الاجابة النموذجية لامتحان المعلومات والوثائق الرقمية

السؤال الأول: 4ن يُعتبر الموقع الإلكتروني وثيقة رقمية لعدة أسباب:

1. **الإتاحة الإلكترونية :**المواقع الإلكترونية موجودة على خوادم (Servers) ويمكن الوصول إليها عبر الإنترنت في أي وقت ومن أي مكان، مما يطابق الخصائص الأساسية للوثائق الرقمية التي تتمثل في الإتاحة عبر الوسائط الرقمية.
2. **تنوع المحتوى الرقمي :**المواقع تحتوي على محتويات متعددة الأشكال (نصوص، صور، فيديوهات، جداول، روابط)، وهذه العناصر تندرج ضمن أنواع الوثائق الرقمية. فعلى سبيل المثال:
   - صفحة في موقع إخباري تحتوي على مقال مكتوب، وهو نص رقمي.
   - صفحة تعليمية تحتوي على فيديوهات تعليمية، وهي ملفات فيديو رقمية.
   - صفحة تفاعلية تحتوي على استمارات إلكترونية، وهي أيضاً جزء من المحتويات الرقمية.
3. **التخزين الرقمي :**يتم تخزين محتويات الموقع الإلكتروني على خوادم في شكل ملفات رقمية يمكن استرجاعها ومعالجتها من خلال الويب، مما يجعل الموقع يتماشى مع مفهوم الوثائق الرقمية التي تُخزن وتدار إلكترونيًا.
4. **إمكانية التعديل والتحديث :**مثل الوثائق الرقمية الأخرى، يمكن تحديث محتويات المواقع الإلكترونية بسهولة وإضافة أو إزالة المعلومات حسب الحاجة. هذا التعديل يمكن أن يتم بشكل مستمر، مما يجعل الموقع الإلكتروني وثيقة حية ومتجددة.
5. **إمكانية الأرشفة :**المواقع الإلكترونية يمكن أرشفتها باستخدام أدوات مثل"Wayback Machine" ، مما يعني أنه يمكن حفظ نسخ من الموقع بشكل دائم كوثائق رقمية يُعاد الوصول إليها لاحقًا، حتى لو تم تعديل أو حذف المحتويات الأصلية.

السؤال الثاني: 4ن يحقق الارشيف المفتوح العدالة العلمية من خلال انه يساعد في زيادة شفافية البحوث العلمية عندما يتم نشر المعلومات المستخدمة في الدراسات بشكل مفتوح وبهذا يمكن للباحثين والمهتمين التحقق من النتائج وإعادة تحليل المعلومات مع إمكانية مراجعة النتائج والأبحاث و التحقق من صحة النتائج والتأكد من استدامتها. كما يمكن الارشيف المفتوح من زيادة مرئية الأبحاث وبالتي امكانية الوصول الى الابحاث العلمية واستخدامها لكافة الباحثين تكون متساوية .على المستوى العالمي. وهذا ما يمكن من تعزيز التعاون بين الباحثين والمؤسسات، و تقاسم المعرفة والخبرات مما يسهم في تحقيق تقدم أسرع في مجالات مختلفة.

السؤال الثالث: 4 تعتبر إتاحة الأطروحات الرقمية وسيلة فعالة للحد من السرقات العلمية، وذلك للأسباب التالية:

1. **الشفافية والوصول المفتوح**:
عندما تكون الأطروحات متاحة رقميًا، يمكن للباحثين والطلاب الوصول إليها بسهولة، مما يزيد من فرص اكتشاف أي أعمال مسروقة أو منسوخة. هذا الوصول المفتوح يعزز الشفافية ويجعل من الصعب على الأفراد سرقة أعمال الآخرين دون أن يتم اكتشافهم.
2. **التتبع والاستشهاد**:
الأطروحات الرقمية تُسجل وتُفهرس في قواعد بيانات أكاديمية، مما يسهل تتبعها والاستشهاد بها بشكل صحيح. هذا يقلل من فرص السرقة العلمية، حيث يمكن بسهولة التحقق من المصادر الأصلية.
3. **أدوات الكشف عن الانتحال**:
مع وجود الأطروحات الرقمية، يمكن استخدام أدوات متخصصة للكشف عن الانتحال (Plagiarism Detection Tools)لمقارنة النصوص مع قاعدة بيانات كبيرة من الأعمال المنشورة. هذه الأدوات تساعد في تحديد أي تشابه غير مسموح به بين الأطروحات والأعمال الأخرى.
4. **التوثيق الزمني**:
عند نشر الأطروحة رقميًا، يتم تسجيل تاريخ النشر بشكل دائم، مما يوفر دليلًا على أولوية العمل. هذا يمنع الآخرين من ادعاء ملكية العمل لاحقًا. وهذا من خلال تحصلها على معرف رقمي دائما خاصة عند نشرها في مستودعات رقمية وأرشيفات مفتوحة .
5. **التوعية الأكاديمية**:
إتاحة الأطروحات الرقمية تعزز ثقافة النزاهة الأكاديمية، حيث يصبح الطلاب والباحثون أكثر وعيًا بأهمية الاستشهاد الصحيح واحترام حقوق الملكية الفكرية.

السؤال الرابع: 4ن

Algerian Scientific Journal Platform: ASJP

Portail National de Signalement des Thèses : PNST

Digital Object Identifier : DOI

Open Researcher and Contributor ID : ORCID

International Standard Book Number:ISBN

International Standard Serial Number: ISSN

Internet Protocol: IP

Research Organization Registry. : ROR

السؤل الخامس: 4ن

لمخاطر التي تتعرض لها المكتبات الرقمية:

1. **الاختراقات الإلكترونية** :سرقة البيانات أو تعطيل الخدمات.
2. **فقدان البيانات** :بسبب أعطال تقنية أو كوارث طبيعية.
3. **الوصول غير المصرح به** :استخدام غير قانوني للموارد.
4. **انتهاك حقوق النشر** :توزيع غير قانوني للمواد المحمية.
5. **التلف الرقمي** :تدهور جودة الملفات مع الزمن.

أدوات تحقيق الأمن في المكتبات الرقمية:

1. **التشفير** :لحماية البيانات أثناء التخزين والنقل.
2. **جدران الحماية** :**(Firewalls)** لمنع الوصول غير المصرح به.
3. **أنظمة النسخ الاحتياطي** :لضمان استعادة البيانات عند الضرورة.
4. **إدارة الهوية والوصول** :**(IAM)** للتحكم في الوصول إلى الموارد.
5. **برامج مكافحة الفيروسات والبرامج الضارة** :لحماية الأنظمة من الهجمات.
6. **التوقيع الرقمي** :لضمان صحة وسلامة الوثائق.