1. مقدمة :

إن الإعداد المنهجي للبحث والإلتزام بأساسيات الكتابة العلمية هو المدخل لإعداد بحوث جيدة شكلاً ومضموناً. إن مشاريع التخرج للطلاب الجامعيين تمثل فرصة جيدة للطلاب لتعلم وتطبيق منهج بحثى وإتقان أساسيات الكتابة التقنية.

من المهم لمؤسسة تعليمية مثل كلية علوم الحاسوب وتقانة المعلومات، بجامعة العلوم والتقانة أن توحد وترسخ لطريقة علمية ومنهجية في إعداد مشاريع التخرج لطلابها، لهذا جاء هذا الدليل.

1.1 أهداف الدليل :

لقد عملت إدارة كلية علوم الحاسوب وتقانة المعلومات على إصدار هذا الدليل بعد أن لاحظت التباين الكبير في طرق كتابة وإعداد مشاريع التخرج وفي المحتوى العلمي لهذه المشاريع الذي اتسم في أحايين كثيرة بالضعف. إن الأهداف الرئيسية من وراء إعداد هذا الدليل تتمثل في الآتي :

1- توفير مرجعية منهجية للأساتذة والطلاب في كيفية إعداد مشاريع التخرج.

2- تحديد الأطر العلمية لموضوع مشروع التخرج.

3- تحديد منهجية علمية موحدة لإخراج مشاريع التخرج لكافة طلاب الكلية.

4- توفير مرجعية لأساسيات الكتابة التقنية بوصفها واحدة من أهداف مشروع التخرج.

2.1 تعاريف أساسية :

نقدم في هذا البند تعاريف تبين الفرق بين البحث العلمي (Scientific Research) والتقرير العلمي (Scientific Report) والذي يسمى أيضا التقرير التكنلوجي (Technical Report)، وذلك من أجل أن نبين الطبيعة العلمية لمشروع التخرج.

1.2.1 البحث العلمي :

البحث العلمي يبنى على دراسة ظاهرة أو مشكلة محددة وإستخدام منهج علمي متفق عليه فى الوصول إلى نتائج جديدة أو حلول مبتكرة.

2.2.1 التقرير العلمي :

هو وثيقة تصف إما معالجة (Process) لتطوير تطبيق أو منتج ما أو التطور في مجال معرفي محدد أو الحلول التي قدمت لمشكلة تقنية أو بحثية أو نتائج بحث علمي.

2. مشروع التخرج :

بناء على تعريفي البحث العلمي والتقرير العلمي أعلاه نجد نظرياً أن مشروع التخرج يمكن أن يكون بحثاً علمياً أوتقريراً علمياً، ولكن عملياً نجد أن مشاريع التخرج للطلاب الجامعيين هي تقارير علمية وذلك لأن مطلوبات البحث العلمي المعرفية والمادية والزمنية لاتتوفر للطلاب الجامعيين.

على الرغم من أن مشروع التخرج عملياً هو تقرير إلا أننا سنستخدم في هذا الدليل مصطلح "بحث" ليعبر عن مشروع التخرج لشمولية المصطلح وللإبقاء على التقليد المتبع في تسمية مشاريع التخرج.

1.2 مجالات مشروع التخرج :

بناء على تعريف التقرير العلمي نجد أن مجالات مشاريع التخرج للطلاب الجامعين في مجال دراسات الحاسوب تشمل (ولا تقتصر على) الآتي :

1- تحليل وتصميم نظم المعلومات.

2- حل مشاكل في المجتمع بإستخدام حلول التقنية.

3- تطوير نظم معلومات وتطبيقات بإتباع معالجة معرفة علمياً.

4- دراسة الحلول المقترحة لمشكلة محددة.

5- دراسة الوضع الحالي لمشكلة أو تقنية.

6- دراسة مقارنة.

7- دراسة التطور التقني في مجال محدد.

8- تطبيق خوارزمية أو خوارزميات معروفة لتقديم حل لمشكلة.

2.2 هيكل مشروع التخرج :

إن الهيكل العام لمشروع التخرج يجب أن يتبع الهيكل التالي (حسب الترتيب أدناه).

1.2.2 صفحات البداية :

1- صفحة الغلاف (العنوان).

2- صفحة الموافقة.

3- الإهداء (Dedication).

4- الشكر (Acknowledgement).

5- المستخلص باللغة العربية (Abstract).

6- المستخلص باللغة الإنجليزية [إذا كان البحث مكتوباً باللغة الإنجليزية].

7- المحتويات (Content).

8- قائمة الأشكال (List of Figures).

9- قائمة الجداول (List of Tables).

10- قائمة المختصرات (Abbreviation List).

2.2.2 جسم البحث :

1- المقدمة (Introduction).

2- فصول البحث.

3- الخلاصة والتوصيات (Conclusion and Recommendations).

3.2.2 صفحات النهاية :

1- المراجع (References).

2- الملحقات (Appendices).

سنناقش فيما يلي كلاً من عناصر الهيكل أعلاه :

1.2.2 صفحات البداية :

صفحات البداية هي الصفحات ماقبل الفصل الأول من البحث وتشتمل على :

1- صفحة الغلاف (العنوان) :

تحتوي هذه الصفحة على :

- العبارة " جامعة العلوم و التقانة - كلية علوم الحاسوب و تقنية المعلومات ".
- القسم.
- الدفعة.
- عنوان البحث.

- العبارة "بحث تكميلي مقدم للإيفاء بمطلوبات نيل درجة "البكلاريوس في علوم الحاسوب/ البكلاريوس في تقنية المعلومات/ الدبلوم في تقنية المعلومات/الدبلوم في نظم الشبكات".
- إعداد

  اسم الطالب ورقمه الجامعي.
- إشراف - اسم المشرف.
- تاريخ تقديم الرسالة.

بسم الله الرحمن الرحيم
جامعة العلوم والتقانة
كلية علوم الحاسوب وتقانة المعلومات
قسم تقنية المعلومات
الدفعة الثانية

قياس أمن خوارزميات التشفير

بحث تكميلي مقدم للإيفاء بمطلوبات نيل درجة البكلاريوس / الدبلوم في تقنية المعلومات

إعداد
ناصر محمد خالد رقم 200
مزمل فتحي محمد رقم 201

إشراف
الدكتور / عبدالله محمد أحمد

فبراير 2008 م

الشكل (1.1.2.2) هو مثال لصفحة عنوان باللغة العربية

2- صفحة موافقة المشرف على تقديم البحث :

تحتوي هذه الصفحة على :

- عنوان الرسالة.

- اسم الطالب.
- موافقة المشرف على تقديم البحث.
- اسم المشرف وتوقيعه.
- التاريخ.

جامعة العلوم والتقانة
كلية علوم الحاسوب وتقانة المعلومات
قسم تقنية المعلومات

لجنة الإشراف على مشاريع التخرج للدفعة الثانية

الدرجة العلمية : .....

اسم المشروع : .....

اسم الطالب : 1- .....
2- .....
3- .....

لقد أكمل الطلاب إعداد البحث و أوافق على تقديمه.

اسم المشرف : ..... **التوقيع :** .....

التاريخ : .....

الشكل (2.1.2.2) هو مثال لصفحة موافقة المشرف

3- صفحة الإهداء :

هذه الصفحة إختيارية، ويتم فيها إهداء البحث من قبل الطلاب الباحثين للأشخاص الذين يحبون إهداء عملهم لهم.

4- صفحة الشكر :

في هذه الصفحة يتم تقديم الشكر من قبل الطلاب الباحثين للأشخاص والمؤسسات التي قدمت لهم مساعدات مؤثرة أثناء إعدادهم للبحث (مثل مساعدة من المشرف ، دعم مالي من مؤسسة،.. إلخ).

5- صفحة المستخلص (Abstract) :

على الرغم من أن المستخلص هو في بداية البحث الإ أنه يكتب بعد الإنتهاء من البحث ويأتي عادةً في أقل من صفحة واحدة، ويجب أن يكون شارحاً لنفسه ولايحتاج لمرجعية. يحتوي المستخلص على :

- وصف للمجال المعرفي للبحث أو إعطاء خلفية علمية لموضوع البحث.
- تحديد مشكلة أو مسألة (موضوع) البحث.
- وصف للمنهجية (الإجراءات) المتبعة في البحث.
- وصف للحل المقدم (الإسهام في حل) للمشكلة.
- النتائج (Results) التي تم التوصل إليها.
- الخلاصة المستمدة من نتائج البحث (Conclusion).

المستخلص

إن أمن المعلومات أصبح من المجالات المعرفية التي تجد إهتماما متعاظماً مع إزدياد إستخدام الشبكات والإنترنت في نقل بيانات عالية القيمة وفي إجراء معاملات عالية الخصوصية. إن أهم القضايا التي يعالجها أمن المعلومات هي السرية والتكاملية والتوفر.

إن السرية تعني أن لايطلع على البيانات إلا الشخص المخول له ذلك . إن أحد أهم التقنيات التي توفر السرية للبيانات هي التشفير بشقيه التماثلي واللاتماثلي وقد تم تطوير العديد من خوارزميات التشفير.

إن إستخدام خوارزمية تشفير آمنة وسريعة هي من القضايا المهمة في أمن المعلومات. إن تحديد مدى أمن خوارزمية هو القضية التي يعالجها هذا البحث.

في هذا البحث تم تحديد ثلاثة مؤشرات لقياس أمن خوارزمية التشفير هي : طول المفتاح، حجم البيانات التي تعالجها الخوارزمية كدفعة واحدة، مدى تعقيد العمليات الداخلية التي تكون الخوارزمية، وقد وتم إستخدام هذه المؤشرات لقياس أمن ثلاثة خوارزميات تشفير هي R1، R2 و R3.

لقد بينت نتائج القياس أن زيادة طول المفتاح لمدى معين يزيد من أمن الخوارزمية إلا أن ذلك مرتبط بتعقيد العمليات الداخلية للخوارزمية مما يجعل من تعقيد العمليات الداخلية للخوارزمية المؤشر الأهم في أمن الخوارزميات.

6- المحتويات :

المحتويات هي جدول يوضح تنظيم البحث بأقسامه الثلاثة، حيث يبين تبويب البحث من صفحات المقدمة إلى الفصول المكونة للبحث والمراجع والملاحق. صفحات المقدمة من البحث ترقم عادةً بالأرقام الرومانية (i, ii, iii, ...) بينما يرقم جسم ونهاية البحث بالأرقام العربية (1, 2, 3, ...).

المحتويات

7- قوائم الأشكال والجداول والمختصرات :

إذا تم إستخدام شكلان أو أكثر في البحث أو تم إستخدام جدولان أو أكثر فإنه يجب إضافة قائمة للأشكال وأخرى للجداول بعد جدول المحتويات. الجداول (1) و (2) تبين على التوالي كيفية إعداد قوائم الأشكال والجداول.

أيضاً إذا تم في البحث إستخدام مكثف للمختصرات فيجب إعداد قائمة للمختصرات تحتوي على الإسم الكامل للمصطلح و المختصر المقابل له.

الجدول (8.1.2.2): قائمة الأشكال

الجدول (9.1.2.2): قائمة الجداول

2.2.2 جسم البحث :

يتكون من ثلاثة أجزاء وهي :

1.2.2.2 المقدمة (Introduction) :

المقدمة يجب أن تأخذ القاريء من مستوى المعرفة الصفرية إلى المستوى الذي يمكن القاريء من فهم البحث، ومحتواها يختلف وفقاً لطبيعة البحث، ولكن بشكل عام قد تحتوي المقدمة على :

- خلفية للمجال المعرفي للمشكلة أوالموضوع الذي يتناوله البحث.
- تحديد مشكلة أوموضوع البحث.
- تحديد الوضع الراهن للقضية التي يتناولها البحث.
- الفرضيات التي بني عليها البحث.
- الكيفية التي يعالج بها البحث المشكلة.
- النتائج التي توصل إليها البحث.
- الصعوبات والعقبات التي واجهت البحث.
- فكرة عامة عن محتويات البحث.

2.2.2.2 فصول البحث :

جسم البحث يحتوي على المعلومات المتحصل عليها أثناء إعداد البحث والعمل الذي تم إنجازه مما أدى إلى خلاصة وتوصيات البحث.

يتكون جسم البحث من مجموعة من الفصول وتحدد طبيعة البحث عدد هذه الفصول وترتيبها ومحتواها. كمثال إذا كان البحث هو " قياس أمن خوارزميات التشفير" **فقد** يشتمل جسم البحث على :

1- خلفية علمية لمجال البحث (التشفير).
2- عرض الجهود التي بذلت لحل المشكلة (الجهود العلمية في قياس أمن الخوارزميات).
3- تحديد طبيعة الحل المقترح (تحديد المؤشرات التي يقترحها البحث للقياس).
4- كيفية تطبيق الحل المقترح (تحديد المنهجية العلمية في تطبيق المؤشرات على الخوارزميات).
5- نتائج تطبيق الحل المقترح (نتائج تطبيق القياس).

كمثال آخر إذا كان البحث هو "تطوير نظام لإدارة عيادة طبية" **فقد** يشتمل جسم البحث على :

1- مقدمة في نظم المعلومات.
2- دورة إنشاء نظام المعلومات.
3- تقنيات تطوير نظم المعلومات.
4- إجراءات وتقنيات تأمين البيانات في نظم المعلومات.
5- تحليل وتصميم نظام لإدارة عيادة طبية.
6- تجسيد النظام المطور.
7- نتائج تطبيق النظام المطور.

3.2.2.2 الخلاصة والتوصيات :

بعض القراء يقرؤون المستخلص، المقدمة و الخلاصة والتوصيات فقط للإلمام بما جاء في البحث. لذلك يجب التأكد من أن هذه الأجزاء من الرسالة معبرة عن محتوياتها و متسقة فيما بينها.

إن الخلاصة (Conclusions) هي ليست ملخص (Summary) للبحث ويجب أن لاتشتمل على أي أفكار جديدة وإنما تقدم ملخصاً للأفكار والقضايا التي ناقشها البحث ونتائج البحث كما يمكن أن تشتمل على تقييم لنتائج البحث. كما يجب أن تؤسس الخلاصة وبشكل واضح للأسباب التي ستبنى عليها توصيات البحث.

إن التوصيات التي يقترحها البحث يجب أن تبنى على الخلاصة وهي تشتمل على مجموعة من الأفكار التي تربط نتائج البحث بمجالات معرفية أخرى ومجموعة من المقترحات التي تساهم في تطوير البحث مستقبلاً.

3.2.2 صفحات النهاية :

تحتوي صفحات النهاية في البحث على المراجع والملحقات.

1- المراجع :

المراجع هي قائمة الكتب والأوراق العلمية والمقالات التي استخدمت أثناء إعداد البحث. يجب أن تتم الإشارة للمراجع في متن البحث كما يجب أن تكتب كقائمة في نهاية البحث.

تجب الإشارة للمرجع في متن البحث في الحالات التالية :

- عندما تقتبس من عمل شخص آخر الإقتباس يشمل : النصوص ، الجداول و الرسومات و الصور ...إلخ.
- عندما تعيد صياغة ما كتبه شخص آخر.
- عندما تلخص ما كتبه شخص آخر.

الإشارة للمرجع في متن البحث يمكن أن يتم بطرق مختلفة ولكننا سنعتمد في هذا الدليل طريقتين هما :

1- إستخدام عدد صحيح مفرد لكل مرجع (عادةً ما يبدأ ترقيم المراجع من 1) يكتب بين قوسين مربعين. فيما يلي مثال لإستخدام هذه الطريقة :

" إن النموذج الشبكي الأكثر شيوعاً في تطبيقات الإنترنت هو نموذج العميل/المخدم [3]".

2- إستخدام اسم المؤلف (المؤلفين) ثم تاريخ نشر المرجع بين قوسين مربعين. إذا كان المؤلف شخص واحد أو كانا شخصين فيتم إيراد الإسم أو الإسمين كما في المثال التالي:

" الخدمات الإضافية التي يقدمها بروتوكول TCP تشمل التحكم في تدفق البيانات والتحكم في الإزدحام [Jim Kurose and Keith Ross, 2000]".

أما إذا كان المؤلفون أكثر من إثنين فيتم ذكر اسم المؤلف الأول متبوعاً بالعبارة 'et al.' (وهي إختصار لاتيني يعني وآخرون) إذا كان المرجع باللغة الإنجليزية ، أو متبوعاً بعبارة "وآخرون" إذا كان المرجع باللغة العربية. كمثال :

"إن نسبة الهجمات التي تتم للشبكات من داخلها يبلغ 78% [عثمان الخليفة وآخرون، 2007م]".

إن قائمة المراجع في نهاية البحث يجب أن تكتب مرتبة تصاعدياً إذا تم إستخدام الطريقة الأولى ومرتبة أبجدياً إذا تم إستخدام الطريقة الثانية. في كلا الحالتين إذا كان المرجع عبارة عن كتاب يجب إيراد المعلومات التالية :

- اسم المؤلف أوالمؤلفين.
- اسم الكتاب.
- الناشر.
- رقم الإصدارة.

- تاريخ النشر.

فيما يلي مثال لكيفية إيراد الكتاب كمرجع في قائمة المراجع بإستخدام الطريقة الأولى :

[1] علي نورالدين وآخرون ، "نظم المعلومات المفتوحة" ، الدار العربية للكتاب ، النسخة الثالثة ، 2007م.

أو

[4] D. Lynch, M. Rose, "Internet System Handbook", Addison Wesley, Second Edition, 2004.

أما إذا كان المرجع عبارة عن ورقة علمية منشورة في مجلة علمية أو دورية متخصصة أو في مطبوعة مؤتمر علمي، فيجب إيراد المعلومات التالية :

- اسم المؤلف أو المؤلفون.
- عنوان الورقة أو المقال.
- اسم المجلة أو الدورية أو المؤتمر.
- المجلد ، رقم الإصدارة ، التاريخ.
- أرقام الصفحات.

فيما يلي مثال لكيفية إيراد ورقة علمية أو مقال كمرجع في قائمة المراجع بإستخدام الطريقة الثانية :

[عز الدين عثمان،2006م] عزالدين عثمان ، "مناعة نظم التشغيل" ، المجلة العربية لدراسات الحاسوب ، العدد السابع ، نوفمبر 2006م ، الصفحات 26-34.

أو

[Christian B. et al, 2004] Christian B. et al. "Diffusion and Confusion in Cryptographic Algorithms", In Proceedings of the Fifth International Conference on Cryptography, Orlando, U.S.A, Sep 2004, pp 65-75.

2- الملحقات :

إن الملحق هو عبارة عن معلومات تفصيلية أو طويلة ذات علاقة بإحدى موضوعات البحث (بغض النظر عن شكلها) ووجودها ضمن البحث قد يبعد القاريء من الموضوع الرئيسي، لذلك تتم إضافتها في نهاية البحث ليتمكن القاريء من الرجوع إليها إذا رغب في ذلك.

إن وجود ملحقات في البحث تفرضه طبيعة البحث، فليس بالضرورة أن تكون هنالك ملحقات في كل بحث. كمثال فالملاحق هي المكان المناسب للقوائم أو الجداول الطويلة والمفصلة، شفرة المصدر لبرنامج، الإشتقاقات الرياضية، لمحات من واجهات نظام أو نتائج محاكاة.

3. الخطوط والهوامش والترقيم :

نتناول في هذا البند أنواع وأحجام الخطوط التي يجب إستخدامها في إعداد البحث وكيفية ترقيم الأشكال والجداول.

1.3 خطوط صفحة العنوان : تكون للبيانات في صفحة العنوان الخطوط والضبط المبين في الجدول (1.3).

الجدول (1.3): خطوط وضبط بيانات صفحة العنوان

الجملة	حجم الخط	الضبط
جامعة العلوم والتقانة	24	وسط
كلية علوم الحاسوب وتقانة المعلومات	22	وسط
القسم	20	وسط
الدفعة	18	وسط
عنوان البحث	26	وسط
إعداد وأسماء الطلاب	18	وسط
إشراف واسم المشرف	18	وسط
التاريخ	18	وسط

إذا كان البحث مكتوباً باللغة العربية يكون نوع الخط Simplified Arabic وإذا كان البحث مكتوباً باللغة الإنجليزية يكون نوع الخط Times New Roman.

2.3 خطوط وضبط جسم البحث : تكون للعناوين الرئيسية والفرعية والنص داخل البحث الخطوط والضبط الموضح في الجدول (2.3).

الجدول (2.3): خطوط وضبط العناوين والنص

الجملة	حجم الخط	الضبط
العنوان الرئيسي في الفصل كمثال: 1.4	18 عريض	مضبوط لليمين في العربي ولليسار في اللغة الإنجليزية
العنوان الفرعي الأول كمثال: 1.1.4	16 عريض	مضبوط لليمين في العربي ولليسار في اللغة الإنجليزية
العنوان الفرعي الثاني كمثال: 1.1.1.4	14 عريض	مضبوط لليمين في العربي ولليسار في اللغة الإنجليزية
النص	14	ضبط كلي ومسافات بين الأسطر 1.5"

إذا كان البحث مكتوبا باللغة العربية يكون نوع الخط Simplified Arabic وإذا كان البحث مكتوبا باللغة الإنجليزية يكون نوع الخط Times New Roman .

3.3 الهوامش وترقيم الأشكال والجداول :

تكون للصفحات الهوامش الموضحة في الجدول (3.3). وترقم الأشكال والجداول بناءً على ترتيبها داخل الفصل فالشكل الأول فى الفصل الأول يرقم (1.1) والشكل الثالث فى الفصل الرابع يرقم (3.4) والجدول الثاني في الفصل الخامس يرقم (2.5) ليرمز الرقم الأول للفصل والرقم الثاني لترتيب الشكل داخل الفصل. أرقام الأشكال وعناوينها تكتب تحت الشكل بينما تكتب أرقام الجداول وعناوينها أعلى الجدول.

الجدول (3.3): هوامش الصفحات

الصحفة	الهامش	الحجم
كل صفحات البحث	الأيسر	في اللغة العربية 1.25 بوصة و في اللغة الإنجليزية 1.5 بوصة
	الأيمن	في اللغة العربية 1.5 بوصة و في اللغة الإنجليزية 1.25 بوصة
صفحات بداية الفصل	الأعلى	1.5 بوصة
صفحات بداية الفصل	الأسفل	1.25 بوصة
الصفحات الأخرى	الأعلى	1 بوصة
الصفحات الأخرى	الأسفل	1.25 بوصة