



مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

تكنولوجيا التشفير المتقدمة لحماية البيانات

مكان الإنعقاد : الإمارات العربية المتحدة - دبي

تاريخ الإنعقاد : 21 - 25 / 9 / 2025.





مقدمة :

في عصر الاعتماد المتزايد على التكنولوجيا الرقمية، أصبحت حماية البيانات أولوية قصوى للمؤسسات الحكومية والخاصة على حد سواء. التشفير هو أحد أهم الأدوات المستخدمة لضمان سلامة البيانات وسريتها، خصوصاً في ظل التهديدات المتزايدة التي تستهدف المعلومات الحساسة. مع تطور الهجمات السيبرانية، لم تعد الأساليب التقليدية كافية لحماية البيانات، لذا أصبح استخدام تقنيات التشفير المتقدمة ضرورة حتمية. يهدف برنامج "تكنولوجيا التشفير المتقدمة لحماية البيانات" إلى تزويد المشاركين بالمعرفة العميقة في مجالات التشفير المتقدم وكيفية تطبيقها لحماية البيانات الحساسة وضمان أمانها.

أهداف الورشة:

- فهم مبادئ التشفير المتقدمة وأهميتها في حماية البيانات.
- التعرف على نقاط الضعف في أنظمة التشفير التقليدية وكيفية التغلب عليها.
- إتقان مهارات استخدام خوارزميات التشفير المتقدمة (مثل AES, RSA, ECC).
- فهم مفهوم التشفير الكمي وتطبيقاته المحتملة في المستقبل.
- التعرف على دور البلوك تشين في تعزيز أمن البيانات.
- تطوير استراتيجيات شاملة لحماية البيانات باستخدام تقنيات التشفير المتقدمة.
- تطبيق المعرفة المكتسبة في اختيار وتنفيذ حلول التشفير المناسبة لحماية البيانات في بيئة العمل.

محتويات الورشة:

اليوم التدريبي الأول:

مقدمة إلى التشفير المتقدم

- مراجعة مبادئ التشفير الأساسية (التشفير المتماثل، التشفير غير المتماثل، التشفير باستخدام التجزئة).
- نقاط الضعف في أنظمة التشفير التقليدية وكيفية التغلب عليها.
- التعرف على أحدث التوجهات في مجال التشفير.
- ورشة عمل: تحليل نقاط ضعف في أنظمة تشفير شائعة واقتراح حلول.



اليوم التدريبي الثاني:

خوارزميات التشفير المتقدمة

- استعراض خوارزميات التشفير المتماثل المتقدمة (مثل AES مع أوضاع تشغيل مختلفة).
- استعراض خوارزميات التشفير غير المتماثل المتقدمة (مثل RSA مع مفاتيح طويلة، ECC).
- مقارنة بين الخوارزميات المختلفة من حيث الأمان والأداء.
- ورشة عمل: تطبيق خوارزميات التشفير المتقدمة باستخدام أدوات برمجية.

اليوم التدريبي الثالث:

التشفير الكمي

- مفهوم الحوسبة الكمومية وتأثيرها المحتمل على التشفير التقليدي.
- مبادئ التشفير الكمي (مثل توزيع المفتاح الكمي، التشفير الكمي).
- تطبيقات التشفير الكمي المحتملة في المستقبل.
- التحديات والفرص المتعلقة بالتشفير الكمي.
- ورشة عمل: استعراض أحدث التطورات في مجال التشفير الكمي ومناقشة تطبيقاته المحتملة.

اليوم التدريبي الرابع:

البلوك تشين وأمن البيانات

- مفهوم البلوك تشين ومزاياه في أمن البيانات (مثل اللامركزية، الشفافية، عدم القابلية للتغيير).
- تطبيقات البلوك تشين في حماية البيانات والتحقق من الهوية.
- التحديات والفرص المتعلقة باستخدام البلوك تشين في أمن المعلومات.
- ورشة عمل: تصميم تطبيق بسيط قائم على البلوك تشين لتأمين البيانات.



اليوم التدريبي الخامس:

استراتيجيات حماية البيانات

- تطوير استراتيجيات شاملة لحماية البيانات باستخدام تقنيات التشفير المتقدمة.
- إدارة المفاتيح وتخزينها بشكل آمن.
- التعامل مع حوادث الاختراق الأمني واستعادة البيانات.
- أفضل الممارسات في حماية البيانات.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.