





# نظرية التشفير والتعمية ( الأساسيات ) الجزء الأول

تأليف

د. غ. هوفمان

د. ر. هانكرسون

ك. ك. ليندندر

د. أ. لينورد

ك. أ. روجر

ك. ت. فيلبس

ج. ر. وول

ترجمة

د. فوزي بن أحمد الذكير

د. معروف عبدالرحمن سمحان

قسم الرياضيات - كلية العلوم

جامعة الملك سعود

النشر العلمي والمطابع - جامعة الملك سعود

ص. ب. ٦٨٩٥٣ - الرياض ١١٥٣٧ - المملكة العربية السعودية



ح) جامعة الملك سعود، ١٤٣٥هـ (٢٠١٤م)

هذه ترجمة عربية مصرح بها من مركز الترجمة بالجامعة لكتاب:

Coding Theory and Cryptography: The Essentials

By: D. R. Hankerson, *et al.*

© Taylor & Francis, 2000

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

د. ر. هانكرسون

نظرية التشفير والتعمية: الأساسيات. / د. ر. هانكرسون؛ معروف عبدالرحمن  
سمحان؛ فوزي بن أحمد الذكير. - الرياض، ١٤٣٥هـ  
٢ مج.

٣٧١ ص؛ ٢٤ × ١٧ سم

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٢-٢١٨-٥٠٧-٦٠٣-٩٧٨ (ج ١)

١- الشيفرة ٢- الاختصارات ٣- أمن المعلومات أ. سمحان، معروف  
عبدالرحمن (مترجم) ب. الذكير، فوزي بن أحمد (مترجم) ج. العنوان  
ديوي ٨، ٦٥٢ ١٤٣٥/٩٨

رقم الإيداع: ١٤٣٥/٩٨

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٢-٢١٨-٥٠٧-٦٠٣-٩٧٨ (ج ١)

حكمت هذا الكتاب لجنة متخصصة، وقد وافق المجلس العلمي على نشره في اجتماعه العشرين  
للعام الدراسي ١٤٣٣هـ / ١٤٣٤هـ المعقود بتاريخ ١٦/٧/١٤٣٤هـ الموافق ٢٦/٥/٢٠١٣م.

النشر العلمي والمطابع ١٤٣٥هـ



## مقدمة المترجمين

وقع اختيارنا على ترجمة هذا الكتاب لعدة أسباب أهمّها أن هذا الكتاب يجمع بين موضوعي نظرية التشفير ونظرية التعمية وهما الموضوعان اللذان نقوم بتدريسهما في مقرر تطبيقات الجبر لطلاب قسم الرياضيات ، ولذا فهو يخدم الهدف الذي نسعى إليه وهو توفير مادة علمية باللغة العربية لهذين الموضوعين لتكون في متناول الطالب. ومما يميز هذا الكتاب هو شرح مادة الرياضيات اللازمة لفهم المواضيع في المكان المناسب وبدون تعمق حيث يتطرق فقط إلى المفاهيم التي يحتاج إليها دون الخوض في براهين رياضية صعبة ، وهذه الميزة تجعل هذا الكتاب مناسباً لطلبة الهندسة والحاسب الآلي بالإضافة إلى طلاب الرياضيات.

أثناء ترجمتنا لهذا الكتاب قمنا بتصحيح بعض الأخطاء المطبعية التي تمكنا من اكتشافها والتي لا يكاد يخلو منها أي كتاب. قمنا أيضاً بوضع بعض التفاصيل للمادة العلمية وأضفنا بعض البراهين التي نعتقد ضرورة وجودها وقد تم ذلك دون الإخلال بتسلسل المادة العلمية.

اعتمدنا في ترجمة المصطلحات العلمية على قاموس العلوم الرياضية الذي شارك المترجمان في إعداده والصادر عن منشورات جامعة الملك سعود وهو مبني على

المعجمين الصادرين عن مكتب تنسيق التعريب بالرباط ومعجم الرياضيات الصادر عن مؤسسة الكويت للتقدم العلمي ، واجتهدنا بترجمة المصطلحات التي لم ترد في أي من هذه المعاجم الثلاثة.

ونود أن نشكر مركز الترجمة بجامعة الملك سعود على موافقته على ترجمة هذا الكتاب الذي نأمل أن يكون إضافة مفيدة إلى المكتبة العربية. والله من وراء القصد.

المترجمان

## إهداء المؤلفين

إلى زوجاتنا الحبيبات  
سندي وجيل وجين وأن وجانيت وسو

إلى أولادنا  
نويل وأيان وتيم وكيرت وجيمي وأندرو وميخان وكاترينا وريبركا

وإلى آبائنا وأمهاتنا  
إيلين وريتشارد، فالي وجيل، مارجوري ولويس، ماري وتشارلز،  
إيثل وريتشارد، أيريس وأيان، بيولاه ووالتر.



## شكر وتقدير

### Acknowledgments

نقدم شُكرنا العميق لألفريد مينيزس على اقتراحاته المفصّلة ومراجعاته العديدة للفصول من العاشر إلى الثاني عشر. كان من الممكن أن يحتوي هذا الكتاب على أخطاء أكثر وأن يكون سرد المادة أسوأ لولا ارشاداته الجمّة لنا. كما نود أن نقدم شُكرنا لسيلدا كيوسيكسفي على مراجعتها واقتراحاتها وتصحيحها لبعض الأخطاء. أما روزي توربرت فقد ساهمت مساهمة غير عادية بإنجاز أصول الطبعة الأولى من هذا الكتاب.

إن صبرها وشجاعتها على تحمل الأعباء الناتجة عن المراجعات الكثيرة يضعها في مصاف القديسين. كما نقدم شُكرنا وتقديرنا لهيذر كونر على العمل الرائع التي قامت به أثناء التحضير للطبعة الثانية. ونخص بالشكر مصممة الغلاف سندي أوترسون كما نقدر لها عملها معنا في العديد من المشاريع.

### المؤلفون



## توهيد

## Preface

الهدف من هذا الكتاب المنقح والمحدث من الطبعة الأولى هو تدريس نظرية التشفير والتعمية بأسلوب رياضي معقول لطلبة الهندسة وعلوم الحاسب والرياضيات. يختلف هذا الكتاب عن معظم كتب التشفير والتعمية الأخرى بنقطتين مهمتين هما "في الوقت المناسب" وإهمال التعميمات الرياضية غير المهمة.

إن فلسفة "في الوقت المناسب" مبنية على تقديم مادة الرياضيات اللازمة عند الحاجة إلى تطبيقها، ولذا، فالكتاب لا يحتوي على ٢٠٠ صفحة من الرياضيات (ليست ضرورة في معظمها) ومن ثم ٢٠٠ صفحة أخرى من التشفير والتعمية. وبهذا فإن شكل الكتاب هو على النحو التالي: رياضيات، تطبيقات، رياضيات، تطبيقات وهكذا. إن تجنب التعميمات الرياضية يعني على سبيل المثال، أنه ليس من الضروري وصف الشفرة الدورية على أنها مثالي رئيس. وبهذا فلقد أهملنا في العموم الخوض في التعميمات الرياضية والمفاهيم التي تستخدم عادة لتدريس المقرر لطلاب الرياضيات فقط.

استخدم الجزء الأول من هذا الكتاب (الفصول من الأول إلى التاسع) لتدريس نظرية التشفير في فصلين متتاليين في جامعة أوبرن حيث كان المتطلب الوحيد أن يكون

لدى الطالب معلومات بدائية في الجبر الخطي. وبالطبع كلما كانت معلومات الطالب في الجبر الخطي والجبر المجرد أكثر يكون استيعابه أفضل ومن ثم يحتاج إلى وقت أقصر لتغطية المادة الأولى.

يُركّز جزء نظرية التشفير من هذا الكتاب على إنشاء الشفرات الثنائية والشفرات على حقل مميزه 2، كما يُركّز على عمليتي التشفير وفك التشفير (تصويب الأخطاء) لعائلة من الشفرات المهمة. وعائلة الشفرات المختارة ذات أهمية خاصة للمهندسين ومتخصصي علوم الحاسب مثل شفرات ريد وسولومن وشفرات التلاف المستخدمة في اتصالات الفضاء وإلكترونيات المستهلك، ويعكس هذا الخيار المدى الواسع لخوارزميات التشفير وفك التشفير

أما الجزء الثاني من هذا الكتاب (الفصول من العاشر إلى الثاني عشر) فتبلورت فكرته بعد تدريسنا مقررًا بدائيًا لفصل واحد في نظرية التعمية لطلاب جامعة أوبرن حيث الطلاب المسجلون في هذا المقرر هم خليط من طلاب مرحلة البكالوريوس وطلاب الدراسات العليا من تخصصات علوم الحاسب، الهندسة، الرياضيات، التربية حيث إن المعرفة الرياضية لبعضهم تقتصر على مقرر بدائي في الجبر أو نظرية الأعداد، ويعتبر ذلك كافيًا لتقديم مقرر معقول في علم التعمية. في الحقيقة إن معظم المادة العلمية في هذا المقرر تحتاج فقط إلى النتائج الأساسية للأعداد الصحيحة قياس  $n$  (وهذه مقدمة في الفصل الحادي عشر). إن هدفنا الأساسي هو كتابة مقرر مختصر وتام لمقدمة في التعمية الحديثة مع التركيز على طرائق التعمية ذات المفتاح العلن. في الفصل الثاني عشر قمنا بتغطية المواضيع الرئيسة في بنود قصيرة نسبيًا وتركنا بعض الموضوعات للتمارين (تحتوي هذه التمارين على بعض التفاصيل والمراجع).

بوجه عام، نستطيع القول إن اهتمام نظرتي التعمية والتشفير هو نقل المعلومات إلكترونياً، مع مراعاة السرية في الأولى والموثوقية في الثانية ومع اعترافنا بأن معظم الخطط الدراسية لا يتسع فيها المجال لتخصيص مقررات منفصلة لكل منها فإن هذا الكتاب يتيح تدريس الفصول من الأول إلى الرابع ومن ثم الفصلين الخامس والسادس أو الفصلين السابع والثامن لمقرر واحد في نظرية التشفير. من الممكن أيضاً تدريس الفصول من العاشر إلى الثاني عشر لمقرر في نظرية التعمية. كما أنه من الممكن تدريس الفصول الأول والثاني والثالث والعاشر والثاني عشر مع بعض موضوعات الفصل الحادي عشر لمقرر في التشفير والتعمية.

وأخيراً فالمؤلفون سيكونون ممتنين لأي ملحوظات يقدمها لهم مستخدمو هذا

الكتاب على العنوان الإلكتروني: [rodgec1@auburn.edu](mailto:rodgec1@auburn.edu).



## الرموز Symbols

$C^\perp$  : شفرة ثنوية للشفرة  $C$ .

$C_{23}$  : شفرة جولاي.

$C_{24}$  : شفرة جولاي الممتدة.

$GF(2^r)$  : حقل جالوا.

$GF(2^r)[x]$  : كثيرات حدود بمعاملات في الحقل  $GF(2^r)$ .

$RM(r, m)$  : شفرة ريد ومولر.

$RS(2^r, \delta)$  : شفرة ريد وسولومن.

$S$  : الشفرة المولدة بالمجموعة  $S$ .



## المحتويات

### Contents

هـ.....	مقدمة المترجمين
ز.....	إهداء المؤلفين
ط.....	شكر وتقدير
ك.....	تمهيد
س.....	الرموز

#### الجزء الأول: نظرية التشفير

١.....	الفصل الأول: مقدمة في نظرية التشفير
١.....	(١, ١) مقدمة
٤.....	(١, ٢) فرضيات أساسية
٧.....	(١, ٣) تصويب واكتشاف أنماط الأخطاء
١٠.....	(١, ٤) معدل المعلومات
١١.....	(١, ٥) تأثير تصويب واكتشاف الأخطاء

١٣	..... إيجاد الاحتمالية القصوى لكلمة الشفرة المرسلة (١, ٦)
١٦	..... بعض أساسيات الجبر (١, ٧)
١٨	..... الوزن والمسافة (١, ٨)
٢٠	..... فك التشفير الاحتمالي الأقصى (١, ٩)
٢٧	..... موثوقية MLD (١, ١٠)
٣١	..... شفرات اكتشاف الأخطاء (١, ١١)
٣٩	..... شفرات تصويب الأخطاء (١, ١٢)
٤٧	..... الفصل الثاني: الشفرات الخطية
٤٧	..... (٢, ١) الشفرات الخطية
٥٠	..... (٢, ٢) فضاءان جزئيان مهمان
٥٣	..... (٢, ٣) الاستقلال والأساس والبعد
٦٢	..... (٢, ٤) المصفوفات
٦٥	..... (٢, ٥) أساسات لكل من $C = \langle S \rangle$ و $C^\perp$
٧٢	..... (٢, ٦) المصفوفات المولدة والتشفير
٧٨	..... (٢, ٧) مصفوفات اختبار النوعية
٨٣	..... (٢, ٨) الشفرات المتكافئة
٨٩	..... (٢, ٩) مسافة شفرة خطية
٩٠	..... (٢, ١٠) المجموعات المشاركة
٩٥	..... (٢, ١١) MLD للشفرات الخطية
١٠٦	..... (٢, ١٢) موثوقية IMLD للشفرات الخطية

١٠٩	الفصل الثالث: الشفرات التامة والشفرات ذات الصلة بها
١٠٩	(٣, ١) بعض الحدود على الشفرات
١١٧	(٣, ٢) الشفرات التامة
١٢١	(٣, ٣) شفرات هامينغ
١٢٥	(٣, ٤) الشفرات الممتدة
١٢٨	(٣, ٥) شفرة غوليه الممتدة
١٣٢	(٣, ٦) فك تشفير شفرة غوليه الممتدة
١٣٧	(٣, ٧) شفرة غوليه
١٤٠	(٣, ٨) شفرات ريد ومولر
١٤٦	(٣, ٩) فك تشفير سريع للشفرة $RM(1, m)$
١٥١	الفصل الرابع: الشفرات الخطية الدورية
١٥١	(٤, ١) كثيرات الحدود والكلمات
١٥٨	(٤, ٢) مقدمة للشفرات الدورية
١٦٨	(٤, ٣) المصفوفات المولدة ومصفوفات اختبار النوعية للشفرات الدورية
١٧٣	(٤, ٤) إيجاد الشفرات الدورية
١٨٠	(٤, ٥) الشفرات الدورية الثنوية
١٨٥	الفصل الخامس: شفرات BCH
١٨٥	(٥, ١) الحقول المنتهية
١٩٢	(٥, ٢) كثيرات الحدود الأصغرية

١٩٧.....	(٥, ٣) شفرات هامينغ الدورية
٢٠٠.....	(٥, ٤) شفرات BCH
٢٠٤.....	(٥, ٥) فك تشفير شفرة BCH التي تصوب خطأين
٢١١.....	الفصل السادس: شفرات ريد وسولومن
٢١١.....	(٦, ١) شفرات على $GF(2^r)$
٢١٦.....	(٦, ٢) شفرات ريد وسولومن
٢٢٤.....	(٦, ٣) فك تشفير شفرات ريد وسولومن
٢٣٥.....	(٦, ٤) طريقة التحويل لإنشاء شفرات ريد وسولومن
٢٤٥.....	(٦, ٥) خوارزمية بيرلكامب ومايسي
٢٥٣.....	(٦, ٦) الكلمات المحوّة
٢٦٣.....	الفصل السابع: شفرات تصويب الأخطاء الاندفاعية
٢٦٣.....	(٧, ١) مقدمة
٢٧١.....	(٧, ٢) التوريق البيني
٢٨١.....	(٧, ٣) تطبيقات على الأقراص المدججة
٢٨٧.....	الفصل الثامن: شفرات التلاف
٢٨٧.....	(٨, ١) مسجلات الإزاحة وكثيرات الحدود
٢٩٦.....	(٨, ٢) تشفير شفرات التلاف
٣٠٨.....	(٨, ٣) فك تشفير شفرات التلاف
٣١٩.....	(٨, ٤) فك تشفير فيتربي المبتور

المحتويات

ش

٣٣٩	الفصل التاسع: شفرات ريد ومولر وشفرات بريراتا
٣٣٩	(٩, ١) شفرات ريد ومولر
٣٤٤	(٩, ٢) فك تشفير شفرات ريد ومولر
٣٥٢	(٩, ٣) شفرات بريراتا الممتدة
٣٦٢	(٩, ٤) تشفير شفرات بريراتا الممتدة
٣٦٥	(٩, ٥) فك تشفير شفرات بريراتا الممتدة

الجزء الثاني: نظرية التعمية

٣٧٣	الفصل العاشر: التعمية التقليدية
٣٧٥	(١٠, ١) خطط التعمية
٣٧٩	(١٠, ٢) التعمية ذات المفتاح المتماثل
٣٩٢	(١٠, ٣) أنظمة تعمية فيستل و DES
٣٩٥	(١٠, ٣, ١) البيانات المحكمة الجديدة
٤٠٠	(١٠, ٣, ٢) نظام تعمية البيانات القياسي
٤١٣	(١٠, ٤) حواشي
٤١٧	الفصل الحادي عشر: موضوعات في الجبر ونظرية الأعداد
٤١٨	(١١, ١) الخوارزميات، تعقد الحسابات، حساب التطابقات
٤٣٠	(١١, ٢) الرواسب التربيعية
٤٣٩	(١١, ٣) اختبار الأوليات

٤٤٤.....	(١١, ٤) التحليل والجذور التربيعية.....
٤٤٥.....	(١١, ٤, ١) طريقة رو لبولارد.....
٤٤٨.....	(١١, ٤, ٢) المربعات العشوائية.....
٤٥٢.....	(١١, ٤, ٣) الجذور التربيعية.....
٤٥٧.....	(١١, ٥) اللوغاريتمات المنفصلة.....
٤٥٧.....	(١١, ٥, ١) الخطوة الصغيرة والخطوة الكبيرة.....
٤٥٩.....	(١١, ٥, ٢) حساب الدليل.....
٤٦٣.....	(١١, ٦) حواشي.....
٤٦٥.....	الفصل الثاني عشر: أنظمة التعمية ذوات المفتاح العلن.....
٤٦٧.....	(١٢, ١) دوال الاتجاه الواحد ودوال الترميز.....
٤٧٤.....	(١٢, ٢) نظام RSA.....
٤٨٧.....	(١٢, ٣) الأمن القابل للبرهان.....
٤٩٣.....	(١٢, ٤) نظام الجمل.....
٥٠١.....	(١٢, ٥) بروتوكولات (معاهدات أو اتفاقيات) تعمية.....
٥٠٣.....	(١٢, ٥, ١) اتفاقية ديفي وهيلمان لتبادل المفاتيح.....
٥٠٥.....	(١٢, ٥, ٢) براهين بدون معلومات.....
٥٠٨.....	(١٢, ٥, ٣) رمي النقود والبوكر الذهني.....
٥١٥.....	(١٢, ٦) حواشي.....

المحتويات

ث

الملاحق.....	٥١٩
الملحق (أ): خوارزمية اقليدس .....	٥٢١
الملحق (ب): تحليل $1 + x^n$ .....	٥٢٧
الملحق (ج): مثال على تشفير قرص مدمج .....	٥٢٩
الملحق (د): حلول لتمارين مختارة .....	٥٣٥
المراجع.....	٥٦٧
ثبت المصطلحات .....	٥٧٥
أولاً: عربي - إنجليزي .....	٥٧٥
ثانياً: إنجليزي - عربي.....	٥٨٥
كشاف الموضوعات .....	٥٩٥

