الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة الشهيد حمه لخضر – الوادي
كلية العلوم الدقيقة
قسم الإعلام الألي

تصميم برنامج لإدارة و حفظ كلمات المرور

تخصص: نظم المعلوماتية

إعداد الطلبة:

- قرفي طه
- مسعودي فوزي
- علاق سفيان

تحت اشراف:

- د. بوشريط عمار

لجنة المناقشة:

الاسم واللقب	الصفة
د.يعقوب محمد أمين	مناقش
د.غربي قدور	مناقش
د. بوشريط عمار	مشرف و مقرر

السنة الجامعية: 2020 / 2021

تشكر

بعد إنجازنا لهذا العمل المتواضع، نرسل خالص شكرنا لمشرفنا الأستاذ: بوشريط عمار لمساعدته ونصائحه القيمة ومساندته الدائمة لنا.

وفي النهاية، نود أن نشكر كل أولئك الذين ساعدونا وشجعونا من الأقارب والأصدقاء.

الإهداء

أكرس هذا العمل إلى أكثر إثنين كانا سببا في وجودي: أبي و أمي كنتما دوما إلى جانبي لدعمي و تشجيعي منذ أول يوم دخلت فيه إلى الدراسة من السنة 1 إبتدائي إلى ما أنا عليه الآن , وها قد جاء اليوم الذي ستجنيان منه تعبكما لأكون فخرا لكما .

أسأل الله أن يحميكما يا أبي و أمي و يمن عليكما بالصحة و العافية لتنظرى لأبنكما بكل فخر.

- إلى أمي
- إلى إخوتي و كل من أحب
- إلى جميع أصدقائي في السنة الثالثة نظم المعلوماتية 2021/2020 وكل من ساهم في هذا المشروع
- إلى الأصدقاء علي سلطاني ,علاء الدين عباسي , سهيل شنوف
- إلى كل من ساهم في هذا المشروع و نسيت ذكره أنا أشكركم و ممتن لكم على جهودكم المبذولة

Résumé

Avec l’expansion d’Internet et du monde numérique, nous utilisons quotidiennement des dizaines de sites et d'applications qui nécessitent une authentification par identifiant et un mot de passe. En revanche, parmi les principaux risques liés au mot de passe figurent sa divulgation et son oubli.

Par conséquent, la gestion des mots de passe est un aspect majeur pour la sécurité de nos données et informations sensibles. Afin d'atteindre cet objectif, nous tenterons dans ce projet de créer un outil de gestion et de sauvegarde des mots de passe pour assurer leur protection et leur confidentialité.

ملخص

مع التطور التكنولوجي في العالم الرقمي والأنترنت، أصبحنا نستعمل عددا كبيرا مواقع الانترنت والتطبيقات التي تحتاج لمعلومات الدخول من أجل ضمان سريتها. ومن جهة أخرى، فإنّ من بين أهم المخاطر التي تواجهنا عند استخدام معلومات الدخول هي تسربها أو نسيانها.

لذلك، تعد إدارة كلمات المرور أمرا رئيسيًا لأمان بياناتنا ومعلوماتنا الحساسة. ولتحقيق هذا الهدف، سنحاول في هذا المشروع إنشاء أداة لإدارة كلمات المرور وحفظها لضمان حمايتها وسريتها..

الفهرس

صفحات

الفصل الثالث : التطوير والإنشاء

مقدمة:

مع تطور العلم اصبحت الإنترنت مصدر كبير من مصادر المعرفة و اصبحت أغلب المواقع و التطبيقات تستخدم كلمات السر لحماية خصوصيات المستخدمين , و نحن نهدف في مشروعنا هذا إلى إنشاء برنامج لإدارة كلمات السر التي أصبح اغلب المستخدمين في وقتنا الحالي يجدون صعوبة في الحفاظ عليها و تأمينها , فلذا من أجل تجنب نسيان أو فقدان كلمات المرور تلك ومن أجل سرعة الوصول إليها قررنا إنشاء هذا البرنامج لتنظيم و تأمين كلمات السر الخاصة بالمستخدمين .

- تتكون مذكرتنا من 3 فصول .

الفصل الأول: يتناول هذا الفصل أساليب و طرق لحماية و تأمين المستخدمين عبر الأنترنت والتي هي التشفير و تحدثنا أيضا عن أمن المعلومات و أساليب العمل فيها

الفصل الثاني: يتناول هذا الفصل

- مقدمة خفيفة عن ماهية عمل البرنامج
- مخططات UML .
  1. مخطط الفصل
  2. مخطط حالة الإستخدام
  3. مخطط النشاط

الفصل الثالث:

- استعراض لغة البرمجة المستخدمة
- عرض كيفية عمل البرنامج

الفصل الأول

السياق العام

I)أمن المعلومات

I-1) مقدمة عن أمن المعلومات:

علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات [1].

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى:

- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج والتطبيقات
- أنظمة حماية قواعد البيانات
- أنظمة حماية الولوج أو الدخول إلى الأنظمة [1]

I-2)ما هو أمن المعلومات:

أمن المعلومات هو السيطرة التّامة على المعلومات، من حيث تحديد من سيستلم هذه البيانات، وتحديد صلاحيّات الوصول إليها، واستخدام مجموعة من التقنيّات من أجل ضمان عدم اختراقها من قبل أي جهة، وتتضاعف أهميّتها من الحفاظ على الخصوصيّة، إلى الحفاظ على بيانات هامّة مثل حسابات العملاء في البنوك[1]

I-3) طرق وأدوات للحماية في أمن المعلومات:-

1- التأمين المادي للأجهزة والمعدات

2- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري

3- تركيب أنظمة كشف الاختراق وتحديثها

4- تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية

5- عمل سياسة للنسخ الاحتياطي

6- نشر التعليم والوعي حول أمن المعلومات

7- دعم أجهزة عدم انقطاع التيار

8- استخدام أنظمة قوية لتشفير المعلومات المرسلة

II) تخصيص المشروع:

وفي هذا العمل سيقتصر عملنا على تخزين وحماية كلمات السر التي اصبحنا في عصرنا الحالي نستخدمها بشكل يومي في شتى المواقع و التطبيقات و البرامج ...الخ فنظرا لكثرتها و صعوبة حفظها وحتى نتفادى هذا المشكل سنتطرق الى انشاء برنامج لإدارة كلمات السر و أثناء تخزين تلك البيانات ستكون كلمة السر مشفرة لحماية أكثر.

III) مدخل في التشفير :

على مر العصور والحضارات اكتشف الإنسان طرق للتواصل وكانت تبادل الرسائل أحد طرقها وكون الانسان بشكل غريزي يخفي رسائله ليحافظ على سريتها وهنا برع الإنسان في تبني مفهوم الشيفرة.

يعد التشفير أحد العلوم المسيطرة في عالمنا اليوم وهو واحد من أهم العناصر التي تدخل في صناعة البلوك شين والعملات الرقمية الحديثة.

إن تقنيات التشفير المستخدمة اليوم هي نتيجة لتاريخ طويل للغاية من التطور، وفي هذا المقال نتعرف عن هذا العالم الرائع كيف بدأ وما الذي جعله ذو أهمية فائقة لتاريخ البشرية. فما هي الشيفرة ؟ وما هو التشفير؟ ولماذا اصبح حديثًا قويًا اليوم ؟

III-1)علاقة بين أمن المعلومات والتشفير:-

إن علم البيانات علم قديم جدًا ولكن زادت الحاجة إليه مع انتشار استخدام الإنترنت والتكنولوجيا والإعتماد عليه في كافة مجالات حياتنا وتبادل الرسائل المختلفة تعددت طرق الحماية لهذه المعلومات إما عن طريق حمايتها بشكل فيزيائي توظيف حارس أمن مثلًا أو تأمين مكان مناسب لهذه البيانات أو الحماية باستخدام البرمجيات أو الأجهزة أو المعدات ولعل أهم طرق حماية هذه البيانات والحفاظ على سريتها كان التشفير. إذا ما هو التشفير ؟

VI) التشفير:

ويطلق عليه باللغة الإنجليزية encryption أو ciphering في حين encryption مأخوذة من الكلمة اللاتينية cryptography وتعني الكتابة السرية و أما ciphering فيقال أنها مأخوذة من الكلمة العربية صفر و تعني جعل القيمة صفر بلا معنى.

إذا التشفير هو علم تحويل المعلومات من بيانات مقروءة إلى بيانات غير مقروءة إلا لمن يملك مفتاح خاص لفك تشفيرها و يقصد بفك التشفير عملية إستخدام المفتاح لإعادة النص المشفر إلى هيئته السابقة [2]

1-VI) أنواع التشفير

في وقتنا الحالي يوجد نوعان من التشفير هما :

- التشفير التقليدي(ConventionalCryptography)
- التشفير المفتاح العام(Public KeyCryptography)[3]

1-1-VI)التشفير التقليدي (Conventional Cryptography)

وهو يستخدم مفتاح واحدً لعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. مثال على ذلك؛ إذا أراد زيد إرسال رسالة مشفرة إلى عبيد، عليه إيجاد طريقة آمنة لإرسال المفتاح إلى عبيد. فإذا حصل أي شخص ثالث على هذا المفتاح فإن بإمكانه قراءة جميع الرسائل المشفرة بين زيد وعبيد كما في الصورة ادناه[3] :

توضح عمل التشفير باستخدام المفتاح الواحد

مثال على التشفير التقليدي:

شيفرة قيصر:

وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها. المثال التالي يوضح طريقة عمل شيفرة "SECRET"قيصر: إذا شفرنا كلمة

واستخدمنا قيمت المفتاح 3، فإننا نقوم بتغيير مواضع الحروف ابتداءً من وعليه فان ترتيب الحروف سوف يكون على Dالحرف الثالث وهو الحرف

الشكل التالي :

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

الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" تكون على الشكل الحالي:

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

والآن قيمة Aهي Dوقيمة B هي Eوقيمة C هي F وبهذا الشكل فإن كلمة VHFUHW تصبحSECRET يجب أن تعطي مفتاح فك التشفير 3 لتعطي اي شخص إمكانية قراءة رسالتك[3]

2-1-VI) تشفير المفتاح العام (Public key Cryptography)

أو ما يعرف بالتشفير اللاتماثلية CryptographyAsymmetric تم تطوير هذا النظام في السبعينيات في بريطانيا و كان استخدامه حكرا على قطاع الحكومة. و يعتمد في المبدأ على وجود مفتاحين وهما المفتاح العام و المفتاح الخاص حيث ان المفتاح العام هو لتشفير الرسالة و المفتاح الخاص لفك تشفير الرسالة . المفتاح العام يرسل لجميع الناس و أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسل لأحد فمن يحتاج أن يرسل لك رسالة مشفرة انه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها و فك تشفيرها بمفتاحك الخاص كما في الصورة أدناه

توضح عمل التشفير باستخدام المفتاح العام والمفتاح الخاص

بعض الأمثلة على أنظمة تشفير المفتاح العام و الخاص:

PGP, DSA, Deffie-Hellman, Elgamal, RSA

جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص[3]

دراسة الموجود:

أهمية استخدام برنامج لإدارة كلمات المرور

في الآونة الاخيرة أصحنا نسمع كثيرا عن الهجمات الإلكترونية على الإنترنت والتي لم تعد تستهدف المواقع والشركات فقط بل أصبحت تستهدف المستخدمين العاديين كذلك بهدف السطو معلوماتهم الشخصية، ولعل أحد أبرز الاساليب المستخدمة في هذه الهجمات هي كلمات السر بطريق عديدة مثل التخمين أو إعادة استخدام كلمات السر التي تم الحصول عليها من قواعد بيانات تم تسريبها أو غير ذلك، فكلمة السر تعتبر الدرع الأول الذي يحمي حسابات الأشخاص أو المؤسسات، ولهذا يجب الحرص على أن تظل كلمات السر في أمان.

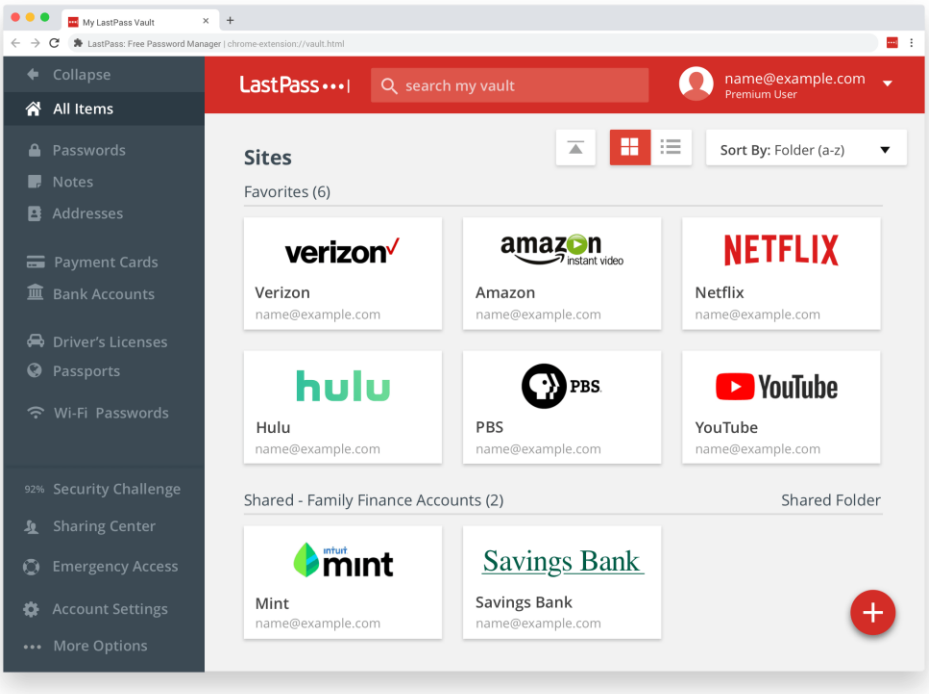
ومن جهة أخرى، ونظرا لصعوبة تذكّر كلمات سر المختلفة التي نستخدمها في مواقع الأنترنت التي نشترك بها، أو للبرامج التي نستخدمها، فإن أغلب المستخدمين يفضلون إعادة استخدام نفس كلمة السر أو تغييرها بشكل بسيط حتى يسهل عليه تذكّرها. وعلى الرغم من سهولة هذه الخطوة، حيث لن يكون لدى المستخدم إلا كلمة سر واحدة لكل المواقع والخدمات التي يشترك بها، إلا أنّ الخيار يجعل من عملية اختراق المعلومات الشخصية أكثر سهولة، وعن طريق كلمة مرور واحدة يستطيع شخص آخر ان يعرف كل خصوصياتنا.

ولهذا فإن استخدام برامج متخصصة في إدارة كلمات المرور سيسهل على المستخدم الاحتفاظ بكلمات مرور مختلفة مع ضمان سريتها. وعليه فكل ما يحتاجه المستخدم تذكر كلمة سر رئيسية واحدة للوصول لكل كلمات السر الأخرى مما يجعل عملية تعبئة نماذج تسجيل الدخول في المواقع أسهل وأبسط.

أمثلة عن بعض البرامج والإضافات

1. LastPass :

تسمح إضافة LastPass إمكانية تسجيل الدخول لكل مواقع الانترنت بشكل تلقائي دون الحاجة لكتابة معلومات الدخول في الحقول. كما يمكن إضافة معلومات البطاقات الائتمانية والملفات والصور المهمة ليتم حفظها بشكل آمن فيه.



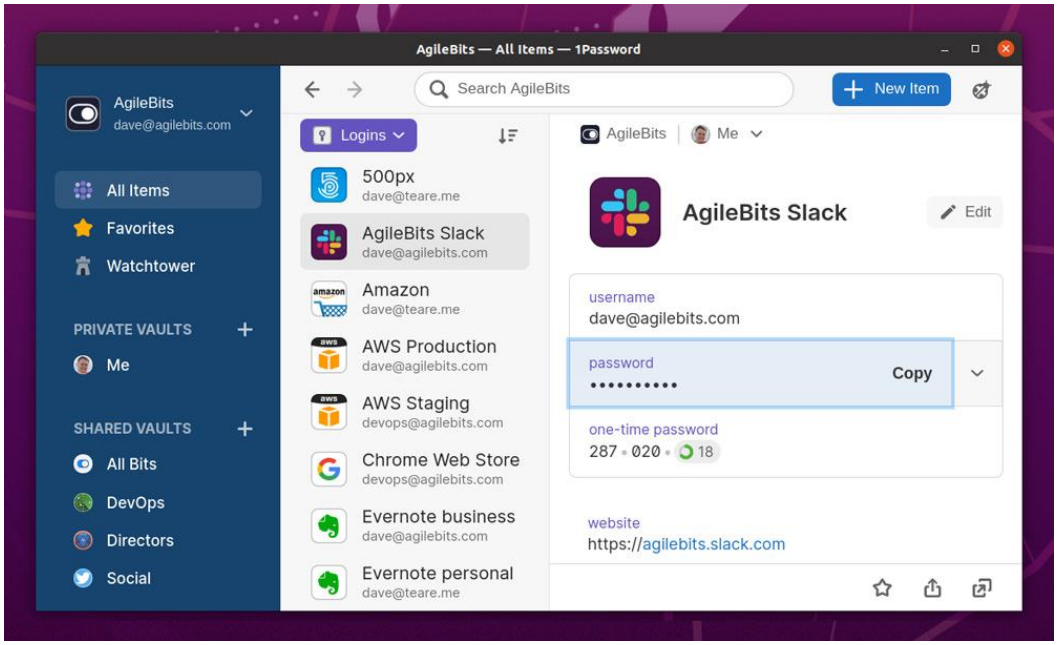
واجهة برنامج Lastpass

يمكن للمستخدم الاستفادة من هاته الإضافة واستخدامها مجانيا على من أي جهاز كمبيوتر أو جهاز جوال، وذلك من خلال أحد المتصفحات. كما توجد نسخة أخرى لهاته الإضافة في شكل تطبيق يعمل على أجهزة الأيفون والاندرويد. والويندوز.

يعمل على: أي متصفح، الايفون، الاندرويد، ويندوز.

2- 1Password:

يعتبر برنامج 1 Password من بين أكثر البرامج شهرة في عالم برامج إدارة كلمات السر، يعمل البرنامج على أغلب المتصفحات وأنظمة التشغيل. كما يتيح مزايا مهمة مثل ميزة فحص الأمان، والتي تقوم بفحص كلمات السر الخاصة بالمستخدم وإيجاد كلمات السر المكررة أو الضعيفة واستبدالها بكلمات سر أقوى.



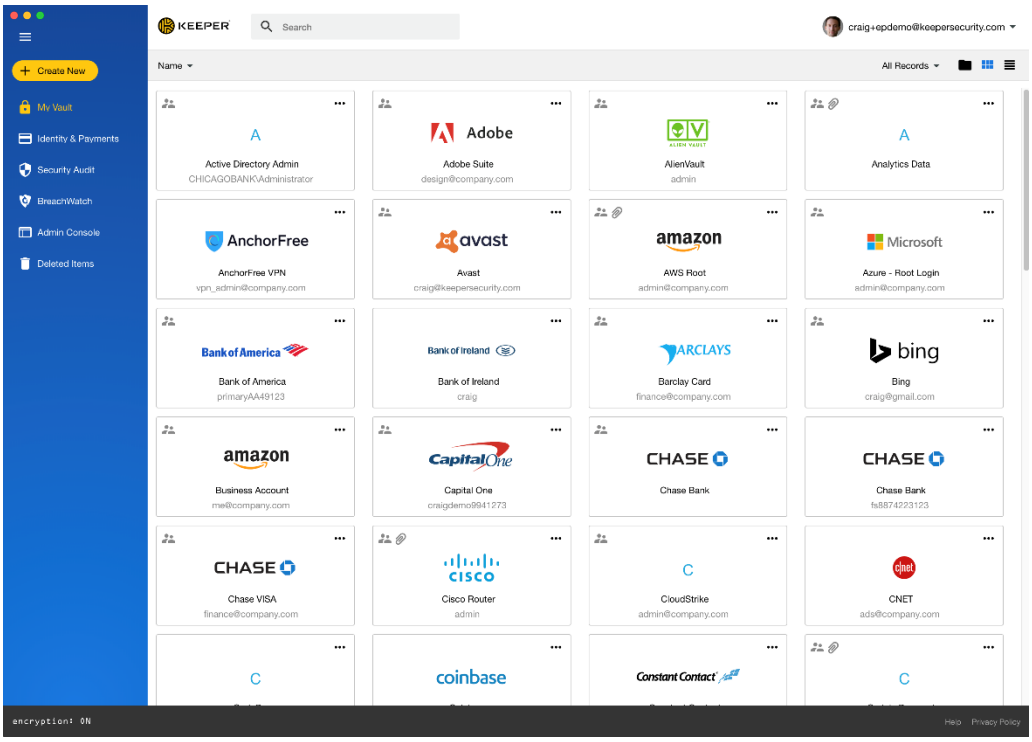
واجهة برنامج 1Password

كما يمكن لمستخدمي هذا البرنامج اختيار مكان خاص بهم لحفظ كلمات السر الخاصة بهم، حيث يمكنهم البرنامج من حفظها في حساب على الدروب بوكس أو الآي كلاود. كما يتوفر البرنامج مجانيا وعلى أغلب المنصات.

يعمل على: أي متصفح، الايفون، الاندرويد، ويندوز.

3- Keeper:

يعتبر برنامج Keeper مسيِّرا فعالا لكلمات السر مستخدم بكثرة لدى الشركات، كما يمكن استخدامه بمثابة مدير كلمات مرور على المستوى الشخصي باستخدام الإصدار التجريبي المجاني لمدة 30 يوم. ونظرا لكونه يتيح مختلف أشكال المصادقة الثنائية لإبقاء المخترقين بعيداً فقد تجاوز البرنامج العديد من المراجعات المستقلة التي تؤكد أنه آمن وموثوق.



واجهة برنامج Keeper

التعليق عن البرامج الموجودة:

إنّ استخدام واحد من برامج إدارة كلمات المرور أصبح ذو أهمية كبيرة لتحسين مستوى حماية الأشخاص والمؤسسات على الإنترنت. تلك البرامج تجعل من السهل اتباع ممارسات كلمات المرور القوية وتجنب التوابع الخطيرة للاختراقات الأمنية.

كما لاحظنا انّ أغلب هذه البرامج تشترك في عدة نقاط أهمها:

- سهولة التعامل مع البرنامج ووضوح الواجهة.
- استخدام كلمة سر رئيسية واعتماد المصادقة الثنائية. وبهذه الطريقة، لن تكون كلمات المرور مهددة حتى إذا تمكن شخص ما من الوصول إلى كلمة المرور الرئيسية.
- تشفير كلمات السر داخل قاعدة البيانات التي تحوي كلمات السر.
- تبويب كلمات السر على حسب نوعها (موقع، برنامج ....)


الفصل الثاني
النمذجة

I) مقدمة:

الهدف من هذا الفصل هو نمذجة نظامنا لتحقيق إدراك جيد في نهاية الدراسة .

لتصميم نظام جيد وضعنا لأنفسنا الأهداف التالية :

1. ضمان حماية و سرية تامة للمعلومات الشخصية
2. سهولة استخدام للبرنامج

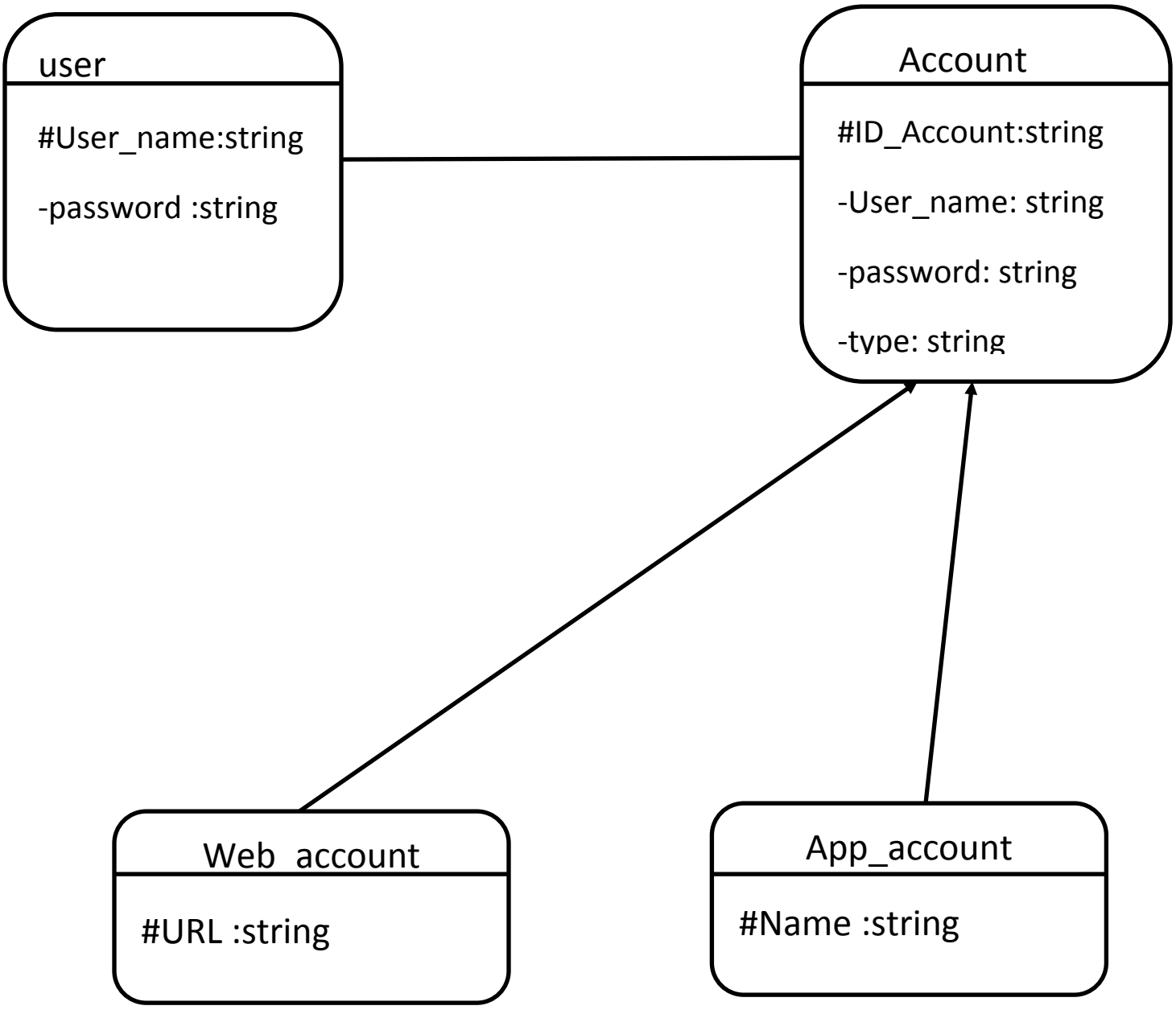
ولضمان كل هذا من الضروري إستخدام طريقة أو نهج للتصميم ولذالك سنعتمد طوال هذا الفصل على الUML طوال دورة التطوير.

II) وصف المشروع :

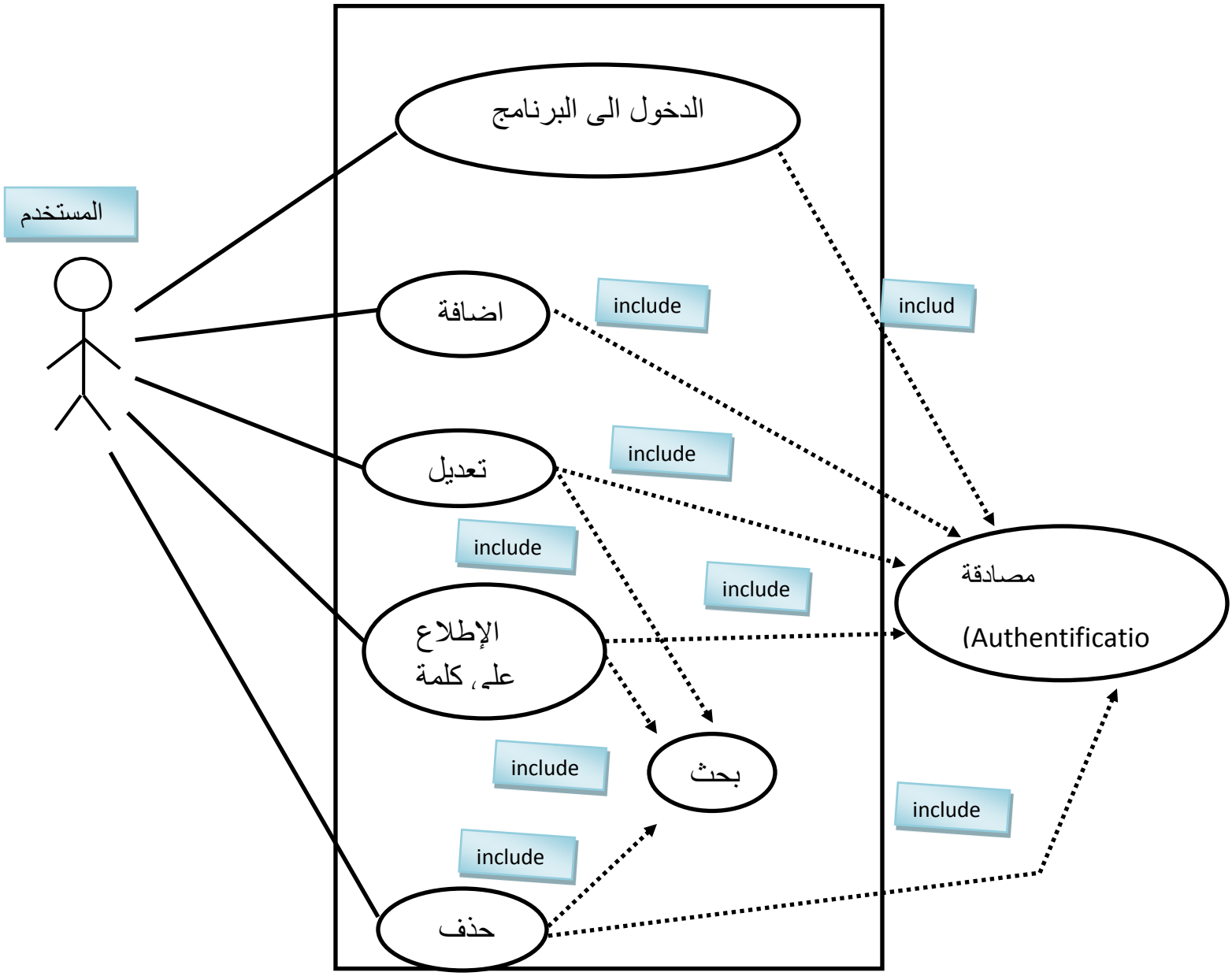
الهدف من مشروعنا هو إدارة و حفظ كلمات المرور. حيث يسمح لك بإنشاء أكثر من حساب على نفس الجهاز ليسمح لك بحفظ معلومات تسجيل دخولك لمختلف حساباتك في شتى المواقع و التطبيقات مع مكانية تشفير كلمة المرور لضمان حماية و سرية أكثر لمعلوماتك الشخصية .

III) مخططات UML :

III-1)مخطط الفصل

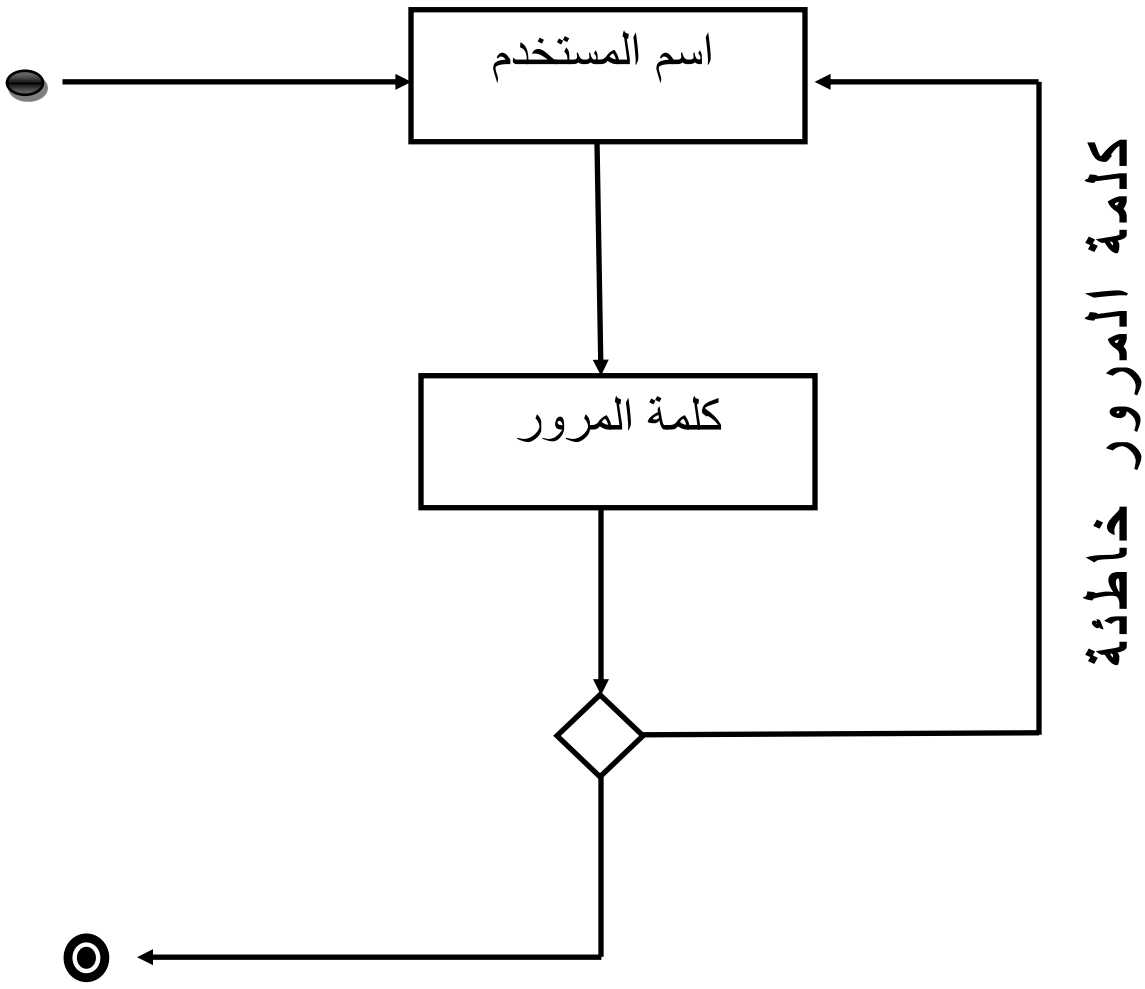


III-2)مخطط حالة الاستخدام

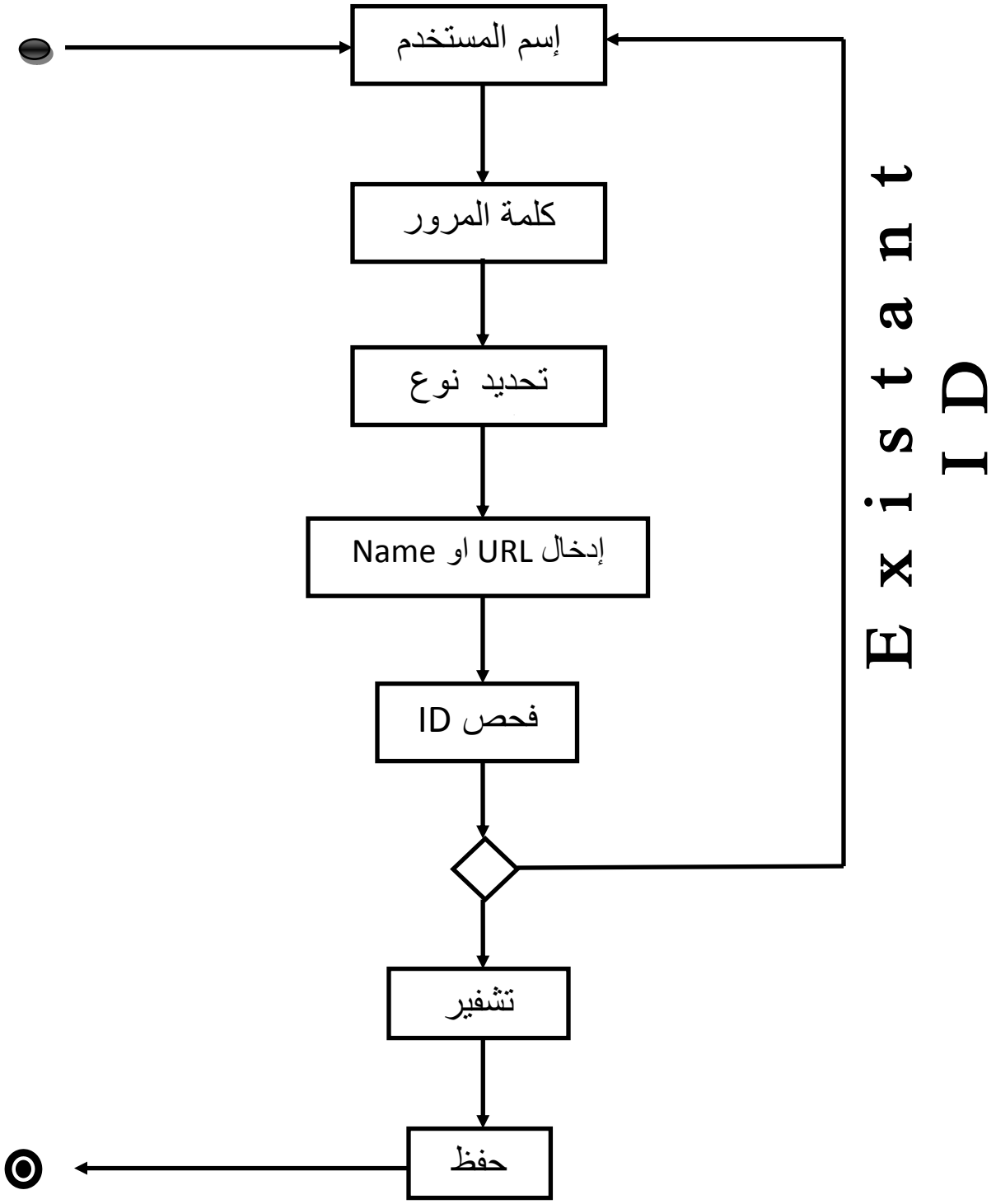


III-3) مخططات النشاط:

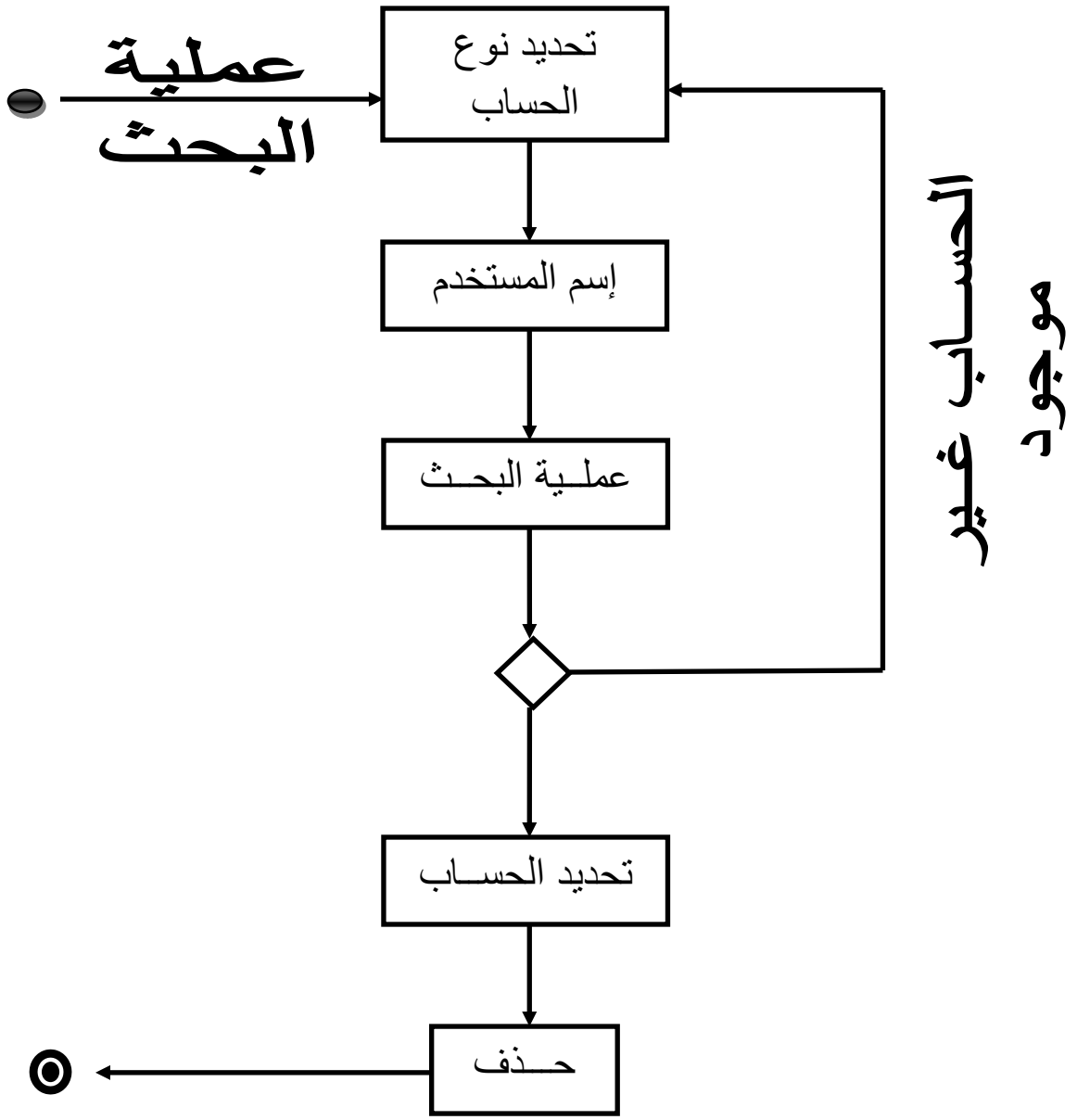
III-3-1) الدخول الى البرنامج:-



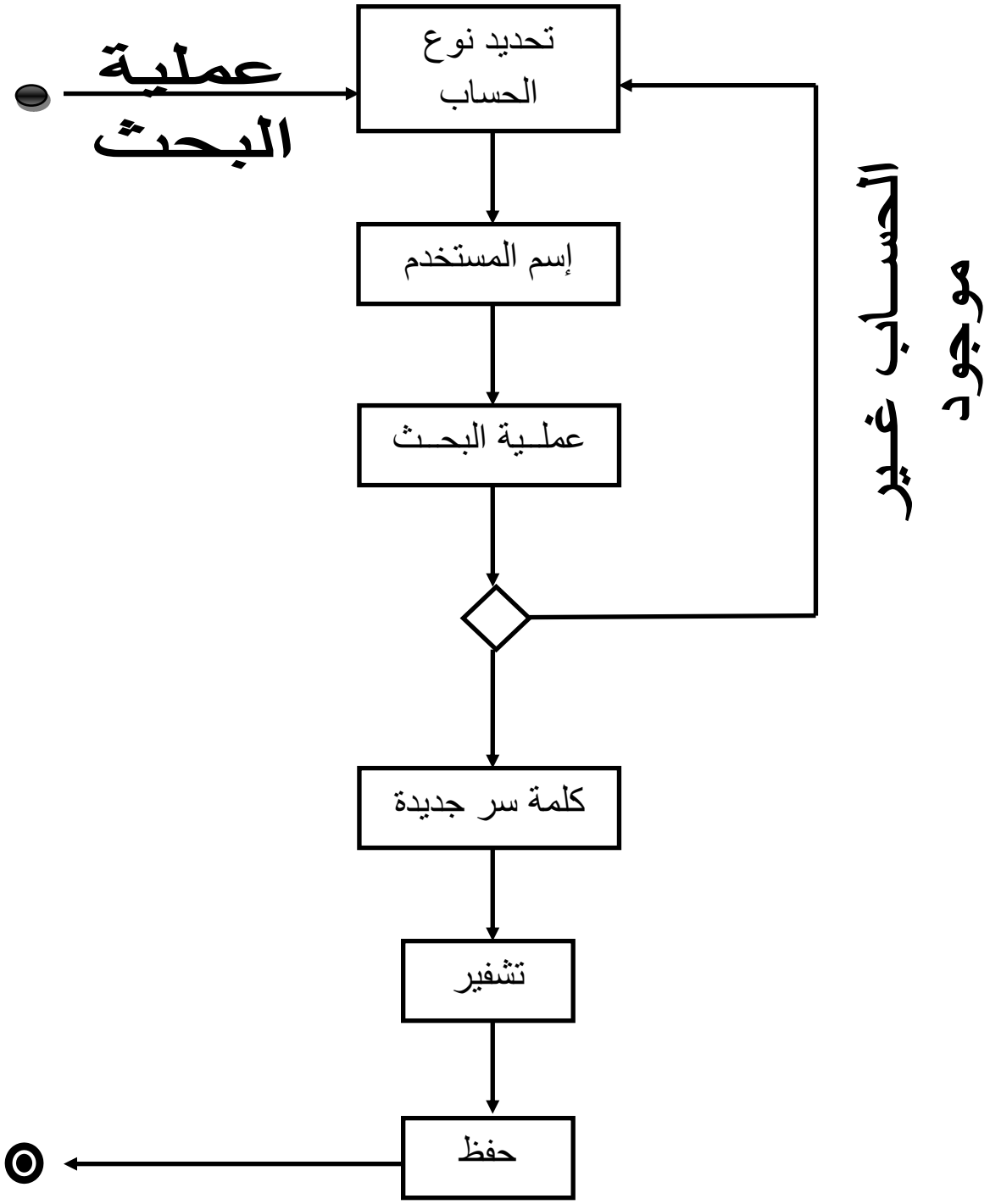
III-3-2) الإضافة:-



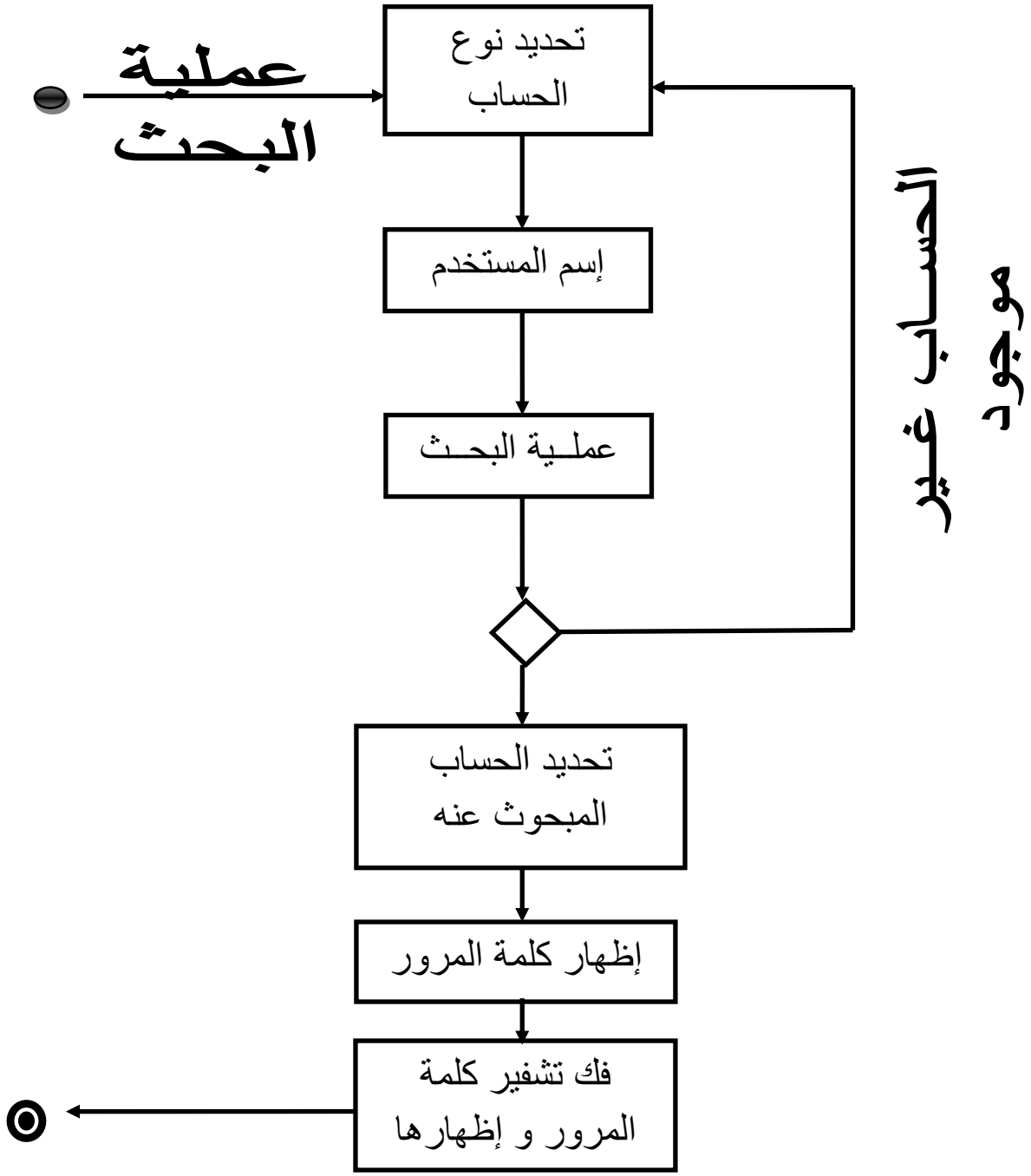
III-3-3) الحذف:-


عملية البحث
تحديد نوع الحساب
إسم المستخدم
عملـية البحـث
الحسـاب غير موجود
تحديد الحسـاب
حـذف

III-3-4) تعديل:-


عملية البحث
تحديد نوع الحساب
إسم المستخدم
عملـية البحـث
الحساب غير موجود
كلمة سر جديدة
تشفير
حفظ

III-3-5) الإطلاع على كلمة المرور:-




الفصل الثالث
التطوير و الإنشاء

I) مقدمة:

هذا الفصل مخصص للإدراك العملي الفعلي. سنتحدث فيه عن الأدوات المستخدمة مثل نظام إدارة قواعد البيانات ولغةالبرمجة المختارة. أخيرًا سنقدم رسومًا توضيحية للواجهات الرئيسية لـتطبيقنا

II)اللغات البرمجية : اللغة المستعملة في تصميم البرنامج هي C# و لغة SQL Server في تنضيم قواعد البيامات

C#: وهي لغة برمجة متعددة الأنماط تتمتع بكونها سكونية التنميط وأمرية وتعريفية ووظيفية وتعتبر كائنية التوجُّه أو البرمجة الشيئية وعمومية وشيئية المنحى (غرضية التوجه) (باستخدام الفئات) كما تخضع لمبادئ البرمجة التركيبية المنحى.

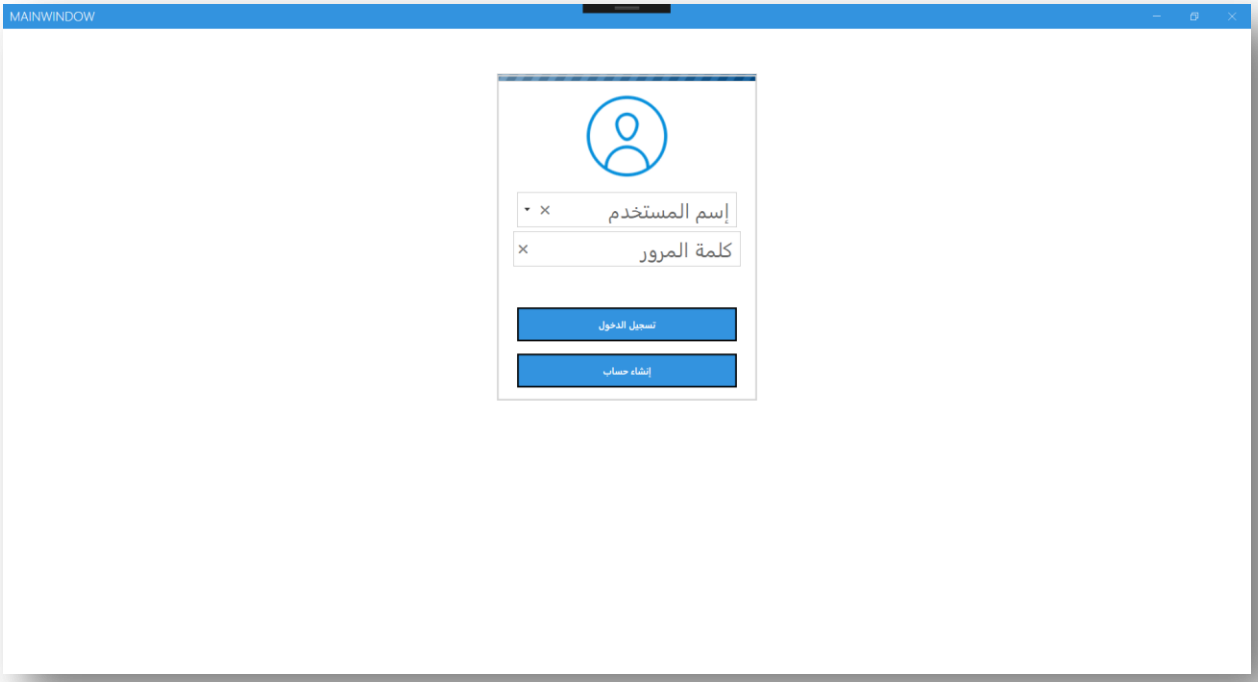
قامت مايكروسوفت بتطوير هذه اللغة في إطار عملها على تطوير NET.وتمت الموافقة على تعييرها من منظمة Ecma المعيار (Ecma-334) والمنظمة الدولية للمعايير (المعيار ISO/IEC 23270:2006) إن سي شارب إحدى لغات البرمجة المصممة للعمل على البنية التحتية المشتركة للغات البرمجة .(CLI) صُممت لغة سي شارب لتكون لغة بسيطة وحديثة وعامة الأغراض وشيئية المنحى.[4]

SQL Server:هي لغة برمجة غير إجرائية، وهي بذلك تختلف عن لغات البرمجة المعتادة مثل C أو JAVA، حيث أن اللغات غير الإجرائية هي لغات متخصصة. ولذلك فإن لغة الاستعلامات البنائية هي لغة للتعامل والتحكم مع قواعد البيانات المترابطة من خلال التعامل مع تراكيب البيانات وإجراء عمليات إدخال البيانات والحذف والفرز والبحث والتصفية والتعديل وخلافه.[5]

III) صور للبرنامج الذي تم تصميمه:

III-1) واجهة الدخول إلى البرنامج :

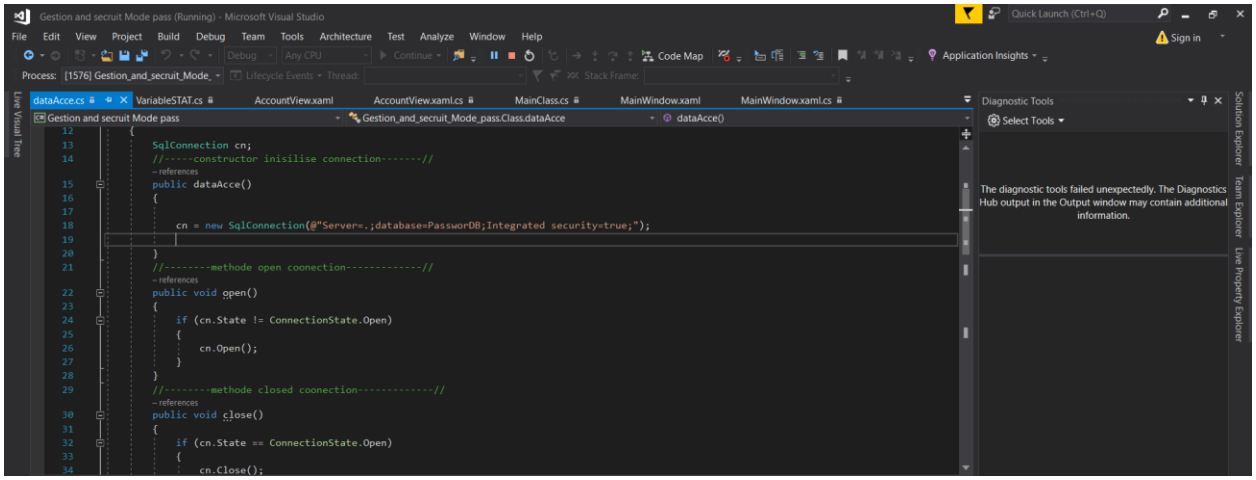
يمكننا في هذه الخطوة الدخول إلى حسابنا أو إنشاء حساب جديد



III-2)واجهة البرنامج من الداخل :

تحتوي هذه الخطوة على الإضافة و التعديل و الحذف و إظهار كلمة المرور

3-III) كود الإتصال بقاعدة البيانات :



المراجع

[1] : 02ABNT Catalogo أبريل 2018 على موقع Way Back Machine

[2] : 02 Symmetric-key encryption Software أغسطس 2017 على موقع Way Back Machine

[3]: من موقع معايير رخص المعلمين , رابط الموقع http://tc.hasibna.com/?page_id=373

[4]: توصيف لغة C#. 2006 .Ecma International. مؤرشف في 24 ديسمبر 2019. اطلع عليه بتاريخ 11 كانون الأول 2013.على موقع ecma . الرابط : https://www.ecma-international.org

[5] : Mimer SQL, Built on Standards". Mimer SQL official website. Mimer Information Technology. 2009. مؤرشف في 03 مايو 2016