الوحدة الأولى: الأمن السيبراني

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

مفهوم الأمن السيبراني (CyberSecurity):

يتعلق بحماية أجهزة الحاسب والشبكات والبرامج والبيانات من الوصول غير المصرح به، والذي قد يهدف إلى الحصول على المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل عمليات المؤسسة عموماً.

ويعبّر مصطلح الأمن السيبراني عن جميع الممارسات التي تتم لحماية المعلومات من المخاطر والهجمات التي تتمثل الوصول غير المصرح به بغرض الاستخدام غير المشروع أو التعديل أو الإتلاف أو النسخ غير المصرح أو تزوير المعلومات.

أهمية الأمن السيبراني:

كلما زادت أهمية البيانات والمعلومات المتوفرة على الشبكة وزاد عدد مستخدميها، تكون عرضة لهجمات القرصنة الحاسوبية بهدف السرقة أو الحجب عن المستخدمين، ويتمثل دور الأمن السيبراني في منع التهديدات الداخلية والخارجية واكتشافها والقيام بالاستجابة المناسبة لها حسب الضرورة.

أهداف أنظمة الجاهزية العالية:

الحفاظ على إمكانية الوصول إلى المعلومات في جميع الأوقات وعدم انقطاع الخدمة لأي سبب "كانقطاع التيار الكهربائي أو تعطل الأجهزة أو عمليات تحديثات النظام"، وتتضمن منع هجمات إيقاف الخدمة.

مفهوم مثلث الحماية (CIA):

التركيز على حماية متوازنة للمعلومات والبيانات من حيث السرية والتكامل والتوافر.

عناصر مثلث الحماية (CIA):

العنصر	الوصف	أمثلة على أساليب الحماية
السرية	إتاحة البيانات والمعلومات للأشخاص المعنيين بها والمسموح لهم فقط	اسم المستخدم وكلمة المرور
التكامل	الحفاظ على دقة المعلومات وصحّتها، وعدم تعديلها إلّا من الأشخاص المصرح لهم.	تحديد الأذونات والصلاحيات، التشفير
التوافر	ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة	الحفاظ على سلامة الخوادم، النسخ الاحتياطي، التحديث، كفاءة الشبكة

الجرائم الإلكترونية (CyberCrime):

استخدام الحاسب والشبكة كأداة لتحقيق غايات غير قانونية مثل الاحتيال أو التوزيع غير القانوني للمواد المحمية بحقوق الطبع والنشر أو سرقة الهويات وانتهاك الخصوصية، ومن أمثلة الجرائم الإلكترونية:

- الاحتيال الإلكتروني: يتقمص المجرم دور جهة موثوقة يتعامل معها الضحية، للحصول على بيانات شخصية.
- سرقة الهوية: انتحال شخصية الضحية باستخدام بياناته المسروقة لإجراء معاملات مالية أو أعمال غير قانونية.
- المضايقات عبر الإنترنت: تهديدات عبر البريد الإلكتروني أو رسائل فورية أو مشاركات مسيئة في وسائل التواصل الاجتماعي.
- التسلل الإلكتروني: الوصول لأجهزة الضحايا باستخدام برامج ضارة للتجسس وجمع البيانات الخاصة.
- انتهاك الخصوصية: التطفل على الحياة الشخصية لشخص آخر، وذلك باختراق الحاسب أو قراءة البريد الإلكتروني أو مراقبة الأنشطة الشخصية الخاصة.

الاختراق الأمني (Security Breach):

تجاوز طرف غير مصرح به لتدابير الحماية للوصول إلى مناطق محمية من النظام، قد يؤدي إلى سيطرة المتسللين على معلومات قيّمة مثل حسابات الشركات ومعلومات العملاء الشخصية والتي تشمل الأسماء والعناوين وأرقام الهواتف والمعلومات البنكية.

الوحدة الأولى: الأمن السيبراني

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

اختراق البيانات:
يحدث نتيجة حدوث اختراق أمني وقد تحدث في مواضع مختلفة، حيث تؤدي سرقة كلمات المرور مثلاً إلى اختراق العديد من الأنظمة الأخرى

الهجمات الإلكترونية (Electronic Attacks):
هي محاولات لسرقة المعلومات أو كشفها أو تعطيلها أو إتلافها من خلال الوصول غير المصرح به إلى جهاز الحاسب، وهي أيضاً محاولة الوصول إلى نظام الحوسبة أو شبكة الحاسب بقصد إحداث ضرر.

هجمات (حجب الخدمات) و (حجب الخدمات الموزع):
هجمات إلكترونية تهدف إلى تعطيل توفر موارد شبكة معينة، مثل موقع ويب أو خادم:

- هجوم حجب الخدمات: يقوم جهاز حاسب واحد أو شبكة بإغراق موقع أو خادم مستهدف بحركة المرور، مما يؤدي إلى إرباكه وجعله غير متاح للمستخدمين.
- هجوم حجب الخدمات الموزع: هو إصدار أكثر تقدماً من السابق، فيه يتم استخدام العديد من أجهزة الحاسب والعديد من الشبكات لإغراق موقع ويب أو خادم مستهدف بحركة المرور، مما يجعل الدفاع ضده أكثر صعوبة.

هجوم الوسيط (Man-in-the-Middle):
نوع من الهجمات الإلكترونية يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق، ويبقى في منتصف الاتصال متظاهراً بأنه الطرف الآخر، ويمكنه قراءة أو تعديل أو إضافة البيانات خلال الاتصال، ويستخدم هذا الهجوم لسرقة معلومات حساسة أو نشر برامج ضارة، ويمكن مقاومة هذه الهجمات باستخدام التشفير والمصادقة، ومن أمثلة هجوم الوسيط الإلكتروني:

- التنصت على الواي فاي: إعداد شبكة واي فاي مخادعة تسمح باعتراض وقراءة البيانات للضحايا المتصلين بالشبكة المخادعة.
- انتحال أسماء النطاقات: إعادة توجيه الضحايا إلى موقع ويب ضار بدلاً من الموقع المقصود.
- التصيد الاحتيالي للبريد الإلكتروني: يقوم المهاجم باعتراض رسائل البريد الإلكتروني ويغيّر محتواها أو يضيف مرفقات وروابط ضارة لسرقة معلومات حساسة أو نشر البرامج الضارة.

تدابير ينصح باتخاذها للوقاية من الجرائم الإلكترونية:
- التحديث الدوري للبرامج لإزالة الثغرات الأمنية.
- استخدام برامج مكافحة الفيروسات وجدار الحماية فهي تساعد على حجب المتسللين والفيروسات والأنشطة الضارة.
- التواصل الرقمي الحذر وتجنب الرسائل مجهولة المصدر والتأكد من الروابط قبل فتحها وعدم مشاركة المعلومات الشخصية.
- استخدام كلمات مرور قوية ومعقدة وتغييرها بشكل دوري واستخدام أدوات إدارة كلمات المرور.
- التحقق الثنائي أو المتعدد وهي طريقة إضافية للوصول للمواقع والتطبيقات باستخدام رموز إضافية عبر الهاتف أو بصمة الإصبع أو التعرف على الوجه وغيرها....
- النسخ الاحتياطي الدوري للبيانات وذلك لاستعادة البيانات عند فقدانها أو تلفها.
- تجنب استخدام شبكات الواي فاي العامة.

حماية الحاسب الشخصي:
يجب حماية الحاسب الشخصي من السرقة أو التلف الذي يلحق بها أو بالبيانات الإلكترونية، وحماية الحاسب من البرمجيات الضارة.

البرمجيات الضارة:
تعدّ الفيروسات أحد أبرز البرمجيات الضارة وبرامج التجسس التي يتم تثبيتها على جهاز الحاسب دون موافقة ومعرفة المستخدم، وقد تتسبب في تعطل الأجهزة أو مراقبة أنشطة المستخدمين لها.

حالات قد تكون مؤشر لإصابة الجهاز بالبرمجيات الضارة:
بطء في الأداء، رسائل خطأ متكررة، عرض صفحات ويب لم نزرها، وجود برامج أو أشرطة أدوات غير متوقعة، عدم القدرة على أغلاق الجهاز، لا يمكن حذف التطبيقات غير المرغوب بها، استنزاف البطارية، كثرة إعلانات صفحات الويب، نوافذ منبثقة كثيرة.. وغيرها.

الوحدة الأولى: الأمن السيبراني

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

بعض أساليب الوقاية من البرمجيات الضارة:

تثبيت وتحديث مكافح الفيروسات، استخدام جدار الحماية، لا تفتح مرفقات البريد الإلكتروني المجهولة، تحميل البرامج من المواقع الموثوقة، لا تضغط على إعلانات تحسين أداء الجهاز، فحص وحدات التخزين الخارجية قبل استخدامها، النسخ الاحتياطي للبيانات....

التعامل مع البرمجيات الضارة في حال الاشتباه بوجودها في جهازك:

- التوقف عن التسوق الإلكتروني أو استخدام الخدمات المصرفية والتوقف عن الأنشطة التي تتطلب إدخال معلومات الحساسة.
- تحديث برنامج الحماية وفحص الحاسب للبحث عن الفيروسات وبرامج التجسس وحذف العناصر المشتبه بها.
- التحقق من المتصفح والتأكد من أدوات حذف البرمجيات الضارة وإعادة تعيين المتصفح إلى إعداداته الافتراضية.
- الاستعانة بالدعم الفني من خلال الاتصال بالشركة المصنعة للحاسب.

هجوم الفدية (Ransomware):

أحد البرمجيات الضارة ويقوم بقفل جهاز الحاسب أو منع الوصول إلى الملفات لابتزاز الضحية بدفع الأموال مقابل إلغاء تأمين القفل، وقد يرى المستخدم نافذة تعلمه عن هجوم الفدية وطلب الدفع.

المعلومات المتداولة عبر الإنترنت:

جميع المعلومات المتداولة عبر الإنترنت تسجل بشكل دائم في سجل رقمي مفصل للبيانات التي تتم معالجتها أو نقلها على القرص الصلب وخادم مزود خدمة الإنترنت وقواعد بيانات حكومية أو خاصة.

تفهرس شبكة الإنترنت صفحات الويب بشكل دوري، وأي معلومة يتم نشرها قد تبقى على شبكة الإنترنت للأبد.

البيانات التي يجمعها المتصفح عبر الإنترنت:

عند استخدام الإنترنت فإن المستخدم يترك معلومات رقمية يمكن أن تستخدمها المواقع الإلكترونية لتتبع أنشطتك والتعرف عليك، كموقعك، نوع جهازك ومواصفاته، المواقع التي تزورها، الإعلانات التي تضغط عليها، كلمات المرور وغيرها...

كيفية حماية جهاز الحاسب الشخصي من الهجمات الإلكترونية:

- حذف بيانات التصفح
- تعطيل النوافذ المنبثقة في المتصفح
- تمكين "ويندوز ديفندر سمارت سكرين" والذي يحمي جهازك من مواقع وتطبيقات الاحتيال الإلكتروني والبرامج الضارة

نصائح لتصفح الشبكات الاجتماعية بشكل آمن:

- الحذر من مشاركة الكثير من المعلومات ولا تشارك المعلومات الشخصية.
- ضبط إعدادات الخصوصية في الشبكات الاجتماعية.
- التحقق من الأشخاص الذين تتواصل معهم.
- التحقق من حسابك الخاص ومعرفة ما يمكن للآخرين مشاهدته عنك.
- معرفة سياسات جهة عملك ومعرفة ما يمكنك مشاركته.
- التحكم في المعلومات التي يتم مشاركتها مع مصادر خارجية.
- الحذر من الصداقات الكثيرة ومراعاة اختيار الأشخاص الجديرين بالثقة فقط.
- التعرف على كيفية منع المتنمرين وكيفية حظر الأشخاص.
- استخدام كلمات مرور قوية وتغييرها بشكل مستمر.

قيم وسلوكيات المواطنة الرقمية:

يجب تجنب نشر ما يمكن أن يُسيء لوطنك وقيمك وأخلاقك ومبادئك مثل الصور غير اللائقة، التعليقات السلبية، التعليقات العنصرية، المؤهلات الكاذبة والمعلومات السرية.

الوحدة الثانية: قواعد البيانات

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

قاعدة البيانات (Database):
مجموعة من البيانات المخزنة بشكل منظم ومترابط يسمح بالوصول إليها وتعديلها وإدارتها بسهولة.

نظام إدارة قواعد البيانات (DBMS):
برنامج مصمم لإنشاء قواعد البيانات وإدارتها، ويعمل كواجهة بين قاعدة البيانات والتطبيقات أو المستخدم الأخير لتسهيل الوصول للمعلومات في قاعدة البيانات واسترجاعها ومعالجتها.

تتميز نظم إدارة قواعد البيانات بالسرعة العالية في تخزين البيانات واستعادتها ومعالجتها ومنع محاولة وصول المستخدمين غير المصرح لهم، وتوفر النسخ الاحتياطي لحمايتها من الضياع.

مكونات قاعدة البيانات:
تحتوي قاعدة البيانات على جدول أول أكثر ويتكون من الآتي:

- الحقل: يشبه الحاوية، ويحتوي على نوع معين من البيانات مثل الاسم أو العمر أو العنوان.
- السجل: مجموعة من الحقول تحتوي على بيانات خاصة بعنصر معين في قاعدة البيانات.
- الجدول: بيانات منظمة في صفوف (سجلات) وأعمدة (حقول) تتعلق بموضوع مرتبط بالجداول الأخرى.

أمثلة على المؤسسات التي تستخدم نظم قواعد البيانات:
- المؤسسات التعليمية: تستخدم لحفظ سجلات الطلاب في ملفات أو جداول مختلفة كالاختبارات ومعلومات الطلاب.
- المستشفيات والمراكز الصحية: لحفظ سجلات المرضى وتحتوي على ملفات المرضى والأطباء والأجهزة الطبية وغيرها.
- الدوائر الحكومية: كإدارة المرور مثلاً، تحتوي قاعدة بياناتها على ملفات السيارات والحوادث وغيرها.
- البنوك: لحفظ بيانات العملاء كالمعلومات الشخصية والحسابات البنكية والودائع وغيرها.
- شركات التجارة الإلكترونية: إدارة نماذج المنتجات وطلبات العملاء ومعلومات الشحن وغيرها.

مزايا استخدام قاعدة البيانات:
- حفظ كم كبير من البيانات في مساحة تخزينية قليلة.
- سهولة البحث عن البيانات
- سهولة إضافة البيانات أو تعديلها أو حذفها.
- حماية وتأمين البيانات بطريقة أفضل من الملفات الورقية.
- تقليل الأخطاء من خلال خاصية التحقق من البيانات المدخلة.
- إمكانية مشاركة البيانات بين المستخدمين.
- توفير الوقت وزيادة الإنتاجية من خلال إنشاء التقارير وجدولتها تلقائياً.

مراحل بناء قاعدة البيانات:

المرحلة	الوصف
١. تحديد المتطلبات	تحديد الغرض من قاعدة البيانات والبيانات التي سيتم تخزينها
٢. تحليل المتطلبات	تحليل المتطلبات بالتفصيل لتحديد هيكل قاعدة البيانات وتحليل الجداول والحقول والعلاقات وغيرها
٣. تصميم قاعدة البيانات	يتم إنشاء مخطط لكيفية هيكلة قاعدة البيانات وتنظيمها بما فيها الجداول والحقول والعلاقات
٤. إنشاء قاعدة البيانات	البدء باستخدام برنامج لإنشاء قاعدة البيانات وإدخال البيانات وإنشاء الجداول والحقول وإعداد العلاقات
٥. اختبار قاعدة البيانات	اختبار قاعدة البيانات للتأكد من أنها تعمل كما هو متوقع واختبار إدخال البيانات واسترجاعها ومعالجتها
٦. صيانة قاعدة البيانات	تنفذ بانتظام للمحافظة على قاعدة البيانات مثل النسخ الاحتياطي ومراقبة الأداء وتحديث بنية قاعدة البيانات

يستخدم برنامج **مايكروسوفت أكسس** (Microsoft Access) لإنشاء قواعد البيانات وإدارتها.

الوحدة الثانية: قواعد البيانات

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

أنواع البيانات:

نوع البيانات هو تصنيف يحدد نوع البيانات التي يمكن تخزينها في حقل أو عمود من الجدول ومن أنواع البيانات: (النص – الرقم – التاريخ والوقت – الترقيم التلقائي – نعم ولا)

خصائص الحقل:

يمكن تحديد خصائص الحقل مثل: (حجم الحقل – تنسيق الحقل – القيمة الافتراضية – التحقق من الصحة – مطلوب*)

* الحقل المطلوب هو حقل يجب إكماله بقيمة قبل التمكن من حفظ السجل ولا يمكن تركه فارغاً.

المفتاح الأساسي:

هو حقل مميز وفريد لكل سجل لا يمكن تكراره في السجلات الأخرى، ويمكن استخدامه للإشارة للحقول الأخرى في نفس السجل.

حقل السجل المدني يمكن استخدامه كمفتاح أساسي في قاعدة البيانات حيث لا يمكن لشخصين أن يكون لهما نفس رقم السجل المدني.

المفتاح الأجنبي:

هو حقل أو مجموعة حقول تكون قيمته مطابقة لقيمة مفتاح أساسي في جدول آخر ويستخدم للربط بين الجداول.

علاقات الجداول

يستخدم المفتاح الأساسي لربط الجداول معاً، العلاقات تدمج البيانات في الجداول ويمكن استخراج البيانات المرتبطة من جداول مختلفة وهناك ثلاثة أنواع من العلاقات:

- علاقة رأس برأس (واحد إلى واحد): لكل معلم رقم وظيفي واحد، ولكل رقم وظيفي معلم واحد.
- علاقة رأس بأطراف (واحد إلى متعدد): كل معلم يعمل في مدرسة واحدة في حين أن المدرسة بها أكثر من معلم.
- علاقة أطراف بأطراف (متعدد إلى متعدد): لكل معلم العديد من الطلبة، ولكل طالب العديد من المعلمين.

أدوات أخرى لقاعدة البيانات:

- النموذج: واجهة رسومية تمكن المستخدم من إدخال البيانات المحفوظة وتحريرها وعرضها في قاعدة البيانات بكل سهولة وبشكل أفضل وأكثر فعالية.
- الاستعلام: استرجاع البيانات من جدول أو أكثر وفق معايير يحددها المستخدم.
- التقرير: عرض البيانات وتنسيقها وطباعتها بأشكال وتنسيقات مختلفة وجذابة وتقسيم البيانات إلى فئات تسهل قراءتها.

الوحدة الثالثة: البرمجة المتقدمة في بايثون

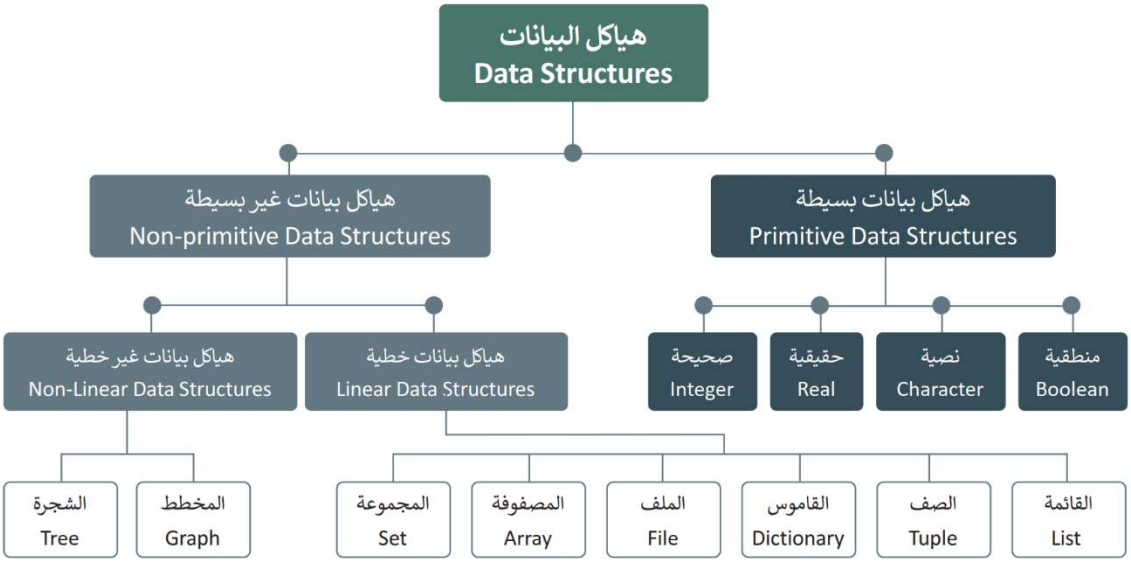
هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

القوائم وصفوف البيانات:

تستخدم القوائم وصفوف البيانات في البرمجة، وقد تحتوي القائمة أو الصف على أي نوع من الكائنات(Objects)، ويختار المبرمج الصفوف أو القوائم خلال البرمجة وحسب نوع المشكلة المراد حلها بعد الاطلاع على مزايا وعيوب هذه الأنواع من هياكل البيانات.

هياكل البيانات (Data Structures):

تعدّ هياكل البيانات وسيلة لتخزين وتنظيم البيانات في ذاكرة الحاسب، ويمكن تصنيفها على النحو الآتي:



هياكل البيانات البسيطة:

تحتوي على قيم بسيطة من البيانات وهي:

- الأرقام الصحيحة (Integers): مثل 1 ، 4 ، 18-
- الأرقام العشرية (Floating Points): مثل 3.14 ، 56.232
- النصوص (Strings): مجموعات نصية تتكون من أحرف وكلمات.
- البيانات المنطقية (Boolean): تأخذ قيمتي صواب (True) و خطأ (False).

هياكل البيانات غير البسيطة:

هياكل متخصصة تخزن مجموعة من القيم، يتم إنشاء هذه الهياكل بواسطة المبرمج ولا يتم تعريفها بواسطة بايثون كما هو الحال في هياكل البيانات البسيطة، ويتم تصنيف هياكل البيانات غير البسيطة إلى:

- هياكل البيانات الخطية: تخزن البيانات بصورة متسلسلة أو متتالية.
- هياكل البيانات غير الخطية: لا تحتوي على ارتباط تسلسلي بين عناصر البيانات ويمكن ربط أي مجموعة من عناصر البيانات ببعضها بدون تسلسل محدد.

القائمة (List):

أحد أكثر هياكل البيانات الخطية استخداماً في بايثون، وتتكون من سلسلة مرتبة من كائنات مستخدمة لتخزين البيانات بأنواعها، حيث لا يشترط أن تكون عناصر القائمة من نفس النوع، ويتم فصل عناصر القائمة بإضافة الفواصل بينها وذلك داخل أقواس مربعة، ويمكن تعريفها بالصيغة:

```
List_Name=[item1,item2,...,itemN]
```

متغير يمثل اسم القائمة.
عناصر القائمة.

الوحدة الثالثة: البرمجة المتقدمة في بايثون

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

فهرسة القوائم (List Indexing):

يتميز كل عنصر في القائمة برقم تسلسلي فريد يسمى الفهرس ويحدد موقعه داخل القائمة ويمكن للمستخدم الوصول إلى عناصر القائمة بكتابة اسم القائمة والرقم التسلسلي للعنصر بين قوسين مربعين، وتبدأ الفهرسة من العدد (0) وليس من العدد (1).

دوال بايثون التي يمكن استخدامها مع القوائم:

- الدالة len( ) : ترجع عدد عناصر القائمة أو عدد حروف المتغير النصي أو عدد خانات متغير رقمي.
- الدالة sum( ) : ترجع مجموع عدة عناصر.
- الدالة max( ) : ترجع قيمة أكبر عنصر في القائمة.
- الدالة min( ) : ترجع قيمة أصغر عنصر في القائمة.
- الدالة listName.append(x) : تضيف العنصر (x) لنهاية القائمة.
- الدالة listName.remove(x) : تزيل العنصر (x) من القائمة.
- الدالة listName.count(x) : تحسب عدد مرات ظهور العنصر (x) داخل القائمة.
- الدالة listName.sort( ) : ترتب عناصر القائمة.
- الدالة listName.reverse( ) : ترتب عناصر القائمة عكسياً.
- الدالة listName.clear( ) : تزيل كافة العناصر من القائمة.

يجب استبدال
listName
باسم القائمة التي أنشأتها

صفوف البيانات (Tuples):

أحد هياكل البيانات الخطية في بايثون، ويضم عدداً مرتباً من البيانات، ويمكن أن يخزن داخلها أي نوع من القيم، يكتب على شكل قائمة من القيم بينها فواصل داخل أقواس دائرية، ولا يمكن تغيير القيم في الصف "هيكل بيانات غير قابل للتعديل"، ويمكن تعريفه بالصيغة:

```
tuple_name=(item1,item2,...,itemN)
```

متغير يمثل اسم الصف.

عناصر الصف.

فهرسة الصفوف (Tuples Indexing):

تتم فهرسة عناصر الصف برقم فريد، كما في القوائم، ويمكن للمستخدم الوصول إلى عناصر الصف بكتابة اسم الصف والرقم التسلسلي للعنصر بين قوسين دائريين، وتبدأ الفهرسة من العدد (0) وليس من العدد (1).

المكتبات البرمجية (Programming Library):

تُعَدّ المكتبة البرمجية مجموعة من التعليمات البرمجية المدمجة سابقاً في لغات البرمجة، وتستخدم لتقليل الوقت المستغرق في البرمجة الفعلية، ويمكن إعادة استخدامها في أي برنامج، لأنها مستقلة عن البرامج التي يتم كتابتها، ومن خصائص المكتبة البرمجية ما يلي:

- يمكن كتابتها بأي لغة برمجة، وتستخدم غالباً في تطوير بيئات تطوير البرامج.
- مفيدة للوصول للتعليمات البرمجية المكتوبة سابقاً والمستخدمة بشكل متكرر بدلاً من كتابتها من الصفر في كل مرة.
- تنظم المكتبة البرمجية بحيث يمكن استخدامها من قبل برامج ذات طبيعة مختلفة.
- تستدعى الوظيفة أو المهمة التي تقدمها المكتبة البرمجية عبر آلية تتوفر في لغة البرمجة.
- يحتاج المستخدم فقط إلى معرفة وظيفة المكتبة البرمجية وليس تفاصيلها الداخلية.

المكتبات في بايثون:

النموذج البرمجي هو حزمة من الملفات تحتوي مقاطع برمجية تسمح لك بتنفيذ العديد من الإجراءات دون كتابة مقطع برمجي كبير، يتم استيرادها إلى البرنامج لتنفيذ وظائف مختلفة، ويكون امتدادها عادةً (py).

تتوفر في بايثون مكتبة قياسية ويمكن الوصول إلى الآلاف من المكتبات التي بُنيَت من قبل المطورين حول العالم.

الوحدة الثالثة: البرمجة المتقدمة في بايثون

هذا الملخص للمراجعة فقط
ولا يغني عن كتاب الطالب

أمثلة النماذج البرمجية القياسية في بايثون:

- واجهة المستخدم الرسومية (tkinter module).
- معرفة خصائص الحاسب ونظام التشغيل (Platform module).
- نموذج السلحفاة (turtle module).
- أوبين بيكسل (openpyxl module).

مكتبة بايثون القياسية:

مكتبة بايثون القياسية تشير إلى النموذج البرمجي الذي يُثبّت تلقائيا عند تثبيت بايثون، وتكون جزءاً أساسياً من لغة بايثون، وتحتوي هذه المكتبة على أكثر من ٢٠٠ نموذج برمجي.

يمكن تنزيل مكتبات إضافية وتثبيتها لإضافة دوال أخرى قد تحتاجها في برامج أخرى، بمجرد تثبيتها فإنها تتصرف كبقية مكتبة بايثون القياسية.

استخدام مكتبة بايثون القياسية:

لاستخدام نماذج مكتبة بايثون القياسية أنت بحاجة فقط إلى استيراد نماذجها البرمجية إلى البرنامج عن طريق إضافة سطر أوامر في أعلى المقطع البرمجي، وهناك عدة طرق للقيام باستيراد نماذج المكتبة القياسية وأكثرها شيوعاً:

١. استيراد الكل: وذلك بتضمين كافة محتويات المكتبة في المقطع البرمجي، وتتميز بتوفير الوقت للكتابة عند الحاجة لاستخدام الكثير من الدوال وتفيد عند الحاجة لدالة لا تتذكر إلى أي نموذج برمجي تنتمي، ومن عيوبها زيادة المقطع البرمجي في البرنامج دون حاجة وزيادة أعباء الصيانة والأمن.
٢. استيراد الدوال التي تحتاجها فقط من نموذج برمجي.
٣. استيراد النماذج البرمجية

النماذج البرمجية الأكثر استخداماً في المكتبة القياسية:

- نموذج sys البرمجي: يساعد المطور على معرفة خصائص النظام الخاص بجهاز المستخدم ومشغل بايثون الذي ثُبّت على الجهاز.
- نموذج os البرمجي: يستخدم للتفاعل مع جهاز المستخدم وإجراء العديد من مهام نظام التشغيل تلقائياً مثل إنشاء مجلد وإزالته وجلب محتوياته وتغيير المسار الحالي وغيرها.
- نموذج dir() البرمجي: تستخدم لمعرفة محتويات نموذج برمجي.
- نموذج math البرمجي: تُعرّف بعض الدوال الرياضية الأكثر شيوعاً.
- نموذج تكينتر tkinter البرمجي: لإنشاء واجهة المستخدم الرسومية.
- نموذج time البرمجي: يوفر دوال للعمل مع الأوقات.
- نموذج datetime البرمجي: يوفر دوال للعمل مع التواريخ والوقت.

مدير حزم بايثون:

يساعد مدير حزم بايثون (Python PIP) في تثبيت حزم إضافية غير متوفرة في مكتبة بايثون القياسية.

الألوان في بايثون:

تتوفر في النموذج البرمجي "تكينتر" جميع الألوان مع درجاتها وهناك طريقتان لتحديد هذه الألوان:

١. استخدام اسم لون معياري محدد "أبيض – أسود – أحمر – أزرق – أخضر – سماوي – أصفر – أرجواني"
٢. يمكن استخدام نموذج ألوان RGB: وهو نموذج ألوان يستخدم لتمثيل ألوان الصور في الأنظمة الإلكترونية والتصوير الفوتوغرافي، ويعتمد على استخدام ثلاثة أرقام تتراوح بين (0) و (255) تحدد نسبة الأحمر والأخضر والأزرق لتمثيل جميع الألوان.

الإحداثيات في بايثون:

تكون نقطة الإحداثيات (0,0) موجودة في الزاوية اليسرى العليا من لوحة الرسم، وتزداد قيمة x كلما اتجهنا يميناً، بينما تزداد قيمة y كلما اتجهنا للأسفل.