

دليل المعلم الإرشادي الشامل والموسوعي لتدريس منهج البرمجة والذكاء الاصطناعي

الصف الثاني الثانوي – الفصل الدراسي الأول (العام الدراسي 2026 / 2027)

إشراف وتنسيق تربوي وهندسي: المهندس / السيد سامي أفندي
المراجع الحصرية المعتمدة: كتاب وزارة التربية والتعليم والتعليم الفني الرسمي (95 صفحة) + المذكرة الشاملة المعتمدة (50 صفحة)

استراتيجية إدارة الحصة النموذجية (معمارية ال 45 دقيقة)

مرحلة الحصة	الزمن المقترح	الإجراء التدريسي المعتمد للمعلم داخل الفصل
1. التهيئة والعصف الذهني	5 دقائق	طرح السؤال الاستقصائي المعتمد من واقع الحياة اليومية للطالب لربط الدرس بالواقع.
2. التأسيس والعمق التقني	15 دقيقة	شرح الركائز والمفاهيم العميقة ومصطلحات الفيزياء والحوسبة (الصفحة الأولى من المذكرة).
3. التطبيق وركن المهندس	15 دقيقة	تنفيذ النشاط المعلمي وحل سيناريو «مهندس: فكر وقرر» (الصفحة الثانية بالمذكرة).
4. تفكيك الفخاخ الامتحانية	5 دقائق	مناقشة كادر ` ⚠️ فخ امتحاني وزاري ` لتحسين الطالب ضد المشتتات وأخطاء الصياغة.
5. التقويم وتذكير الخروج	5 دقائق	حل السؤال المقالي الوزاري (نظام ال 6 درجات) والتحقق من تحقيق نواتج التعلم.

الفصل الأول: تكنولوجيا المعلومات والمجتمع (الوحدة الأولى)

الدرس 1-1: تطور تكنولوجيا المعلومات والتحول الاجتماعي

- النطاق المعتمد: كتاب الوزارة (ص 5 - 12) | المذكرة الشاملة (ص 3 - 4).
- سؤال التهيئة الاستقصائي (5 ق):

«إذا اشترى زميلك إفطاره اليوم بتطبيق دفع ومسح رمز QR، ثم رفع واجبه على Google Drive؛ كم مرحلة تاريخية من تكنولوجيا المعلومات اجتمعت في هذه اللحظة؟»

- خريطة التدريس والمفاهيم الأساسية (15 ق):

- رسم الخط الزمني للمراحل ال 5 (الأربعينيات: الصمامات المفرغة و ENIAC → السبعينيات: الحواسيب الشخصية والمعالجات → التسعينيات: شبكة الويب WWW → العقد الأول: الهواتف الذكية → العقد الثاني: السحابة والذكاء الاصطناعي).
 - شرح قانون مور (تضاعف عدد الترانزستورات كل عامين وانخفاض التكلفة).
 - المقارنة بين الحوسبة السحابية (Cloud) والطرفية (Edge) والكمومية (Quantum).
- ركن العمق التقني للمعلم (كيف تشرح المفاهيم المعقدة للطالب الذكي؟):

* 1. ما هو النفق الكمومي (Quantum Tunneling)؟

* الشرح للمعلم: عندما نقوم بتصغير الترانزستور ليصل شُك بوابته العازلة إلى بضعة نانومترات (أبعاد ذرية)، تفقد الإلكترونات سلوكها كجسيمات مادية صلبة وتتصرف وفق ميكانيكا الكم كموجات احتمالية. هذا يسمح للإلكترون باختراق الحاجز العازل والقفز عبره دون وجود جهد كهربائي كافٍ! * التشبيه للطلاب: * تخيل جداراً سميكاً لا تستطيع المرور منه، لكن عندما يصبح الجدار برقة ورقة سيارة، تستطيع طاقتك الموجية العبور من خلاله كشبح! هذا الاختراق يعني أن الترانزستور لم يعد بالإمكان إغلاقه بالكامل (لا يثبت على الصفر 0).

* 2. ما هي تيارات التسرب (Leakage Currents)؟

* الشرح للمعلم: نتيجة النفق الكمومي، تتسرب الإلكترونات باستمرار عبر البوابة حتى عندما يكون الترانزستور في وضع إيقاف التشغيل (Off). هذا التسرب يولد طاقة حرارية مهددة مستمرة، مما أدى لظهور ما يُعرف بـ (Thermal Wall)؛ حيث لا يمكن زيادة تردد المعالج (Clock Speed) دون

أن يحترق!

* 3. الحل الهندسي (لماذا تعددت الأنوية Multi-core؟):

بدلاً من زيادة سرعة نواة واحدة وتوليد حرارة خانقة، لجأ المهندسون إلى وضع نواتين و4 و8 أنوية تعمل بتوازي (Parallel Processing) بترددات معتدلة لتوفير طاقة أعلى بحرارة أقل.

* 4. الكيوبت (Qubit) وخاصية التراكب الكمومي (Superposition):

البت التقليدي إما 0 أو 1. أما الكيوبت فيمكن أن يمثل (0 و 1) معاً في نفس اللحظة بفضل التراكب الكمومي، مما يضاعف القوة الحسابية بشكل أسّي (2^n).

• التطبيق المعلمي وركن المهندس (15 ق):

* نشاط كتاب الوزارة ص 11: توجيه الطلاب لتحليل المجتمع غير النقدي (Cashless Society): ما أثره على صاحب متجر صغير؟ وعلى مسن لا يحمل هاتفاً ذكياً؟

• الفخ الامتحاني الوزاري (كتاب الوزارة ص 8):

تنبيه الطلاب: إياك أن تختار في الامتحان أن "قانون مور" قانون فيزيائي حتمي! هو ملاحظة تجريبية وتاريخية صاغها جوردون مور، وتواجه اليوم حدوداً فيزيائية (النفق الكمومي).

• التقويم وتذكرة الخروج (5 ق):

حل السؤال المقالي (المذكرة ص 4): «حلل كيف غير انتشار الحوسبة السحابية طريقة استهلاك التكنولوجيا من تملك العتاد إلى خدمات عند الطلب (As a Service)؟»

📌 الدرس 1-2: كيف يعمل الذكاء الاصطناعي

• النطاق المعتمد: كتاب الوزارة (ص 13 - 18) | المذكرة الشاملة (ص 5 - 6).

• سؤال التهيئة الاستقصائي (5 ق):

«عندما يكتب لك ChatGPT مقالاً كاملاً أو يقترح YouTube فيديو يطابق ذوقك بدقة؛ هل يفكر الحاسوب مثل عقل الإنسان، أم يطبق معادلات رياضية على بيانات سابقة؟»

• خريطة التدريس والمفاهيم الأساسية (15 ق):

1. رسم الدوائر الهرمية: الذكاء الاصطناعي (AI) → التعلم الآلي (ML) → التعلم العميق (DL) → الذكاء الاصطناعي التوليدي (GenAI).

2. المقارنة بين البرمجة التقليدية والتعلم الآلي.

3. شرح ظاهرة "الهلوسة" (Hallucination) والتحقق من المخرجات.

• ركن العمق التقني للمعلم:

* 1. لماذا يُعد التعلم العميق (Deep Learning) عميقاً؟

لأنه يستخدم شبكات عصبية اصطناعية (Artificial Neural Networks) تحتوي على طبقات خفية متعددة (Multiple Hidden Layers) بين المدخلات والمخرجات. كل طبقة تستخلص خصائص مجردة أعلى: الطبقة الأولى تكتشف الخطوط والزوايا، الثانية تكتشف الأشكال والأنسجة، والثالثة تكتشف الوجوه الكاملة!

* 2. ما الميكانيكية الحقيقية لظاهرة الهلوسة (Hallucination)؟

النماذج اللغوية الكبيرة (LLMs) لا تفهم الحقائق ولا تملك قاعدة بيانات للمعلومات الصحيحة؛ هي تعمل بآلية التنبؤ بالرمز/الكلمة التالية الأكثر احتمالاً إحصائياً (Next-Token Prediction). إذا لم تجد الكلمة الحقيقية، ستختار كلمة تتناسب لغوياً وسياقياً بنسبة عالية حتى لو كانت كاذبة تماماً وتاريخياً وهماً!

* 3. التعلم الخاضع للإشراف (Supervised) مقابل غير الخاضع (Unsupervised):

في التعلم الخاضع للإشراف، نعطي النموذج البيانات وتسمياتها الصحيحة (Labelled Data) مثل: صورة قطة مكتوب عليها "قطة". أما غير الخاضع، فيترك النموذج لاكتشاف الأنماط والمجموعات المتشابهة ذاتياً (Clustering) دون تسميات مسبقة.

• التطبيق المعلمي وركن المهندس (15 ق):

* نشاط كتاب الوزارة ص 16: تجربة صياغة أوامر (Prompts) على نموذج ذكاء اصطناعي توليدي، ورصد حالات الهلوسة، ووضع استراتيجيات للتحقق من المخرجات عبر مراجع موثوقة.

• الفخ الامتحاني الوزاري (كتاب الوزارة ص 14):

التحذير من الخلط الهرمي: **التعلم العميق جزء فرعي من التعلم الآلي** مبني على الشبكات العصبية، وليس بديلاً أو مظلة مستقلة عنه.

• **التقويم وتذكرة الخروج (5 ق):**

سؤال سريع: «ما الفرق بين النموذج التنبئي (Predictive) والنموذج التوليدي (Generative) مع ذكر مثال لكل منهما؟»

📌 الدرس 1-3: الذكاء الاصطناعي في الحياة اليومية والصناعة

• **النطاق المعتمد:** كتاب الوزارة (ص 19 - 24) | المذكرة الشاملة (ص 7 - 8).

• **سؤال التهيئة الاستقصائي (5 ق):**

«إذا شُخص نظام ذكاء اصطناعي أشعة مريض وقال بنسبة 95% يوجد ورم؛ هل يُسمح للنظام بإجراء الجراحة فوراً أم يتدخل الطبيب؟ ولماذا؟»

• **خريطة التدريس والمفاهيم الأساسية (15 ق):**

1. مجالات الاستخدام: الرعاية الصحية، النقل الذكي، التعليم المخصص، والصناعة الذكية.

2. نقاط القوة: كشف الأنماط الخفية في ملايين البيانات، العمل المستمر 24/7 دون إجهاد.

3. نقاط الضعف: غياب الفهم السياقي، انعدام التعاطف والحس السليم.

• **ركن العمق التقني للمعلم:**

* 1. كيف تعمل الصيانة التنبؤية (Predictive Maintenance)؟

عبر تركيب حساسات إنترنت الأشياء (IoT Sensors) على الماكينات في المصانع (لقياس الاهتزازات الدقيقة، ودرجة الحرارة، ومستوى الصوت). يقوم نموذج التعلم الآلي بمقارنة هذه القراءات الحالية مع الأنماط التي سبقت الأعطال في السنوات الماضية، فيحذر المهندس: "محمل الموتور سيتلف بعد 48 ساعة"؛ مما يمنع توقف خط الإنتاج المفاجئ.

* 2. ما الفرق الجوهرى بين الصيانة الدورية والصيانة التنبؤية؟

الصيانة الدورية مجدولة بالزمن (مثل تغيير زيت السيارة كل 3 أشهر سواء استهلك أم لا). أما التنبؤية فتعتمد على الحالة الفعلية الدقيقة للقطعة لحظة بلحظة عبر الحساسات والذكاء الاصطناعي.

* 3. مبدأ الإشراف البشري الكامل (Human-in-the-Loop - HITL):

هو معيار أممي وأخلاقي يمنع الأتمتة الكاملة في القرارات الحيوية؛ حيث يعمل الذكاء الاصطناعي كنظام دعم قرار (Decision Support System) يقدم التوصيات، بينما يملك الإنسان المؤهل صلاحية الاعتماد أو الرفض النهائي.

• **التطبيق المعلمي وركن المهندس (15 ق):**

* نشاط كتاب الوزارة ص 22: تطبيق سيناريو «الإشراف البشري الكامل (HITL)» وتحديد حدود الأتمتة المقبولة طبياً وقضائياً.

• **الفخ الامتحاني الوزاري (كتاب الوزارة ص 21):**

الذكاء الاصطناعي **يفتقر للحس السليم والتعاطف الأخلاقي**؛ لذا لا يُترك له القرار النهائي المنفرد في المجالات الحيوية الحساسة.

• **التقويم وتذكرة الخروج (5 ق):**

حل تدريب ص 8 بالمذكرة: «علل: تُعد الصيانة التنبؤية أعلى كفاءة وأوفر تكلفة من الصيانة الدورية المجدولة؟»

📌 الدرس 1-4: القضايا الأخلاقية للذكاء الاصطناعي

• **النطاق المعتمد:** كتاب الوزارة (ص 25 - 31) | المذكرة الشاملة (ص 9 - 10).

• **سؤال التهيئة الاستقصائي (5 ق):**

«لو دُرِّبنا خوارزمية توظيف على ملفات شركة كانت توظف الرجال فقط طوال العشرين سنة الماضية؛ كيف ستتعامل الخوارزمية مع طلبات توظيف النساء اليوم؟»

• **خريطة التدريس والمفاهيم الأساسية (15 ق):**

1. شرح مفهوم التحيز الخوارزمي (Algorithmic Bias).

2. المبادئ الأخلاقية الأربعة: العدالة وعدم التمييز، الشفافية وقابلية التفسير (XAI)، حماية الخصوصية، والمساءلة القانونية.

3. معضلة الصندوق الأسود (Black Box Problem).

• ركن العمق التقني للمعلم:

* 1. لماذا تنشأ معضلة الصندوق الأسود (Black Box Problem)؟

النماذج العميقة تحتوي على مليارات المعاملات الرياضية والأوزان غير الخطية (Weights & Biases). نحن نعرف المدخلات بدقة، ونرى المخرجات، لكن العمليات الوسيطة في الطبقات الخفية معقدة لدرجة يعجز حق المهندس الذي صمم النموذج عن تقديم تفسير منطقي خطوة بخطوة لسبب اختيار قرار دون غيره!

* 2. ما هو الذكاء الاصطناعي القابل للتفسير (Explainable AI - XAI)؟

هي خوارزميات مساندة تهدف لتحويل الصندوق الأسود إلى صندوق زجاجي شفاف؛ حيث تُبرز الخصائص أو الكلمات أو المناطق في الصورة التي اعتمد عليها النموذج لإصدار قراره (Feature Attribution)، مما يسمح للأطباء والقضاة بالتحقق من منطقية القرار قبل اعتماده.

* 3. أين يقع التحيز الخوارزمي في دورة حياة النظام؟

التحيز لا يدخل في كود الخوارزمية (كود الرياضيات محيد)، بل يكمن في: (1) انحياز جمع البيانات التاريخية (Historical Bias)، (2) عدم توازن تمثيل الفئات في العينة (Representation Bias)، أو (3) أخطاء التسمية البشرية للبيانات.

• التطبيق العملي وركن المهندس (15 ق):

* نشاط كتاب الوزارة ص 29: تحليل حالة رفض قروض بنكية لحي سكاني معين بسبب انحياز البيانات التاريخية، واقتراح حلول لموازنة البيانات.

• الفخ الامتحاني الوزاري (كتاب الوزارة ص 26):

التحيز الخوارزمي لا ينشأ من سوء نية الخوارزمية ذاتها، بل ينعكس من بيانات التدريب التاريخية غير المتوازنة.

• التقويم وتذكرة الخروج (5 ق):

حل السؤال المقال (المذكرة ص 10): «كيف تسهم تقنيات الذكاء القابل للتفسير (XAI) في تفكيك معضلة الصندوق الأسود في المستشفيات؟»

الفصل الثاني: الأمن السيبراني (الوحدة الثانية)

📌 الدرس 1-2: تقنيات التشفير والمصادقة

• **النطاق المعتمد:** كتاب الوزارة (ص 32 - 38) | المذكرة الشاملة (ص 13 - 14).

• **سؤال التهيئة الاستقصائي (5 ق):**

«عندما يظهر قفل الأمان الأخضر HTTPS في متصفحك، كيف يتأكد جهازك أن الموقع بنك حقيقي وليس صفحة تصيد مزورة؟»

• خريطة التدريس والمفاهيم الأساسية (15 ق):

1. المقارنة بين التشفير المتماثل (Symmetric) وغير المتماثل (Asymmetric).

2. مصادقة TLS وتكامل بروتوكول HTTPS.

3. الشهادات الرقمية (Digital Certificates) وسلطات الاعتماد (CA).

4. فئات المصادقة متعددة العوامل (MFA).

• ركن العمق التقني للمعلم:

* 1. لماذا نستخدم نوعي التشفير معاً في HTTPS بدلاً من نوع واحد؟

* التشفير غير المتماثل (بالمفتاحين العام والخاص): * فائق الأمان لأنه يحل معضلة تبادل المفاتيح بأمان عبر شبكة مفتوحة، لكنه بطيء جداً ويستهلك قدرة المعالج في الحسابات الرياضية المعقدة.

* التشفير المتماثل (بالمفتاح المشترك): * فائق السرعة وخفيف، لكن عيبه الأكبر هو: كيف نرسل المفتاح المشترك للطرف الآخر دون أن يسرقه المخترق؟

* الحل العبقري في مصادقة TLS: * نستخدم التشفير غير المتماثل في أول 3 ثوانٍ فقط لنقل مفتاح جلسة سري (Session Key)، وبمجرد وصوله بأمان، يتحول الاتصال بالكامل للتشفير المتماثل فائق السرعة!

* 2. ما هو التوقيع الرقمي (Digital Signature) رياضياً؟

هو عملية تشفير قيمة تجزئة الرسالة (Hash Value) باستخدام المفتاح الخاص للمرسل. عندما يفك المستقبل التشفير باستخدام المفتاح العام للمرسل ويجد الهاش متطابقاً، يثبت شيئين قطعين: (1) الرسالة لم تُعدل أثناء الإرسال (السلامة Integrity)، و (2) الرسالة صادرة حتماً من صاحب المفتاح الخاص ولا يستطيع إنكارها (عدم التنصل Non-repudiation).

* 3. فئات عوامل المصادقة الثلاثة (MFA Factors):

- (1) ما تعرفه (Something you know: كلمة مرور، PIN).
- (2) ما تملكه (Something you have: هاتف يتلقى SMS، تطبيق مصادقة Authenticator، مفتاح أمني USB).
- (3) ما أنت عليه (Something you are: بصمة إصبع، بصمة وجه، بصمة صوت).

• التطبيق العملي وركن المهندس (15 ق):

* نشاط كتاب الوزارة ص 36: فحص شهادة الأمان لموقع ويب بالنقر على القفل واستخراج: اسم النطاق، تاريخ الصلاحية، وسلطة الإصدار CA.

• الفخ الامتحاني الوزاري (كتاب الوزارة ص 34):

المصادقة متعددة العوامل (MFA) تشترط الجمع بين فئات مختلفة؛ أما إدخال (كلمة المرور + سؤال الأمان) فهما فئة واحدة مكررة (ما تعرفه) ولا يُعدان MFA مطلقاً!

• التقويم وتذكرة الخروج (5 ق):

سؤال سريع: «ما الفرق الجوهرى بين وظيفة التشفير (السرية) ووظيفة التوقيع الرقمي (السلامة وعدم التنصل)؟»

📌 الدرس 2-2: تصميم أمن الشبكات

• النطاق المعتمد: كتاب الوزارة (ص 39 - 44) | المذكرة الشاملة (ص 15 - 16).

• سؤال التهيئة الاستقصائي (5 ق):

«إذا أرادت مدرستنا توفير موقع ويب عام للجمهور، وتخشى اختراق درجات الطلاب على السيرفر الداخلي؛ كيف نفصل بينهما شبكياً؟»

• خريطة التدريس والمفاهيم الأساسية (15 ق):

1. جدران الحماية (Firewalls) وقاعدة الرفض الافتراضي (Default Deny).
2. المنطقة منزوعة السلاح (DMZ) وتكوينها المعتمد (الشكل 2.2.1 ص 40).
3. الشبكة الافتراضية الخاصة (VPN) وتشفير النفق (Tunneling).
4. استراتيجية الدفاع في العمق (Defense in Depth).

• ركن العمق التقني للمعلم:

* 1. المعمارية الهندسية للمنطقة المعزولة (DMZ Architecture):

هي شبكة فرعية بسيطة (شبه موثوقة Semi-trusted) تقع بين الإنترنت العام غير الموثوق (Untrusted) والشبكة الداخلية للشركة عالية الموثوقية (Trusted). تعتمد عادة على جداري حماية:

- الجدار الناري الخارجي: يسمح فقط بحركة المرور للخدمات العامة (منفذ 80 و 443 للويب) للوصول إلى سيرفر الويب في DMZ.
- الجدار الناري الداخلي: يفصل DMZ تماماً عن الشبكة الداخلية، ويمنع أي اتصال يبدأ من خوادم DMZ باتجاه الشبكة الداخلية!
- * النتيجة الهندسية: إذا تمكن المخترق من السيطرة الكاملة على خادم الويب، سيجد نفسه محبوساً داخل DMZ ولا يستطيع القفز أفقياً (Lateral Movement) للوصول لسيرفر قواعد البيانات أو أجهزة الموظفين.

* 2. قاعدة الرفض الافتراضي (Default Deny / Implicit Deny):

في عالم أمن الشبكات: "كل ما لم يُسمح به صراحةً بالأعلى، فهو محظور ومرفوض تلقائياً". هذا يحمي النظام من المنافذ المفتوحة المنسية التي تستغلها الفيروسات كأبواب خلفية.

* 3. أرقام المنافذ القياسية (Standard Ports) التي تتكرر بالامتحانات:

- منفذ 80: لبروتوكول HTTP (غير مشفر).
- منفذ 443: لبروتوكول HTTPS (مشفر بـ TLS).
- منفذ 53: لنظام أسماء النطاقات DNS.