
بسم الله الرحمن الرحيم

نظرية التشفير والتعمية (الأساسيات)

الجزء الثاني

تأليف

د. ر. هانكرسون　　د. غ. هوفمان

د. أ. لينورد　　ك. ك. ليندنر

ك. ت. فيلبس　　ك. أ. روجر

ج. ر. وول

ترجمة

د. معروف عبدالرحمن سمحان　　د. فوزي بن أحمد الذكير

قسم الرياضيات – كلية العلوم

جامعة الملك سعود

النشر العلمي والمطابع - جامعة الملك سعود

ص.ب ٦٨٩٥٣ - الرياض ١١٥٣٧ - المملكة العربية السعودية

هذه ترجمة عربية مصرح بها من مركز الترجمة بالجامعة لكتاب:

Coding Theory and Cryptography: The Essentials
By: D. R. Hankerson, *et al*.

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

٢مج

٢٣١ص؛ ١٧×٢٤سم

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٩-٢١٩-٥٠٧-٦٠٣-٩٧٨ (ج٢)

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

ديوي ٦٥٢,٨ ١٤٣٥/٩٨

رقم الإيداع: ١٤٣٥/٩٨

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٩-٢١٩-٥٠٧-٦٠٣-٩٧٨ (ج٢)

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 المترجميْن

وقع اختيارنا على ترجمة هذا الكتاب لعدة أسباب أهمّها أن هذا الكتاب يجمع بين موضوعي نظرية التشفير ونظرية التعمية وهما الموضوعان اللّذان 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. واللّه من وراء القصد.

المترجمان

إهداء المؤلفين

إلى زوجاتنا الحبيبات

سندي وجيل وجين وآن وجانيت وسو

إلى أولادنا

نويل وأيان وتيم وكيرت وجيمي وأندرو وميخان وكاترينا وريبركا

وإلى آبائنا وأمهاتنا

إيلين وريتشارد، ڤالي 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

تمهيد
Preface

الهدف من هذا الكتاب المنقّح والمحدّث 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" مبنيّة 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 المقرّر 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 المجرّد أكثر يكون استيعابه أفضل ومن ثم يحتاج إلى وقت أقصر لتغطية المادة الأوليّة.

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 مقرراً بدائياً 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 كافياً 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 المعلن. في الفصل الثاني عشر قمنا بتغطية المواضيع الرئيسة في بنود قصيرة نسبياً 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 السريّة 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.

الرموز
Symbols

$C^{\perp}$: شفرة ثنوية للشفرة C.

C_{23} : شفرة جولاي.

C_{24} : شفرة جولاي الممتدة.

$GF(2^r)$: حقل جالوا.

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

$RM(r,m)$: شفرة ريد ومولر.

$RS(2^r,\delta)$: شفرة ريد وسولومن.

S : الشفرة المولّدة بالمجموعة S.

المحتويات
Contents

مقدمة المترجمـْن ..... هـ

إهداء المؤلفيـن ..... ز

شكر وتقدير ..... ط

تمهيد ..... ك

الرموز ..... س

الجزء الأول: نظرية التشفير

الفصل الأول: مقدمة في نظرية التشفير ١

(١ , ١) مقدمة ١

(١ , ٢) فرضيات أساسية ٤

(١ , ٣) تصويب واكتشاف أنماط الأخطاء ٧

(١ , ٤) معدل المعلومات ١٠

(١ , ٥) تأثير تصويب واكتشاف الأخطاء ١١

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

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

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

الفصل التاسع: شفرات ريد ومولر وشفرات بريبراتا ٣٣٩

(٩,١) شفرات ريد ومولر ٣٣٩

(٩,٢) فك تشفير شفرات ريد ومولر ٣٤٤

(٩,٣) شفرات بريبراتا الممتدة ٣٥٢

(٩,٤) تشفير شفرات بريبراتا الممتدة ٣٦٢

(٩,٥) فك تشفير شفرات بريبراتا الممتدة ٣٦٥

الجزء الثاني: نظرية التعمية

الفصل العاشر: التعمية التقليدية ٣٧٣

(١٠,١) خطط التعمية ٣٧٥

(١٠,٢) التعمية ذات المفتاح المتماثل ٣٧٩

(١٠,٣) أنظمة تعمية فيستل و DES ٣٩٢

(١٠,٣,١) البيانات المحكمة الجديدة ٣٩٥

(١٠,٣,٢) نظام تعمية البيانات القياسي ٤٠٠

(١٠,٤) حواشي ٤١٣

الفصل الحادي عشر: موضوعات في الجبر ونظرية الأعداد ٤١٧

(١١,١) الخوارزميات، تعقد الحسابات، حساب التطابقات ٤١٨

(١١,٢) الرواسب التربيعية ٤٣٠

(١١,٣) اختبار الأوليات ٤٣٩

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

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