من الأمان والحماية للبيانات. تعتبر AES واحدة من أكثر خوارزميات التشفير شيوعًا وأمانًا في العالم، وقد تم اختيارها كمعيار للتشفير من قبل حكومة الولايات المتحدة الأمريكية.

**عنوان URL للتطبيق :** [**https://www.aescrypt.com/**](https://www.aescrypt.com/)

* **إمكانيات التطبيق المختلفة :**
* تطبيق AES Crypt يوفر عدة إمكانيات تساعد المستخدمين في تأمين ملفاتهم وحمايتها بشكل فعال، من بين هذه الإمكانيات:

1. **تشفير الملفات بسهولة**: يمكن للمستخدمين تشفير الملفات بسرعة وسهولة باستخدام كلمة مرور، بمجرد تحديد الملفات المراد تشفيرها وإدخال كلمة المرور المطلوبة.

2. **فك تشفير الملفات بسرعة**: بعد تشفير الملفات، يمكن للمستخدمين فك تشفيرها بنفس السهولة باستخدام كلمة المرور التي استخدموها للتشفير.

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

3. **حماية البيانات الحساسة**: يوفر AES Crypt طريقة قوية لحماية البيانات الحساسة والملفات الشخصية، مما يضمن سرية المعلومات.

4. **دعم الأنظمة المتعددة**: يتوفر AES Crypt على عدة إصدارات لمختلف أنظمة التشغيل مثل Windows، macOS، Linux وAndroid، مما يجعله متاحًا لمجموعة واسعة من المستخدمين.

5. **سهولة الاستخدام**: يتميز التطبيق بواجهة مستخدم بسيطة وسهلة الاستخدام، مما يجعل عملية تشفير وفك تشفير الملفات مباشرة وسلسة للمستخدمين حتى بدون خبرة سابقة.

* **مميزات التطبيق ( ايجابيات وسلبيات )** :
* **الإيجابيات (المميزات):**

1. **سهولة الاستخدام**: واجهة مستخدم بسيطة وسهلة الاستخدام تجعل عملية تشفير وفك تشفير الملفات مباشرة وميسرة.
2. **قوة التشفير:** يستخدم تقنية التشفير AES (Advanced Encryption Standard)، التي تُعتبر واحدة من أقوى وأكثر الطرق اعتمادًا لتأمين البيانات.
3. **دعم متعدد للأنظمة**: تتوفر إصدارات من التطبيق لأنظمة التشغيل المختلفة مثل Windows، macOS، Linux وAndroid.
4. **سرية المعلومات**: يوفر حماية فعالة للملفات الحساسة والشخصية، مما يضمن سرية المعلومات.
5. **أمان قوي:** يستخدم AES Crypt خوارزمية تشفير قوية (AES) لحماية بياناتك.

* **السلبيات:**

1. **اعتماد على كلمة المرور**: قد يكون اعتماد التطبيق على كلمة مرور واحدة للتشفير قد يعرض البيانات للخطر في حال تسرب هذه الكلمة.
2. **قدرة الهجوم العنيف (Brute Force Attacks)**: في حال استخدام كلمات مرور ضعيفة، فقد تكون عرضة للهجمات العنيفة التي تهدف إلى تخمين كلمة المرور.
3. **توافر الإصدارات المختلفة**: قد يؤدي توافر إصدارات مختلفة لأنظمة التشغيل إلى بعض الفوارق في الوظائف المدعومة وقدرات التكامل.
4. **قد يكون معقدًا للمستخدمين المبتدئين:** قد يكون AES Crypt معقدًا للمستخدمين المبتدئين الذين ليس لديهم خبرة في التشفير
5. **قد يكون بطيئًا:** قد يكون AES Crypt بطيئًا عند تشفير وفك تشفير الملفات الكبيرة.

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

* **سبب اختياري للتطبيق** : تطبيق AES Crypt يُختار بسبب سهولة استخدامه وقوة أمانه. بفضل تقنية التشفير الموثوقة AES وواجهة المستخدم البسيطة، يمكن للمستخدمين تشفير وفك تشفير الملفات بسرعة وسهولة دون الحاجة لمعرفة متقدمة بالأمان. هذا يجعله اختيارًا مثاليًا لحماية البيانات بسرعة وفعالية على مختلف الأنظمة.

****

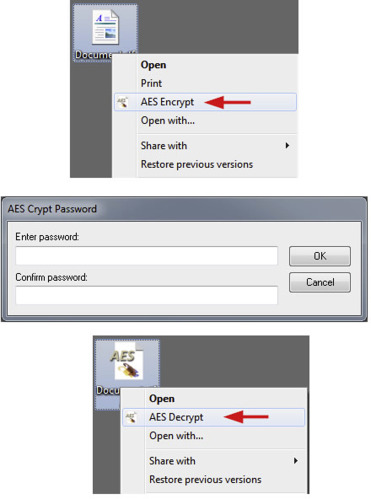
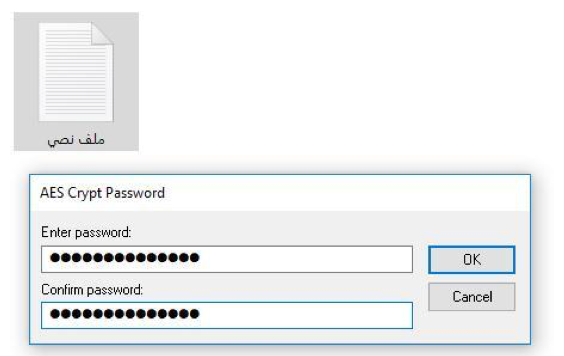
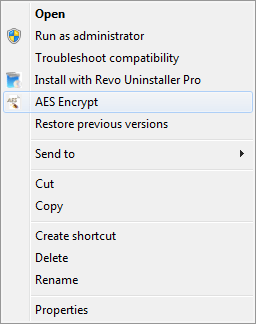
* **آلية عمل التطبيق:**

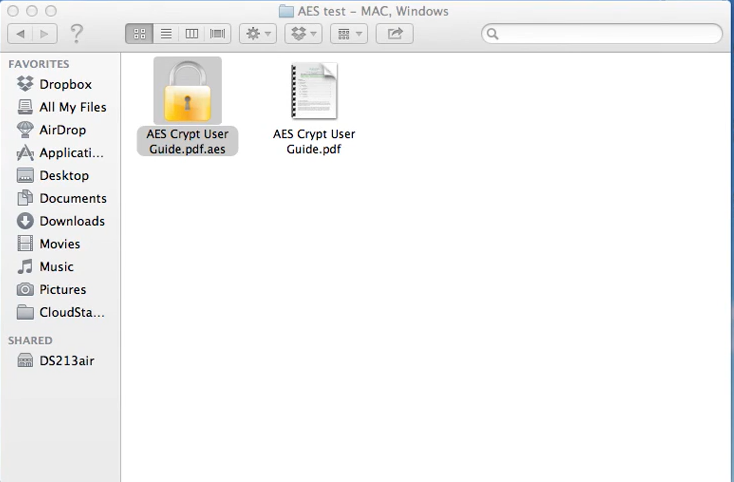
نظرة عامة عن كيفية عمل التطبيق:

1. **فتح التطبيق**: قم بتشغيل تطبيق AES Crypt على جهازك.
2. **تحديد الملفات**: حدد الملفات التي ترغب في تشفيرها من خلال واجهة التطبيق**.**
3. **تحديد كلمة المرور**: ادخل كلمة المرور التي ترغب في استخدامها لتشفير الملفات المحددة.
4. **تشفير الملفات**:
   * عندما يقوم المستخدم بتشفير ملف معين باستخدام AES Crypt، يتم استخدام خوارزمية AES لتشفير المحتوى بناءً على كلمة المرور التي يحددها المستخدم.
   * يتم تحويل كلمة المرور إلى مفتاح تشفير يستخدم لتشفير الملفات. هذا المفتاح يتم استخدامه مع خوارزمية AES لتشفير الملف بشكل آمن.
5. **حفظ المفتاح السري**:
   * لضمان أمان البيانات، يتم حفظ المفتاح السري الذي يتم إنشاؤه باستخدام كلمة المرور بشكل آمن في الملف المشفر.
   * يكون هذا المفتاح السري مطلوبًا لفك تشفير الملفات في المستقبل.
6. **فك تشفير الملفات**:
   * عندما يرغب المستخدم في فتح ملف مشفر، يدخل كلمة المرور المطلوبة في تطبيق AES Crypt.
   * يتم استخدام كلمة المرور لإعادة إنشاء المفتاح السري الذي تم استخدامه لتشفير الملف.
   * يتم استخدام هذا المفتاح لفك تشفير الملف بشكل صحيح، مما يسمح للمستخدم بالوصول إلى المحتوى الأصلي للملف.

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

* **الخطوات موضحة بالصور:**



****

* **ثانيا: التطبيق الذي يقوم بتشفير وفك التشفير باستخدام مفتاح غير متناظر(Asymmetric-key)**
* **نبذة مختصرة عن تطبيق GnuPG (GNU Privacy Guard) :**

هو برنامج مفتوح المصدر يستخدم لتشفير وفك تشفير البيانات، بما في ذلك البريد الإلكتروني والملفات، باستخدام التشفير بمفتاح غير متناظر (Asymmetric-key). يعد GnuPG بديلاً مجانيًا لبرنامج PGP (Pretty Good Privacy) المغلق المصدر.

يعتمد GnuPG على تقنيات التشفير المعتمدة عالميًا، مما يجعله من الأدوات الشائعة للحفاظ على الخصوصية والأمان في الاتصالات الإلكترونية. يوفر GnuPG مجموعة واسعة من الميزات، بما في ذلك تشفير وفك تشفير البريد الإلكتروني، وتوقيع الرسائل الإلكترونية للتحقق من هوية المرسل، وتشفير الملفات.

**عنوان URL للتطبيق :** <https://www.gnupg.org/>

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

* **إمكانيات التطبيق المختلفة :**

1. **تشفير وفك تشفير البريد الإلكتروني**: يتيح GnuPG للمستخدمين تشفير رسائل البريد الإلكتروني باستخدام مفتاح عام للتشفير، مما يضمن سرية المحتوى والبيانات المرسلة.
2. **توقيع الرسائل الإلكترونية**: يتيح للمستخدمين توقيع رسائل البريد الإلكتروني باستخدام مفتاح خاص، مما يسمح للمستلمين بالتحقق من هوية المرسل وسلامة الرسالة.
3. **إنشاء وإدارة المفاتيح العامة والخاصة**: يوفر GnuPG أدوات لإنشاء وإدارة مفاتيح التشفير العامة والخاصة، بما في ذلك تصدير واستيراد المفاتيح وتوليد الأزواج الرئيسية.
4. **تشفير وفك تشفير الملفات**: يمكن استخدام GnuPG لتشفير وفك تشفير الملفات باستخدام الأوامر في واجهة السطر الأمري، مما يوفر طريقة آمنة لحماية البيانات.
5. **التوافق مع بروتوكول :OpenPGP** يتوافق GnuPG مع بروتوكول OpenPGP، مما يسمح للمستخدمين بالتفاعل مع الأدوات والخدمات الأخرى التي تدعم هذا البروتوكول.

* **مميزات التطبيق ( ايجابيات وسلبيات )** :

**الإيجابيات (المميزات):**

1. **أمان عالي**: يوفر GnuPG مستوى عالٍ من الأمان من خلال استخدام تقنية التشفير بمفتاح غير متناظر (Asymmetric-key)، مما يحافظ على سرية البيانات وحمايتها من الوصول غير المصرح به.
2. **مفتوح المصدر**: يعتبر GnuPG برنامجًا مفتوح المصدر، مما يعني أنه متاح للجميع للتحميل والاستخدام مجانًا، ويسمح بالتحقق من الأمان وتحسين البرنامج بواسطة المطورين المجتمعين.
3. **مرونة**: يمكن استخدام GnuPG في مجموعة متنوعة من الاستخدامات، بما في ذلك تشفير وفك تشفير البريد الإلكتروني، وتشفير الملفات، وإدارة المفاتيح، وغيرها، مما يجعله أداة متعددة الاستخدامات.
4. **توافق متعدد للأنظمة**: يتوفر GnuPG على إصدارات لمختلف أنظمة التشغيل مثل Windows، macOS، Linux، وغيرها، مما يجعله متاحًا لجميع أنواع المستخدمين.

**السلبيات:**

1. **تعلُّم منهجية الاستخدام**: قد يكون هناك منحى تعلُّمي لاستخدام GnuPG، خاصة بالنسبة للمستخدمين الجدد، نظرًا لتعقيد بعض الإعدادات والإجراءات.
2. **قد يتطلب التكوين**: قد يحتاج بعض المستخدمين إلى إجراءات تكوين إضافية لاستخدام GnuPG بشكل مثالي وفقًا لاحتياجاتهم.
3. **تحديثات مستمرة**: نظرًا لطبيعة الأمان، قد تتطلب بعض التحديثات الأمنية التكرارية لتأمين البرنامج والحفاظ على سلامة البيانات.

**سبب اختياري للتطبيق**: يُختار تطبيق GnuPG (GNU Privacy Guard) بسبب قوته في توفير الأمان وحماية الخصوصية في الاتصالات الإلكترونية، إلى جانب ميزاته المتعددة وتوافقه مع مختلف أنظمة التشغيل.

الاسم:هديل فؤاد فاروق حرب الرقم الجامعي :0123012110056

* **آلية عمل التطبيق:**

1. **إنشاء مفاتيح التشفير**:
   * يبدأ المستخدم بإنشاء زوج من المفاتيح: مفتاح عام (Public Key) ومفتاح خاص (Private Key).
   * يتم استخدام المفتاح العام لتشفير البيانات، بينما يتم استخدام المفتاح الخاص لفك تشفيرها.
2. **تشفير البيانات**:
   * عندما يريد المستخدم تشفير بيانات معينة، يستخدم مفتاح المستلم (مفتاحه العام) لتشفير البيانات.
   * يتم إرسال البيانات المشفرة إلى المستلم.
3. **فك تشفير البيانات**:
   * عند استلام البيانات المشفرة، يستخدم المستلم مفتاحه الخاص لفك تشفيرها والحصول على البيانات الأصلية.
4. **التوقيع الرقمي**:
   * يمكن استخدام GnuPG أيضًا لتوقيع الرسائل الإلكترونية بواسطة مفتاح خاص.
   * يمكن للمستلم استخدام مفتاح المرسل العام للتحقق من صحة التوقيع الرقمي.
5. **إدارة المفاتيح**:
   * يوفر GnuPG أدوات لإدارة مفاتيح التشفير بما في ذلك إنشاء وحذف المفاتيح واستيرادها وتصديرها.

* **الخطوات موضحة بالصور:**

