مَجمع اللغة العربية بدمشق
المؤتمر السنوي الثامن
نحو رؤية معاصرة للتراث العربي
9-2009/11/13

علم التعمية في التراث العربي

مروان البواب
عضو مَجمع اللغة العربية بدمشق

يرمي هذا المقال إلى التنويه بكَشْفٍ عظيمٍ في عِلْمٍ خَفِيٍّ ظلَّ قرونًا متطاولةً حبيسَ خزائن المخطوطات العربية إلى أن قُدِّر له أن يرى النورَ قبل نحوِ عَقْدَيْنِ على أيدي ثلاثةِ باحثين من مركز الدراسات والبحوث العلمية بدمشق.

أما العِلْمُ، فهو: (التعمية واستخراجُ المعَمَّى)، أو: (التشفير وكَسْرُ الشِّفْرة). وأما الكشْفُ، فهو العثورُ على جملةِ مخطوطاتٍ عربية يعود أقدمُها إلى القرن الثالث الهجري (التاسعِ الميلادي) أثبتَتْ أنَّ العربَ هم آباءُ هذا العلم، وأنهم هم الذين أرسَوْا أُسُسَه وصاغوا قواعدَه، وهم الذين وضعوا مصطلحاتِه وابتدعوا منهجياتِه ومبادئَه. وأما الثلاثةُ الباحثون فهم الدكتور محمد مراياتي، والدكتور يحيى مِير عَلَم، والدكتور محمد حسان الطيان. وقد شَرُفْتُ بمشاركتهم في بعض بحوثهم ودراساتهم.

وقبل أن أسوقَ إليكم قصة هذا الكشف، لا بدَّ من تقديم تعريفٍ موجزٍ بهذا العلم وبأهميته.

أولاً: التعريف بعلم التعمية

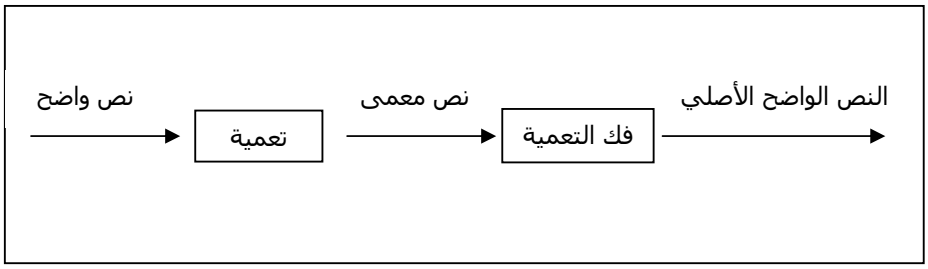
يُقصَد بعلم التعمية Cryptology ركناه الأساسيان: التعميةُ، واستخراج المعمّى.

أما **التعمية** (Cryptography أو Encipherment أو Encryption)، فهي تحويل نصٍّ واضحٍ (Plaintext أو Cleartext) إلى نصٍّ معمًّى غيرِ مفهوم (Ciphertext أو Cryptogram)، وذلك باستعمال طريقةٍ محدَّدة (Cipher method) يستطيع مَن يَعرفُها أن يَفهمَ بها النصَّ الأصليّ.

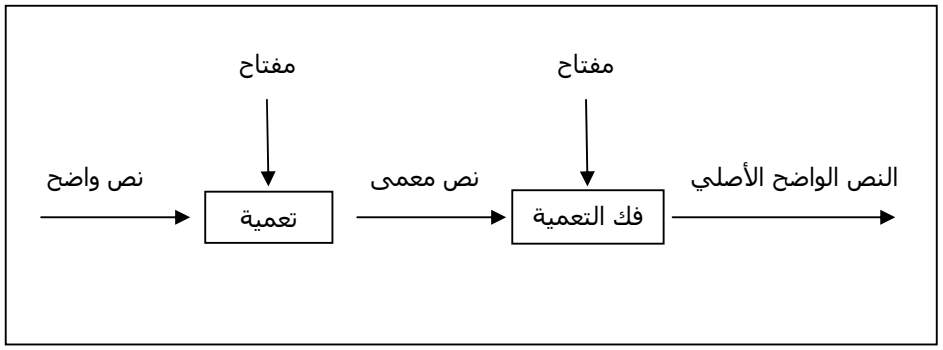
وأما **استخراج المعمّى** (Cryptanalysis)، فهو تحويل النصِّ المعمَّى إلى النصّ الواضح دون معرفة خوارزمية التعمية المستعمَلة.

فإذا ما عُلِمَت الخوارزمية، سُمِّيَ تحويلُ النصّ المعمّى إلى النصّ الواضح بفكّ المعمّى أو فكّ الشِّفرة

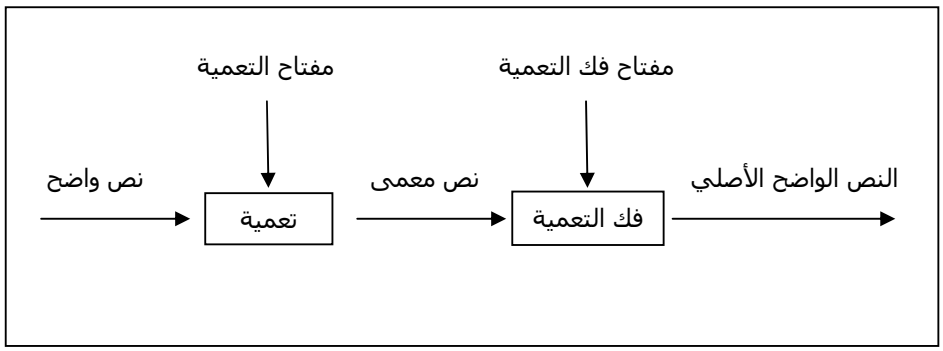
(Decipherment)، كما هو مبيَّنٌ في الشكل الآتي:



ويُستعمل المفتاح (Key) ابتغاء رفع درجة سرية خوارزمية التعمية، حيث يكمن فيه أمانها. يوضِّح الشكل الآتي خوارزمية التعمية بوجود مفتاح:



وفي بعض الحالات تَستعمل بعضُ الخوارزميات مفتاحًا للتعمية مختلفًا عن مفتاح فكِّ التعمية زيادةً في أمنها، كما هو موضَّحٌ في الشكل الآتي:



ويتوسط حقلُ التعمية واستخراجُ المعمَّى منطقةَ التقاطع بين التجسس والدبلوماسية والعمليات الحربية والرياضيات. وكان تاريخه حافلاً بالعديد من الحوادث المثيرة والشخصيات الغريبة والطريفة.

ثانيًا: أهمية علم التعمية

تتجلَّى أهميةُ علم التعمية في تطبيقاته البالغةِ الأهمية. وهذه التطبيقات لا تقتصر –كما قد يُظَنّ– على التطبيقات المتعلقة بالعمليات الحربية والمؤسسات العسكرية، بل تتعدّاها إلى مجالاتٍ شتَّى؛ كأمن الاتصالات والمعلومات، والتجارة، والاقتصاد، والإعلام... وسواها.

فالمصارف مثلاً، تحتاج إلى تعمية حساباتها وتحويلاتِها واتصالاتِها خوفًا من عمليات السطو

والاحتيال. **والنظم الحاسوبية** كذلك، تحتاج إلى تعميةِ قواعدِ معطياتها لمنعِ غيرِ المخوَّلِين من الوصول إليها ومعرفةِ مضمونها، أو العبثِ بها، أو تخريبها. **والإنترنت** التي توفِّر خدماتٍ جُلَّى في حياتنا العملية؛ كالتجارة الإلكترونية (E-Commerce)، والبريد الإلكتروني (E-mail)، وتبادل الملفات FTP (File Transfer Protocol)... هي الأخرى بحاجةٍ إلى التعمية حفاظًا على سِرِّية معلوماتها، وحمايتِها من عبث العابثين واحتيال المتطفلين. **وقنوات البث الفضائية** بحاجةٍ إلى تعميةِ بعضِ برامجها التلفزيونية كيلا يشاهدها إلا المشتركون فيها.

بقي أن نشير إلى أن علم التعمية ذو صلةٍ وثيقةٍ بغيره من العلوم، كعلوم اللغة العربية، والرياضيات، والإدارة، والترجمة. يضاف إلى ذلك أن لهذا العلم الأثرَ الأكبرَ في كشف رموز اللغات البائدة كالهيروغليفية في مطلع القرن الثامن عشر.

ثالثًا: قصة الكشف

والآن إلى قصة هذا الكشف:

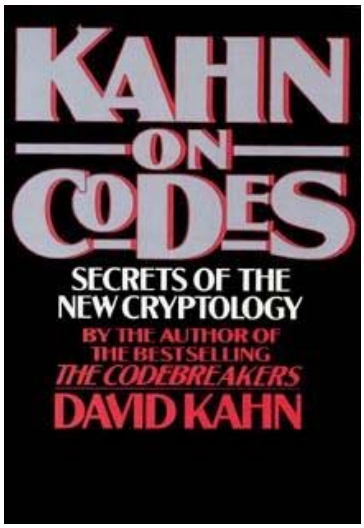
بدأت القصةُ من بضع حقائقَ تاريخيةٍ أوردَها كبيرُ مؤرِّخي هذا العلم البروفسور الأمريكي (ديفيد كان David Kahn) في كتابَيْن؛

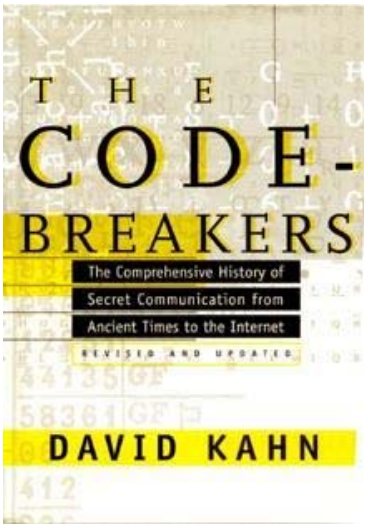
أولهما: *Kahn On Codes: Secrets of the New Cryptology* ((أسرار علم التعمية الجديد)).

وصفتْه صحيفة التايم بأنه: "**ربما كان أفضل وأكمل ما نُشر في علم التعمية حتى الآن.**"

"Perhaps the best and most complete account of cryptography yet published."

وثانيهما: *THE CODEBREAKERS* ((مستخرجو المعَمَّى)). وُسِمَ بأنه من أكثر الكتب مبيعًا.





من هذه الحقائق قولُه في الصفحة الحادية والعشرين من كتاب ((أسرار علم التعمية الجديد)):

"**اطّلعتُ على مقالٍ نُشر في مجلة الدراسات الساميَّة... بيَّن أن العربَ مارسوا استخراج المعمّى قبل الغرب بزمنٍ طويل. ووفَّر لي هذا المقالُ ما أَعُدُّه أكبرَ فتحٍ تاريخيٍّ في كتابي كلِّه.**"

وقولُه في الصفحة الحادية والأربعين من الكتاب نفسه:

"كانت طريقةُ التعمية التي استعملها قيصرُ كافيةً لعصره، لأن أوائلَ مستخرجي التعمية لم يَظهروا إلا بعد عدة قرون منه. فالعربُ هم الذين اكتشفوا مبادئ استخراج المعمّى، إلا أن معرفتهم تقلّصت مع أُفول حضارتهم، ولم يَكتشف الغربُ استخراجَ المعمّى من جديد إلا في عصر النهضة."

وفي الصفحة الرابعة والثمانين بعد المئتين:

"لقد طوّر المسلمون معرفةً نظريةً في استخراج المعمّى تَنِمُّ عن ممارستهم العملية لاعتراض المراسلات واستخراجِ تعميتها، وذلك على الرغم من تشكيكِ بعضِ الباحثين في ذلك. ولمّا كان التراثُ الإسلاميُّ المخطوطُ لا يزال غيرَ مكتشفٍ في معظمه، فقد يُحصّل الباحثُ فيه اكتشافاتٍ جديرةً بالتقدير."

وقولُه في الصفحة الثالثة والتسعين من كتاب ((مستخرجو المعمَّى)):

"لم نَجدْ في أيٍّ من الكتابات التي نَقَّبْنا عنها أيَّ أثرٍ واضحٍ لعلم استخراج المعمّى حتى الآن... ومن ثَمَّ فإن علمَ التعمية الذي يشمل التعميةَ واستخراجَ المعمّى لم يُولَد حتى هذا التاريخ [القرن السابع الميلادي] في جميع الحضارات التي استعرضناها، ومنها الحضارةُ الغربية.

لقد وُلِدَ علم التعمية بشقَّيْه بين العرب؛ إذ كانوا أولَ من اكتشف طرق استخراج المعمّى ودوَّنها. وإن هذه الأمةَ التي انبثقتْ من الجزيرة العربية في القرن السابع الميلادي، والتي أشعَّت فوق مساحاتٍ شاسعةٍ من العالَم المعروف، أخرجتْ بسرعةٍ واحدةً من أرقى الحضارات التي عَرَفها التاريخُ حتى ذلك الوقت. لقد ازدهر العلم، فأصبحتْ علومُ الطبِّ والرياضياتُ أفضلَ ما في العالَم. ومن الرياضيات جاءت كلمة التعمية (cipher) [أي الصفر]... ولما كانت ديانةُ هذه الحضارةِ قد حرَّمت الرسمَ والنحتَ [للأحياء]، فقد حضَّتْ بالمقابل على التعمُّق في تفسير القرآن الكريم، فأدَّى ذلك إلى أن تَنصبَّ الطاقاتُ الخلاَّقةُ الكثيرةُ في متابعة الدراسات اللغوية، وفي الألغاز والأحاجيِّ والرموز والتوريات والجناس وأمثالها من الرياضات الذهنية اللغوية... فأدَّى كلُّ هذا إلى أن يتضمَّن الكتابةَ السرِّية."

ولدى تتبُّعِ هذه الأقوال تَبيَّن أن مؤلِّف هذين الكتابَين اعتمد فيهما على ما جاء في كتاب ((صبح الأعشى في صناعة الإنشا)) للقلقشندي (821 هـ/1418 م) الذي عَقَدَ بابًا سَمَّاه: (باب إخفاء ما في الكتب من السِّر)، أكثرَ النقلَ فيه عن رسالةٍ تدعى: ((مفتاح الكنوز في إيضاح المرموز)) لابن الدُّرَيْهِم. ولئن عبَّر (ديفيد كان) عن أسفه الشديد لِفَقْد رسالة ابن الدريهم، لقد ضَمَّنَ ملحقاتِ كتابِهِ رسائلَ وردتْ إليه تُنْكِر وجودَ ابن الدريهم أصلاً، وتزعم أنه ضربٌ من الخيال أو الوهم.

من هنا بدأتْ رحلةُ البحث والتنقير عن تلكم المخطوطةِ المفقودة: ((مفتاح الكنوز في إيضاح المرموز))، وعن صاحبها المجهول: (ابن الدريهم).

بدأتِ الرحلةُ من المكتبة الظاهرية، فعثر الثلاثةُ الباحثون على مخطوطتَيْن لابن الدريهم، ولكنْ لا علاقةَ لهما بعلم التعمية. غير أنهم عثروا في أثناء بحثهم على رسائلَ في التعمية البديعية، [وهي ضربٌ من ضروب التعمية تعتمد على إخفاء المعاني بالتورية، ومحلُّها الشعر تزيينًا له وإلغازًا فيه، وكان هذا النوع من التعمية منتشرًا في التاريخ العربي الإسلامي، وحُقِّقتْ مخطوطاتٌ عديدةٌ منه]. ومع أن رسائل المعمَّى البديعي لم تكن مقصودَ البحث، غير أنَّ اكتشافها قوَّى عزيمتَهم وشَحَذَ هِمَّتهم لمتابعة البحث، فرحلوا من دمشق إلى اصطنبول؛ من المكتبة الظاهرية إلى المكتبة السُّلَيْمانية حيث ترقد الكثرةُ الكاثرة من المخطوطات العربية. وهناك وجدوا ضالتهم: ((مفتاح الكنوز في إيضاح المرموز)) لابن الدريهم المِوْصِلِيّ، وقد كُتِبَ اسْمُ الرسالة في جذاذة الفهارس هكذا:

غير أن المفاجأة الكبرى لم تكن في عثورهم على هذه المخطوطة التي كانت بحكم المفقودة، بل كانت في عثورهم على **أقدم مخطوطةٍ في علم التعمية وأهمِّها على الإطلاق**، إنها: ((**رسالة الكندي في استخراج المُعَمَّى**)) لفيلسوف العرب المشهور يعقوب بن إسحاق الكِنْدِيّ؛ ذلك أن صاحبها سَبَقَ ابنَ الدريهمِ بخمسةِ قرون؛ إذ إنَّ تاريخ وفاة الكندي كانت سنةَ (260 هـ)، على حينَ كانت وفاةُ ابن الدريهم سنةَ (712–762 هـ/1312–1359 م). فكان الكنديُّ بحقٍّ أبا علمِ التعمية.

وكان من جملة ما عثروا عليه في المكتبة السليمانية كذلك مجموعٌ يَشتمل على ثماني رسائل في التعمية، ومخطوطاتٌ تُعنى بالأقلام القديمة [وهي أقلام ذاتُ صلةٍ وثيقةٍ بعلم التعمية، كان لها الأثرُ الأكبرُ في كشف اللغات القديمة، كما أسلفنا قبل قليل]. من هذه المخطوطات: ((حل الرموز وبرء الأسقام في أصول اللغات والأقلام)) لذي النون المصري (248 هـ/859 م)، تشتمل على مئتي قلم، ومخطوطةٌ أخرى للجَلْدَكِيّ، تشتمل على سبعين قلمًا، ومخطوطةٌ ثالثةٌ مجهولةُ المؤلِّف.

كانت تلكم محطةَ البحثِ الثانيةَ في رحلة الكشف.

أما المحطةُ الثالثةُ فكانت المكتبةَ الوطنيةَ بباريس. فمن هذه المكتبة حَصَلوا على مخطوطةٍ في الأقلام القديمة غايةٍ في الأهمية، عنوانها: ((شوق المستهام في معرفة رموز الأقلام)) لابن وحشيَّةَ النَّبَطِيّ (نحو291 هـ/914 م).

كذلك تجمَّعتْ لديهم جملةٌ صالحةٌ من المخطوطات في علم التعمية، لم يرتحلوا إليها، وإنما ساعدهم على الحصول عليها أساتذةٌ أجلاءُ، وأصدقاءُ نبلاء. ومع ذلك فهم يعتقدون أنها –على غناها وكثرتِها وتنوُّعِها– غيضٌ من فيض؛ ففي جَعْبَتِهم عناوينُ كثيرةٌ لَمَّا يصلوا إليها بَعْد، وما زال البحث عنها جاريًا.

من ذلك مثلاً كتاب ((المعَمَّى)) المنسوب إلى شيخ شيوخ العربية الخليل بن أحمد الفراهيدي (100-170 هـ/718–786 م). نسب إليه الزبيدي في ((طبقات النحويين واللغويين)) [ص 51] كتابًا في المعمّى، ولا أثر له. ونقله عنه ابن نُباتة في كتابه ((سَرْح العيون في شرح رسالة ابن زيدون)) وجعله أوَّل من وضع علم المعمَّى. ثم نقله محمد بن الحنبلي عن ابن نُباتة في رسالته ((شرح كَنْز من حاجى وعَمَّى في الأحاجي والمعَمَّى)) [3/ب – 4/أ] مصورة عن نسخة المكتبة الظاهرية.

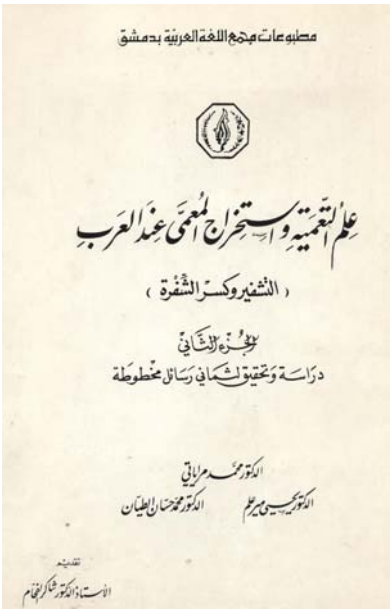
رابعًا: إخراج مخطوطات علم التعمية

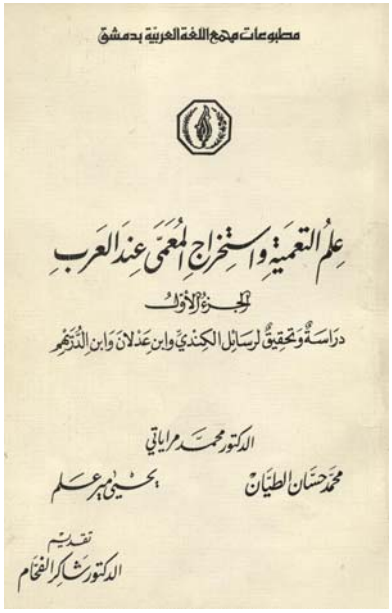
عَكَفَ الثلاثةُ الباحثون على دراسة هذه المخطوطات وتحقيقِها وتحليلِها، وساعدهم في ذلك بادئ الأمر الأستاذُ العلامةُ أحمد راتب النفاخ رحمه الله، فأخرجوا فيها كتابًا في جزأين بعنوان: ((علم التعمية واستخراج المعمى عند العرب))، أصدرهما مجمع اللغة العربية بدمشق ضمن مطبوعاته. وكانت اليدُ الطولى في تيسير إخراج هذا الكتاب للأستاذِ الدكتور شاكر الفحام رحمه الله الرئيسِ السابقِ للمجمع، وللأستاذِ

الدكتور عبد الله واثق شهيد المديرِ السابق لمركز الدراسات والبحوث العلمية.

اشتمل الجزء الأول على دراسةٍ موسَّعة لتاريخ علم التعمية عند العرب، إضافةً إلى دراسةٍ وتحقيقٍ لرسائل الكندي وابن عدلان وابن الدريهم. نُشر سنةَ 1987، ويقع في 438 صفحة.

واشتمل الجزء الثاني على دراسةٍ وتحقيقٍ لثماني مخطوطات لابن دنينير والجرهمي وابنِ وَهَب الكاتب وابنِ طَباطَبا وغيرهم. نُشر سنةَ 1997، ويقع في 474 صفحة.





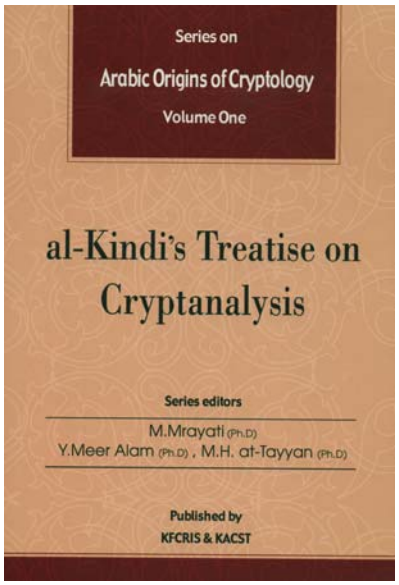
ويجري العمل الآن على إصدار الجزء الثالث الذي يتضمَّن دراسةً وتحقيقًا لمخطوطة «شوق المستهام في معرفة رموز الأقلام» لابن وحشيَّة.

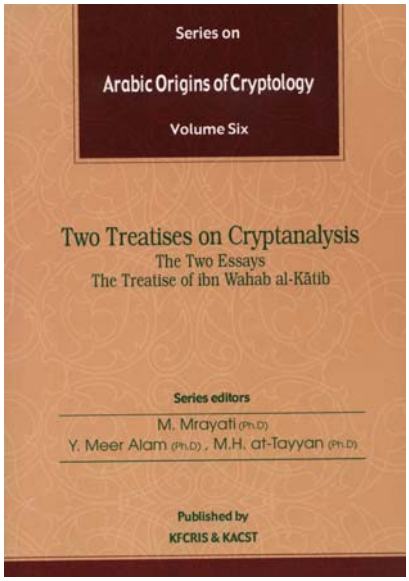
بعد صدور الجزء الأول من كتاب «علم التعمية واستخراج المعمَّى»، واطِّلاع (ديفيد كان) على مستخلصه الإنكليزي، أرسل إلى مركز الدراسات والبحوث العلمية بدمشق رسالةَ شكرٍ قال فيها: "**إنني أرى من المستخلص الإنكليزي أن الكتابَ إسهامٌ عظيمٌ في تاريخ علم التعمية، ومدعاةٌ كبرى لامتناني الشخصي وتقديرِ سائر المهتمين بهذا المبحث والمؤرِّخين له... وأتطلَّع بفارغ الصبر إلى تلقِّي الطبعة الإنكليزية الكاملة من هذا العلم**".

وبالفعل، فقد نهض المترجمُ المفَنّ الأستاذ سعيد الأسعد من مركز الدراسات والبحوث العلمية بترجمة هذا الكتاب بجزأيه إلى الإنكليزية، وراجعه الأستاذ الدكتور إبراهيم القاضي والأستاذ الدكتور محمد السويِّل والأستاذ مروان البواب.

طُبعتْ هذه الترجمةُ بتمويلٍ من مدينة الملك عبد العزيز للعلوم والتقنية بالرياض، ومركز الملك فيصل للدراسات والبحوث الإسلامية. وشغلتْ ستةَ أجزاءٍ من سلسلة Series on Arabic Origins of Cryptology «الأصول العربية لعلم التعمية»، أصدرها مركز الملك فيصل للبحوث والدراسات الإسلامية (KFCRIS)، ومدينة الملك عبد العزيز للعلوم والتقانة (KACST).

وفيما يلي صورة غلاف المجلدَيْن الأول والأخير من هذه السلسلة:





وقد لَقِيَتْ هذه السلسلةُ ترحيبًا واسعًا واهتمامًا كبيرًا في الوسط العلمي ولدى المتخصِّصين والمهتمين في جميع أرجاء العالَم، واقتُبِسَ منها في كتبٍ مختلفة وبرامجَ إذاعيةٍ وتلفازية ووسائلَ نشرٍ متعدِّدة. (يمكن الاطلاع على مقتبساتٍ من مراجعاتٍ نقديةٍ للمجلد الأول من هذه السلسلة على موقع الرابطة الدولية لعلم التعمية: **www.iacr.org/newsletter/v20n3/newbooks.html**)

وإليكم بعضَ التقاريظ التي كُتبت عن هذه السلسلة:

"It is an excellent job, and a major contribution to the history of cryptology." (David Kahn, 18 August 2003)

"إنه عملٌ رائع، وإسهامٌ عظيمٌ في تاريخ علم التعمية." (ديفيد كان)

"It is difficult when reading al-Kindi's treatise on cryptanalysis to imagine that it was written 1150 years ago. It is entirely 'modern' in its scientific methodology and even in its explanations…This is a book that must be read, and re-read, by every person with a real interest in cryptology." (James L. Massey, Copenhagen, Denmark, 31 August 2003)

"يصعب على المرء –عندما يقرأ رسالة الكندي في استخراج المعمَّى– أن يتخيَّل أنها أُلِّفتْ قبل 1150 سنة. إنها رسالةٌ 'حديثة' تمامًا في منهجيتها العلمية، وحتى في شروحها واستقصاءاتها... إنه كتابٌ يجدر بكلّ مَن له اهتمامٌ حقيقيٌّ بعلم التعمية أن يقرأه ويعيد قراءته." (جيمس ماسي)

"We are pleased to review this wonderful work and bring it to the attention of our readers." (Brian Winkkel, Editor of the review Cryptologia. 5 Oct. 2003)

"نحن سعداءُ لمراجعة هذا العمل الرائع، ولَفْتِ نظر قرّاء مجلتنا إليه." (محرّر مجلة Cryptologia)

"One of the most enjoyable parts of Ibn Adlan's manuscript is its closing section where he takes the reader through a complete example of a cryptogram that he had broken 775 years ago, describing his false starts, corrections, and ultimate success. Anyone who has worked in cryptanalysis will recognize this as the authentic experience of a highly skilled cryptanalyst." (James L. Massey, Copenhagen, Denmark, 14 February 2004)

"من أمتعِ ما في مخطوطة ابن عدلان فصلُها الأخير، حيث يُطلع القارئَ على مثالٍ كاملٍ لرسالةٍ معمَّاةٍ كان كَسَرَها قبل 775 سنة، واصفًا بداياته المتعثِّرة، وتصحيحاته، ثم نجاحه النهائي. ولا شك في أن كل مَن يعمل في مجال استخراج المعمَّى سيرى في هذا تجربةً حقيقيةً من مستخرجِ تعميةٍ حاذق." (جيمس ماسي)

"Volume 3 contains Ibn ad-Durayhim's treatise on cryptanalysis. His most important and intriguing contribution was the quite explicit introduction of modular arithmetic… I must say that I found Volume 4 with Ibn Dunaynīr's treatise to be the most interesting of these newly translated books… Ibn Dunaynīr made an important cryptographic innovation, namely the use of numbers to represent letters..." (James L. Massey, Copenhagen, Denmark, 8 February 2007)

"يشتمل المجلد الثالث على رسالة ابن الدريهم في استخراج المعمَّى. وكان إسهامه العظيم والآسر فيها هو المقدمة الجليّة في الحساب المعياري..... وأرى لزامًا عليَّ أن أقول بأنني وجدتُ المجلد الرابع – المتضمّن رسالةَ ابن دنينير– أكثرَ إمتاعًا وإثارةً للاهتمام من بين المجلدات الثلاثة المترجَمة حديثًا [الثالث والرابع والخامس]... ذلك أن ابن دنينير ابتدع أفكارًا تعمويّةً مهمة، ولاسيما فيما يتعلَّق باستعمال الأرقام في تمثيل الحروف... " (جيمس ماسي)

وقبل الحديث عن السَّبْقِ الذي أحرزه علماؤنا العرب في ميدان التعمية واستخراج المعمى، سأوجز القول في وصف أربع مخطوطات منها تَنِمُّ عمَّا وراءَها.

خامسًا: التعريف بأهم مخطوطات علم التعمية وأصحابها

1– رسالة الكندي في استخراج المعمّى

المؤلِّف: فيلسوفُ العرب يعقوب بن إسحاق الكندي، عَدَّهُ الطبيبُ والرياضيُّ الإيطالي كاردانو [1501–1576] واحدًا من أعظم الحكماء الاثني عشر الذين ظهروا في تاريخ الإنسانية. واعترف الفيلسوف الإنكليزي بايكون (Bacon) بفضله فقال: "إن الكندي والحسن بن الهيثم في الصف الأول مع بطليموس". ولد بالكوفة، وكان أبوه أميرًا عليها في عهد الخليفة العباسي المهديّ، ونشأ بالبصرة، ثم انتقل إلى بغداد حيث حصّل جلَّ علومِه، فبرع في الطبّ والفلسفة والحساب والهندسة والفلك وغيرها. وقد أصاب منْزلةً عظيمة لدى خلفاء بني العباس، وتولّى بيتَ الحكمة (أعظمَ صرحٍ ثقافيٍّ عرفته الحضارةُ العربيةُ الإسلامية). توفي سنة 260 هـ/873 م، مخلِّفًا ثروةً فكريةً هائلةً في علوم شتَّى بلغتْ نحوًا من مئتين وتسعين مصنفًا.

الرسالة: رسالةُ الكندي هي أقدمُ ما وقع بين أيدي الباحثين من آثارٍ في التعمية واستخراج المعمّى، إذ يعود تأليفُها إلى القرن الثالث الهجري (التاسع الميلادي). وتقع ضمن مجموعٍ كبيرٍ يشتمل على ستين مصنَّفًا من كتب ورسائل يعقوب بن إسحاق الكندي. وهذا المجموعُ محفوظٌ في خزائنِ مكتبةِ آيا صوفيا ضمن المكتبة السليمانية برقم (4832).

وفيما يلي مصوَّرة الصفحتَيْن (الأولى والأخيرة) من رسالة الكندي:

استكملتِ الرسالةُ أسبابَ التأليف العلميّ المنهجيّ في هذا الفنّ عمقًا وشمولاً، فأبرزتْه عِلمًا قائمًا بذاته، له أصولُه وطرائقُه المختلفة. ولا غرو، فسَعَةُ اطِّلاع مؤلِّفها وتَنَوُّعُ موارده، والمكانةُ التي تبوَّأها: أستاذًا للخلفاء، وصاحبًا للمكتبة الكِنْدِية، ومديرًا لبيت الحكمة، جعلتْ من رسالته المرجعَ الأولَ لأصحاب هذا الفن. فقد عوَّل عليها ابنُ دنَينِير [626 هـ] في مؤلَّفه: ((مقاصد الفصول المترجِمَة في حلّ الترجمة)). وكذلك أفادَ ابنُ الدريهم [762 هـ] من تقسيماتها في مؤلَّفِه: ((مفتاح الكنوز في إيضاح المرموز)).

يمكن تقسيم الرسالة إلى خمسة فصول هي: سُبُلُ استخراج المعمّى، وأنواعُ التعمية العظام، ومناهجُ استخراج بعض أنواع التعمية، ودورانُ الحروف ومراتُبها في اللغة العربية، واقترانُ الحروف وامتناعُهُ في اللغة العربية.

وقد تجلتْ ريادة الكندي في هذه الرسالة بسبقه إلى: التفريق بين طرق التعمية الأساسية، وحديثه عن التعمية المركبة، واستعماله الطرق التحليلية في استخراج المعنى باستعماله تواتر الحروف ومراتبها، واعتماده تواتر الثنائيات لدى استعماله اقتران الحروف وتنافرها، واستعماله مبدأ الكلمة المحتملة، وفهمه الدقيق لطبيعة الحروف وتمييزه بين الصامتة (الخُرْس) والمصوّتة الكبيرة والصغيرة .

2- مقاصد الفصول المترجِمة عن حلّ الترجمة

المؤلِّف: إبراهيم بن محمد بن إبراهيم المعروف بابن دنينير. ولد بالمَوْصل سنة 583 هـ/1187 م، ونشأ فيها ونُسب إليها. برع ابنُ دنينير في التعمية إضافةً إلى الشعر، فله في التعمية كتابان حسبما ذكر

الصفدي [في كتابه...] أولهما: ((الشهاب الناجم عن علم وضع التراجم))، وثانيهما رسالة ((مقاصد الفصول المترجِمَة في حلِّ الترجمة)) التي أشرنا إليها آنفًا. وله في الشعر كتابان؛ الأول: ديوانُه الشعري، والثاني: ((الكافي في علم القوافي)). توفي ابن دنينير في بانياس سنة 627 هـ/1229 م.

الرسالة: اعتمد ابن دنينير في رسالته هذه على الكندي اعتمادًا كبيرًا؛ فهو تارةً يشرح ما أوجزه الكندي، وأخرى يوجز ما بسط القولَ فيه. على أنه أضاف إلى ما ذكره الكندي بعضَ الطرائق التي تحتاج ممارستُها إلى أدواتٍ عمليةٍ كطريقة رقعة الشطرنج، والخرز الملون، والكتابة على دَرْج... إلخ. وأفاض في الكلام على طرق التعمية بالإخفاء (Concealment). وعرض بعض طرائق التعمية المركبة؛ كاستعمال طريقتَي القلب والإعاضة معًا. وكان الموضوع الذي استغرق شطرًا من رسالته هو استخراج المعمّى من الشعر.

3- المؤلَّف للملك الأشرف في حلّ التراجم

المؤلِّف: علي بن عدلان بن حماد بن علي، عفيفُ الدين المَوْصلي النحْوي المترجِم. وُلِدَ بالموصل سنة 583 هـ/1187 م (وهي السنة نفسها التي وُلد فيها ابن دنينير، غير أنه عُمِّرَ بعده ثلاثًا وثلاثين سنة). أخذ النحوَ عن جماعةٍ يَقْدُمُهم أبو البقاء العكبري. كان أعجوبةً في الذكاء، رأسًا في الأدب، شاعرًا مُجيدًا، حتى إن بعضهم عدّه أحد أذكياء بني آدم. وَضَعَ في علم التعمية ثلاثةَ كتبٍ هي: ((عُقلة المجتاز في حلّ الألغاز))، و((المعْلَم))، و((المؤلَّف للملك الأشرف)). ووضع كتابًا في النحو سمّاه: ((الانتخاب لكشف الأبيات المشكلة الإعراب)). توفي بالقاهرة سنة 666 هـ/1268 م.

الرسالة: اختصّتْ رسالةُ ابن عدلان باستخراج المعمّى، إذ لم يتطرقْ فيها إلى أنواع التعمية وطرائقِها المتشعِّبة، بل عرض فيها عشرين قاعدة في استخراج المعمّى، سبقتْها فاتحة، ولَخِقَتْها خاتمة. وأقربُ ما توصف به هذه الرسالة بأنها دليلٌ عملي (Handbook أو Manual) في استخراج التعمية.

4- مفتاح الكنوز في إيضاح المرموز

المؤلِّف: علي بن محمد بن عبد العزيز المعروف بابن الدريهم. وُلد بالموصل سنة 712 هـ/1312م، ونشأ فيها. دَرَسَ على كثير من علماء عصره، وتنقّل تاجرًا بين دمشق والقاهرة غيرما مرة. توفي سنة 762 هـ/1361 م. برع ابنُ الدريهم في كثير من العلوم، لكنَّ شهرتَهُ ومهارته كانت في التعمية والأحاجي والألغاز وحلِّ المترجَم وخواصِّ الحروف... وصنَّف في هذه العلوم كثيرًا من الكتب والرسائل؛ منها: ((إيضاحُ المبهَم في حلِّ المترجَم))، و((غاية الإعجاز في الأحاجي والألغاز))، و((قصيدةٌ في حلِّ رموز الأقلام المكتوبة على البرابي))، و((مفتاح الكنوز في إيضاح المرموز)).

الرسالة: تعدّ هذه الرسالةُ أوسعَ مخطوطات هذا العلم وأكثرَها تفصيلاً، وهي إلى ذلك تدلّ على أن ابن الدريهم عانى هذا العلم ومارسه، يؤيد ذلك أنه عمل في خدمة بعض الملوك كالملك الناصر. وقد

اشتملت الرسالةُ على عدة مواضيع أهمُّها: ضروبُ التعمية، ومنهجيةُ حلّ الترجمة، ومقدمةٌ صرفية، وما لا بدّ منه لِمَن يعاني حلّ الترجمة، وختمها بمثالَيْن عمليَّيْن في حلّ الترجمة.

وفيما يلي مصوَّرة الصفحتَيْن (الأولى والأخيرة) من رسالة ابن الدريهم:

هذا ويمكن أن نوجز نقاط السَّبْق الذي حقّقه علماؤنا العربُ في هذا العلم بما يلي:

1- الكندي أولُ مَن كَتَبَ مخطوطةً في استخراج المعمّى، وذلك في القرن الثالث الهجري (التاسع الميلادي)، أي قبل نحو ستة قرون من الإيطالي ألبيرتي (Alberti) الذي يَصف مؤرِّخو الغرب كتابَه بأنه أول مخطوطة في هذا العلم.

2- الكندي أوّلُ مَن فَرَّق بوضوح بين طريقتَي التعمية الأساسيتَين: الإبدال والقلب، أي قبل بورتا (Porta) بنحو سبعة قرون.

3- الكندي أولُ مَن استخدم فكرة الكلمة المحتملة التي تُنسَب خطأً إلى بورتا.

4- ابنُ عدلان أوّلُ مَن استعمل النصوص بدون فاصل، وأسماها المُدْمَج، وذلك قبل بورتا بثلاثة قرون.

5- ابنُ الدريهم هو صاحب فكرة جدول فيجونيير (Vigenère) المشهور، وذلك قبل فيجونيير بقرنين.

6- ابن الدريهم هو الذي عرض طريقة التعمية باستعمال شبكة بسيطة، وذلك قبل كاردانو

(Cardano) بقرنين أيضًا.

7- ابن وَحشيَّة النَّبَطي أول من كشف اللثام عن رموز اللغة الهيروغليفية القديمة، وذلك قبل فرانسوا شامبليون بتسعة قرون.

وتَحسُن الإشارة هنا إلى أهم أوجه الاستفادة المعاصرة لنتاج تحقيق مخطوطات التعمية؛ من ذلك مثلاً:

- إحياء المصطلحات العربية الأصيلة في هذا العلم الحيِّ والمهم، وانتشار استعمالها عالميًّا.
- انتشار الإشارة إلى الكندي في معظم الكتب العالمية التي تتطرَّق إلى موضوع علم التعمية؛ مثل: كتاب دافنشي كود، إضافةً إلى مقالاتٍ عديدة على الإنترنت.
- الإفادة من مخطوطة الكندي في تدريس مادة أمن المعلومات في العالم العربي، ولاسيما أن البروفسور ماسي قد وصف المخطوطة بأنها "كتاب معاصر".

سادسًا: خوارزميات التعمية

رأَينا أن من تمام البحث أن نلمَّ إلمامةً سريعةً بطرائق التعمية التي ذكرها العلماء العرب، وما آلت إليه في عصرنا الحالي. ذلك أن طرائق التعمية – على كثرة تشعُّبها وتنوُّع وسائلها – بقيتْ مبادئها على ما هي عليه منذ أن وضعها علماؤنا العرب. يؤيد هذا ما أورده بروس شناير مؤلف كتاب "التعمية التطبيقية" [*Applied Cryptography*, 1996] في الصفحة الحاديةَ عشرة:

"قبل عصر الحاسوب، كانت خوارزميات التعمية قائمةً على الحروف، وكانت تقوم إما بإبدال الحرف بغيره أو بتغيير موضعه. وكانت أفضل الخوارزميات تفعل الشيئين معًا، عدَّة مراتٍ لكلٍّ منهما.

ثم غدت الأمور أكثرَ تعقيدًا هذه الأيام، لكن الفلسفةَ بقيت نفسها. والتغيُّر الرئيسي هو أن الخوارزميات تتعامل اليوم مع البتات عوضًا عن الحروف، وهذا عمليًّا ليس سوى تغييرٍ لحجم الأبجدية من 26 عنصرًا [في الإنكليزية] إلى عنصرين [هما الصفر والواحد]. ومازالت معظمُ خوارزميات التعمية الجيدة تَجمع بين عناصر من التعويض وتغيير المواضع".

وسنوجز فيما يلي الكلامَ على أهم هذه الخوارزميات.

1- التعمية بتغيير الموضع (Transposition)

وتكون بتغيير مواضع حروف النص الواضح وفق قاعدة معينة. وهناك أساليبُ كثيرةٌ تتفرع عن هذه الخوارزمية، نكتفي بذكر اثنين منها:

الأسلوب الأول: تغيير موضعَيْ كلِّ حرفين من حروف النص الواضح؛ أي إن الحرفَ الأوّلَ يَحِلُّ مَحَلَّ الثاني، والثاني مَحَلَّ الأول، والثالثُ يحل محل الرابع، والرابع محل الثالث، وهكذا إلى أن ينتهي النص. ويجري فكُّ تعمية هذه الخوارزمية بتغيير موضعي كل حرفين من حروف النص المعمَّى بطريقةٍ معاكسة للتعمية.

مثال: **النص الواضح: مجمع دمشق يرحب بضيوفه**

النص المعمّى: جمعم مدقش ريبح ضبويهف

الأسلوب الثاني: يُكتَبُ النصُّ الواضح على أسطرٍ ذات عرضٍ ثابت، ويُقرأ النصُّ المعمَّى عموديًّا.

ويجري فكُّ تعمية هذه الخوارزمية بعملية معاكسة.

مثال: **النص الواضح**: **م ج م ع**

د م ش ق

ي ر ح ب

ب ض ي و

ف هـ

النص المعمى: **م د ي ب ف ج م ر ض هـ م ش ح ي ع ق ب و**

2- **التعمية بالإعاضة أو التبديل** (Substitution)

وتقوم على تبديل حروف النص الواضح، ووضع حروفٍ أو رموزٍ أخرى مكانها. ولهذه الطريقة كسابقتها أساليبُ كثيرةٌ تتفرع عنها، أشهرها الإعاضة البسيطة (simple substitution)؛ وفيها نستعيض عن كل حرفٍ من النص الواضح بحرفٍ مقابل له. فمثلاً نستعيض عن كل حرف من النص الواضح بالذي يليه في ترتيب حروف المعجم؛ أي نضع حرف الباء بدلاً من حرف الألف، والتاء بدلاً من الباء، والثاء بدلاً من التاء،... وهكذا.

فإذا كان النص الواضح: **مجمع دمشق يرحب بضيوفه**

يصبح النص المعمّى: **نحنغ ذنصك ازخت تطايقو**

وقد صُنِعتْ آلات تعتمد مبدأ الإعاضة البسيطة، سُمِّيت آلات القلب الدوار، كان من أبرزها الآلة Enigma التي استعملها الألمان في الحرب العالمية الثانية.

3- **التعمية بزيادة حروفٍ (أو كلمات) أغفالٍ** (Nulls)

وتقوم على زيادة حروفٍ (أو كلمات) على حروف النص الواضح، وفق قاعدة محددة. ولهذه الطريقة كسابقتَيْها أساليبُ كثيرةٌ تتفرع عنها. مثال ذلك أن نزيد حرفَ اللام بعد كلِّ ميمٍ من النص الواضح، وحرفَ النون بعد كل باء.

فإذا كان النص الواضح: **مجمع دمشق يرحب بضيوفه**

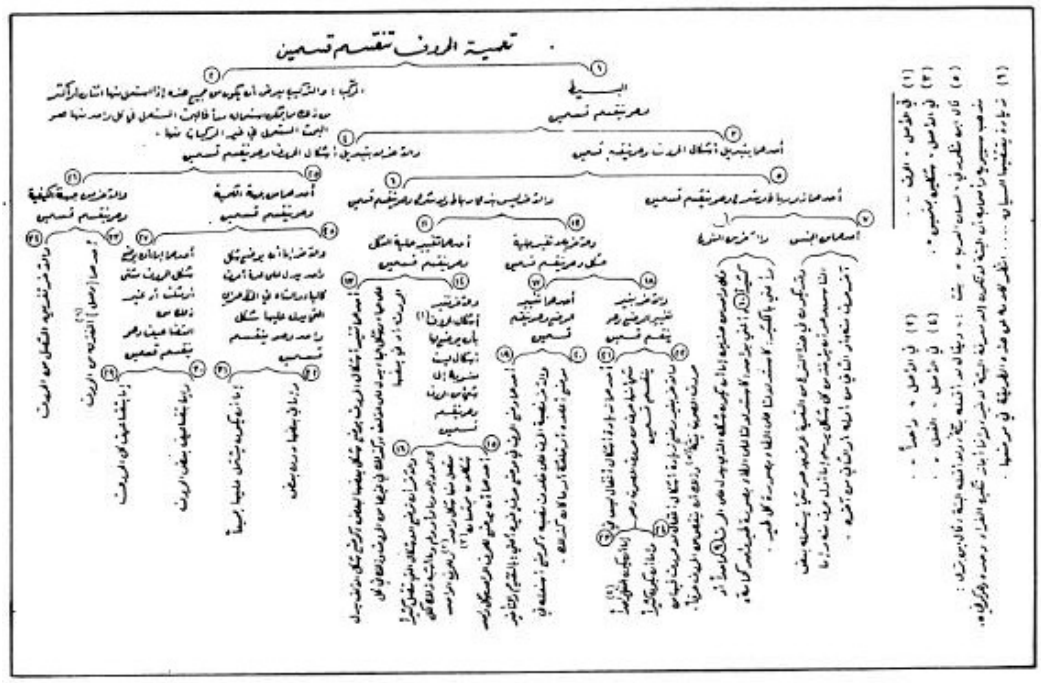
يصبح النص المعمّى: **ملجملع دملشق يرحبن بنضيوفه**

4- التعمية المركبة (Super-encipherment أو Composite Cipher)

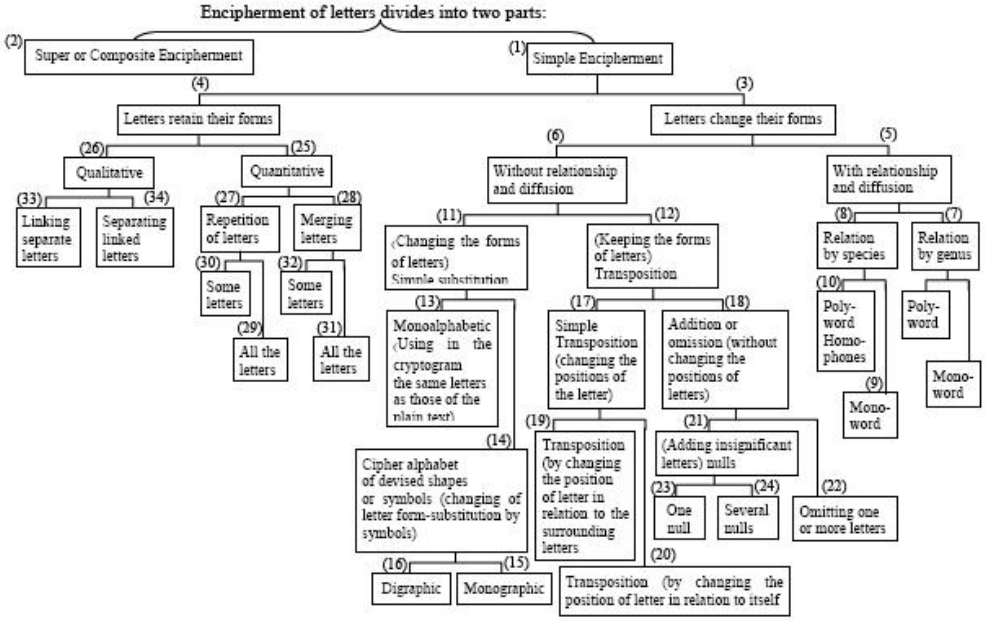
وتكون باستعمال طريقتين أو أكثر من طرائق التعمية الثلاث السابقة في آنٍ واحد. وسوف ينتج عن تطبيق ذلك عدد هائل من أساليب التعمية.

لقد أوفى علماؤنا على الغاية في استقصاء وضع طرائق التعمية؛ وحسبنا أن نشير في هذا المقام إلى ما أورده الكندي في رسالته من أنواع التعمية العظام.

المخطط الشجري لطرائق التعمية كما ورد في رسالة الكندي



المخطط الشجري السابق بعد نسخه من مخطوطة الكندي



الترجمة الإنكليزية للمخطط الشجري السابق

سابعًا: مبادئ استخراج المعمّى

يمكن إعادة أساليب استخراج المعمّى إلى ثلاثة مبادئ أساسية، سنعرضها موجزةً فيما يلي:

المبدأ الأول: استعمال الصفات الكمية للحروف (Quantitative)

ويقوم على معرفة تواتر الحروف (أو دورانها) في النصوص (Frequency Count)؛ أي معرفة مراتب تلك الحروف في الاستعمال، لتقابَلَ بمراتب الرموز المستعملة في الرسالة المعمّاة. وقد أجرى بعض علماء التعمية إحصاءاتٍ للحروف بأنفسهم، وقسَّموا الحروف إلى ثلاث مراتب: كثيرةِ الدوران، ومتوسطةِ الدوران، وقليلةِ الدوران. ففي العربية يجيء حرفُ الألف في المرتبة الأولى في دوران الحروف، يليه حرفُ اللام، ثم الميم... على حين يجيء حرفُ الظاء في المرتبة الأخيرة، وقبلَه حرفُ الغين... وهكذا. ومن المعلوم أن مراتب الحروف تختلف عمومًا باختلاف طبيعة النصوص اللغوية المحصاة.

إن هذا المبدأ هو مما سبق إليه العرب؛ إذ لم يُكتَب عنه لدى الغربيين إلا في القرن الخامس عشر الميلادي، عندما وضع ألبيرتي (Alberti) أولَ رسالة له في التعمية. على حين أن الكندي كتب عن هذا المبدأ في القرن الثالث الهجري/التاسع الميلادي، أي قبل ألبيرتي بستة قرون، وسمّاه: (الحيل الكميّة).

وقد كانت لي تجربةٌ عملية في هذا الصدد؛ إذ وضعتُ برنامجًا حاسوبيًّا يستطيع استخراج النصوص العربية المعمَّاة بطريقة فيجونيير. وقد اعتمدتُ في هذا البرنامج على إحصائيات دوران الحروف التي وردت عند الكندي وابن دنينير وابن عدلان إضافةً إلى ثلاث إحصائياتٍ أخرى أجريتُها على نصوصٍ عربية مختلفة تناولت دوران الحروف الأحادية والثنائية والثلاثية، ودوران الحروف التي ترد في بداية الكلمات وفي نهايتها.

يبيّن الجدول الآتي دورانَ الحروف ونسبَها المئوية مرتبةً تنازليًّا عند الكندي وابن دنينير وابن عدلان:

الكندي			ابن دنينير			ابن عدلان		
الحرف	دورانه	النسبة المئوية	الحرف	دورانه	النسبة المئوية	الحرف	دورانه	النسبة المئوية
الألف	600	16.63	الألف	575	16.76	الألف	600	16.54
اللام	437	12.11	اللام	360	10.50	اللام	400	11.02
الميم	320	8.87	الميم	265	7.73	الميم	320	8.82
الهاء	273	7.57	الهاء	260	7.58	الهاء	270	7.44
الواو	262	7.26	الواو	250	7.29	الواو	260	7.17
الياء	252	6.98	الياء	230	6.71	الياء	250	6.89
النون	221	6.13	النون	225	6.56	النون	220	6.07
الراء	155	4.30	الراء	195	5.69	الراء	155	4.27
العين	131	3.63	العين	170	4.96	العين	138	3.80
الفاء	122	3.38	الفاء	145	4.23	الفاء	122	3.36
التاء	120	3.33	التاء	115	3.35	التاء	118	3.25
الباء	112	3.10	الباء	105	3.06	الباء	112	3.09
الكاف	112	3.10	الكاف	095	2.77	الكاف	112	3.09
الدال	092	2.55	الدال	080	2.33	الدال	092	2.54
السين	091	2.52	السين	075	2.19	السين	086	2.37
القاف	063	1.75	القاف	062	1.81	القاف	063	1.74
الحاء	057	1.58	الحاء	050	1.46	الحاء	057	1.57
الجيم	046	1.27	الجيم	043	1.25	الجيم	046	1.27
الذال	035	0.97	الذال	032	0.93	الذال	035	0.96
الصاد	032	0.89	الصاد	028	0.82	الصاد	032	0.88
الخاء	020	0.55	الشين	017	0.50	الشين	028	0.77
الثاء	017	0.47	الخاء	013	0.38	الضاد	023	0.63
الطاء	015	0.41	الثاء	011	0.32	الخاء	020	0.55
الغين	015	0.41	الزاي	009	0.26	الثاء	017	0.47
الظاء	008	0.22	الطاء	008	0.23	الزاي	016	0.44
الزاي	000	000	الظاء	007	0.20	الطاء	015	0.41
الشين	000	000	الغين	005	0.15	الغين	012	0.33
الضاد	000	000	الضاد	000	000	الظاء	008	0.22
المجموع	3608	%100	**المجموع**	3430	%100	**المجموع**	3627	%100

ويبيّن الجدول الآتي مراتب الحروف في إحصاءات أعلام التعمية:

مراتب الحروف	الكنديّ ابن عدلان ابن دُنَينير	ابن وهب الكاتب	الجرهمي	صاحب المقالتين	ابن الدُّرَيْهِم
1	ا	ا	ا	ا	ا
2	ل	ل	ل	ل	ل
3	م	م	م	م	م
4	ه	ي	ن	ي	ي
5	و	و	ه	ن	و
6	ي	ه	و	و	ن
7	ن	ن	ي	ه	ه
8	ر	ر	ب	ر	ر
9	ع	ع	د	ع	س
10	ف	ف	ر	ف	ب
11	ت	ت	ف	ب	ك
12	ب	ب	ق	ت	ت
13	ك	ك	ك	ك	ع
14	د	د	ت	د	ف
15	س	س	ج	س	ق
16	ق	ق	ح	ق	د
17	ح	ح	س	ح	ذ
18	ج	ج	ع	ج	لا
19	ذ	ذ	ص	ص	ح
20	ص	ص	ش	ذ	ج
21	ش	ش	ط	خ	ص
22	ض	ض	ث	ش	خ
23	خ	خ	خ	ث	ش
24	ث	ث	ذ	ز	ض
25	ز	ز	ز	ط	ز
26	ط	ط	ض	غ	ث
27	غ	غ	ظ	ظ	ط
28	ظ	ظ	غ	ض	غ
29					ظ

المبدأ الثاني: استعمال الصفات الكيفية للحروف (Qualitative)

يقوم هذا المبدأ على معرفة أحكام بنية الكلمة (أو نَسْجها)، وما يكون من حروفها أصليًّا أو زائدًا، وما يقارِن غيرَه من الحروف وما لا يقارنه تقديمًا وتأخيرًا (أي: ما يأتلف وما لا يأتلف)، وما يَكثُرُ دورانُه من الثنائيات (أو أزواج الحروف) Digrams والثلاثيات Trigrams، وما يكثر دورانه في أوائل الكلمات (كالواو، وأل التعريف، والباء...)، وفي أواخرها (كالألف، والهاء، والنون...) وغيرِها.

يبيّن الجدول الآتي ما لا يأتلف من الحروف عند الكندي:

الحرف	الرمز	مالا يأتلف معه						الثنائيات – عديمة الائتلاف					
س	⟷	ث	ذ	ص	ض	ظ		س ث	س ذ	س ص	س ض	س ظ	
								ث س	ذ س	ص س	ض س	ظ س	
ث	⟷	ذ	ز	ص	ض	ظ	س	ث ذ	ث ز	ث ص	ث ض	ث ظ	ث س
								ذ ث	ز ث	ص ث	ض ث	ظ ث	س ث
ث	⟵	ش						ث ش					
ذ	⟷	ز	ص	ض	ط	ظ	س	ذ ز	ذ ص	ذ ض	ذ ط	ذ ظ	ذ س
								ز ذ	ص ذ	ض ذ	ط ذ	ظ ذ	س ذ
ذ	⟵	ش	غ					ذ ش	ذ غ				
ز	⟷	ص	ظ	س				ز ص	ص ز	ز ط	ظ ز	ز س	س ز
ز	⟵	ش	ض					ز ش	ز ض				
ز	⟶	ط						ط ز					
ص	⟷	ض	ط	ظ				ص ض	ض ص	ص ط	ط ص	ص ظ	ظ ص
ص	⟵	ج	ش					ص ج	ص ش				
ص	⟶	د						د ص					
ض	⟷	ط	ظ	ش				ض ط	ط ض	ض ظ	ظ ض	ض ش	ش ض
ض	⟵	ق						ض ق					
ض	⟶	د						د ض					
ظ	⟷	ط	ج	د				ظ ط	ط ظ	ظ ج	ج ظ	ظ د	د ظ
ظ	⟵	ح	ق	ش	خ			ظ ح	ظ ق	ظ ش	ظ خ		
ج	⟷	ط	غ	ق				ج ط	ج غ	ج ق			
								ط ج	غ ج	ق ج			
ح	⟷	خ	ع	غ				ح خ	خ ح	ح ع	ع ح	ح غ	غ ح
خ	⟷	غ						خ غ	غ خ				
خ	⟶	ع						ع خ					
د	⟵	ز	ط					د ز	د ط				
ش	⟶	س						س ش					
ع	⟷	غ						ع غ	غ ع				
غ	⟶	ق						ق غ					

⟷ مالا يأتلف بالتقديم والتأخير

⟶ مالا يأتلف بالتقديم

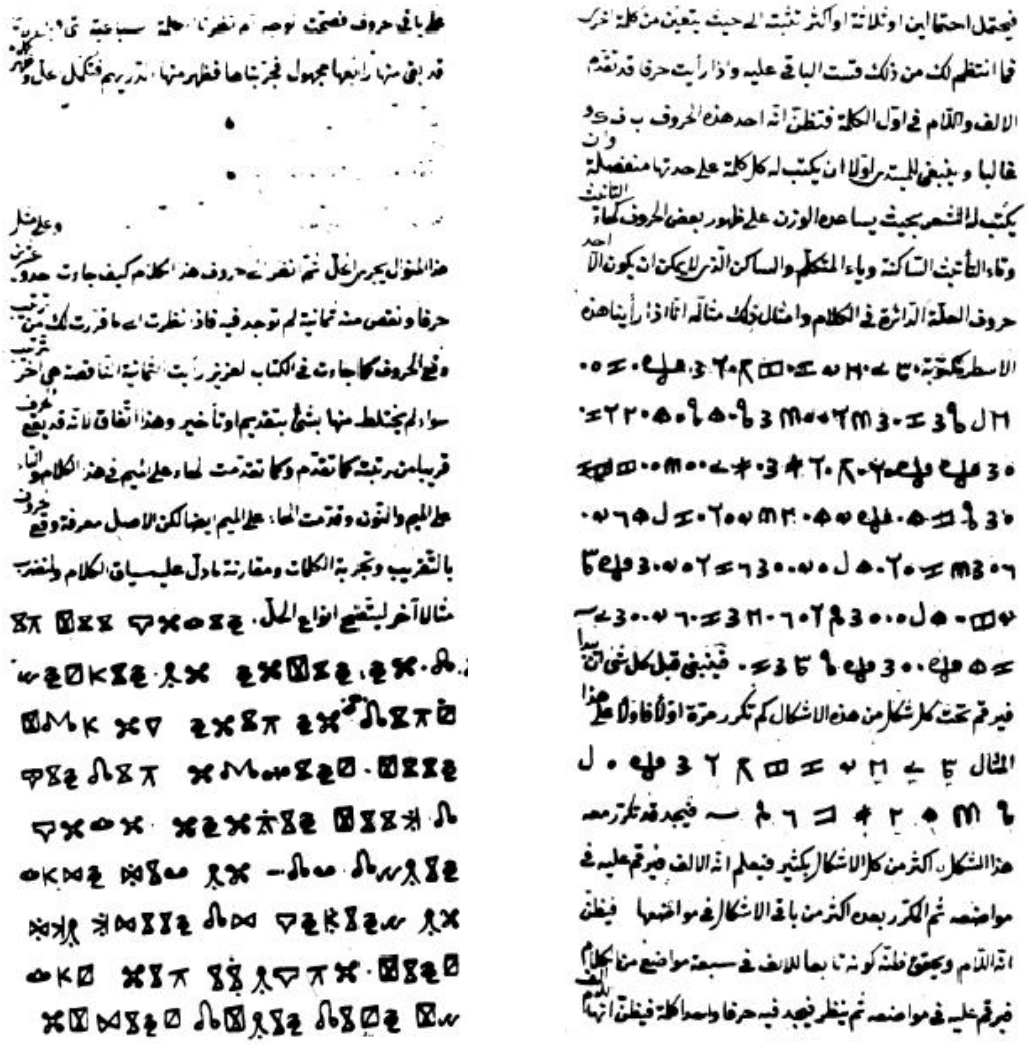
⟵ مالا يأتلف بالتأخير

المبدأ الثالث: استعمال الكلمة المحتملة (Probable Word)

يقوم هذا المبدأ على الاستفادة من معرفة الكلمات التي يُحتمَل وجودها في النص، ومن ذلك فواتحُ الرسائل وخواتِمُها. ويُعدّ الكنديُّ أوّلَ مَن نبَّه على هذه الفواتح، ليُستعانَ بها على استخراج جميع حروف النص، ثم جاء ابنُ عدلان فأكّد أهميتها، وشَرَحَ المقصودَ منها. على أن هذا المبدأ لم يعرفْه الغربيون حتى القرنِ السادسَ عشرَ عندما وضع بورتا (Porta) رسالته في التعمية.

وتجدر الإشارةُ إلى أن استخراج المعمّى المنظوم (الشعر) يقوم على ما سلف من المبادئ، إضافة إلى مبادئَ أخرى تتصل بمعرفة القوافي والعَروض والرَّوِيّ والتشاطير، وعددِ حروف البيت، والحروفِ الصامتة (الخرس) وما يليها من مصوتات (الحركات وحروف المدّ).

وفيما يلي مصوَّرة صفحتَيْن من رسالة ابن الدريهم يشرح فيهما كيفية استخراج المعمَّى لمثالين:



سابعًا: نماذج من مصطلحات علم التعمية

التعمية Cryptography: فنُّ إخفاء معاني الكلام، وهو تحويل نصٍّ واضحٍ (Plaintext) إلى نصٍّ معمًّى غيرِ مفهومٍ (Ciphertext أو Cryptogram)، وذلك باستعمال طريقةٍ محدَّدة، يستطيع مَن يعرفُها أن يفكَّ التعميةَ ويَفهمَ النصَّ الأصليّ. وقد درج في أيامنا هذه استعمالُ كلمة (التشفير) بدلاً من (التعمية). و(التشفير) كلمةٌ وافدةٌ من Cipher التي جاءت بدورها من كلمةٍ عربية النِّجار هي (الصفر) حسبما أشارت إليه كثير من المراجع. ذلك أن العرب حين أدخلوا مفهوم الصفر في الحساب، وطوّروا استعمالَه، لم يكن معروفًا في العالم الغربي، فبدا هذا المفهوم غايةً في الإبهام والتعمية، وصار مثلاً يُطلق على كلّ شيء مبهم.

هذا وقد سَمَّى العلماءُ العربُ مصطلحَ التعمية بأسماءٍ متعددة، وبعضُهم أطلق عليه أكثرَ من تسمية واحدة؛ فقد سمّاه الكندي: (تعمية الحروف)، وسمّاه الفراهيدي والسجستاني وابن كَيْسان وابن طباطبا وابن دنينير: (المعمّى)، وسمّاه ابن طباطبا وابن عدلان: (المترجَم)، وسمّاه ابن وهَب الكاتب وابن دنينير وابن الدريهم والقلقشندي: (الترجمة)، وسمّاه ابن وهب الكاتب: (الكتابة الباطنة).

استخراج المعمّى Cryptanalysis: (أو ما يعرف في أيامنا بكسر الشفرة)، هو عملية تحويل نصٍّ معمّى إلى نصٍّ واضح يقوم بها مُسْتَرِقٌ eavesdropper لا يَعرف طريقةَ التعمية المستعمَلة. ولهذا المصطلح كسابقه تسمياتٌ متعددة؛ فقد سمّاه الكندي وابنُ إسحاق التنوخي وابن طباطبا ومحمد بن سعيد الموصلي وابن وهب الكاتب وابن دنينير: (استخراج المعمّى)، وسمّاه الكندي وابن زيدون وأحمد الشنتمري: (فكّ المعمّى)، وسمّاه غيرُهم: (استنباط الحروف المعمّاة)، و(استنباط المعمّى)، و(استخراج الكلام)، و(استخراج الكَلِم)، و(حلّ الترجمة)، و(حل التراجم)، و(حل المترجَم)، و(حلّ المعمّى)، و(حلّ التعمية)، و(حلّ المبهَم)، و(كشف المعمّى)، و(كشف التراجم)، و(إخراج المكتوبات)...إلخ

حروف التعمية Cipher alphabet: وهي الأشكال المعتمَدة في النصّ المعمّى، وهذه الأشكال يمكن أن تكون أشكالاً ليست منسوبةً إلى شيء من الحروف، كما سمّاها الكندي. ويمكن أن تكون أشكالَ الحروف نفسها، أو تكونَ كلماتِ جنسٍ أو نوع. ويمكن أن تكون حروفًا من كلمات، أو تكونَ أرقامًا على نحو ما ذكره ابن الدريهم.

طريقة التعمية Cipher method: هي الخوارزمية أو العمليات المتتابعة التي تطبَّق على النص الواضح لتحويله إلى نصٍّ معمّى. وثمة نوعان أساسيان للتعمية هما: التعمية بالقلب، والتعمية بالإبدال.

التعمية بالقلب أو البعثرة Transposition: تقوم على تغيير مواقع حروف النص الواضح وفق قاعدة معينة. سمّاها ابن وهب الكاتب: (تغيير مراتب الحروف)، وسمّاها ابن الدريهم: (باب المقلوب)، أما الكندي فقد سمّاها: (لا بتغيير حِليَةِ الشكل وبتغيير الوضع).

التعمية بالإعاضة Substitution: وأبسط طرائقها أن يُستبدل بكل حرفٍ شكلٌ أو رمز وفق قاعدة محدَّدة، كأن يُستبدل بكلّ حرفٍ الحرفُ الذي يليه على حسب ترتيب حروف (أبجد هوز)، أو باستعمال حساب الجمّل...إلخ. ويمكن أن يُستبدل بأحد الحروف أكثرُ من حرف واحد، وهو ما يقابل Homophones. وقد سمّاها ابن وهب الكاتب: (التبديل)، وسمّاها ابن الدريهم: (الإبدال).

الأغفال nulls: مفردُها غُفْل، وهي أشكالٌ زائدة لا معنى لها تُقْحَم في الحروف المعمّاة طلبًا للمبالغة في التعمية، فيصبح استخراجها عسيرًا. وهذا المصطلح مما وضعه الكندي.

الفاصل أو الفصل space أو word-spacer: هو الشكل أو الرمز الذي يمثل الفراغ الفاصل بين كلمتين.

المفتاح key: هو مصطلحٌ بين المتخاطبَيْن بالتعمية، يتألف من حرف أو مجموعة حروفٍ أو أرقام أو بيت من الشعر... يسمح للمخاطَب بقراءة الرسالة المعمّاة دونما صعوبة. وقد سمّاه الكندي وابن دنينير: (الرباط والشرح) و(النظام)، وسمّاه ابن عدلان: (الضوابط). في حين أطلق عليه ابن الدريهم اسم: (الاصطلاح) و (الالتزام)، إضافة إلى (الرباط والشرح).

المُدْمَج no-word-spacer: هو نصٌّ معمّى بدون فواصل. واستخراجُه أصعب من استخراج النص ذي الفواصل.

الكلمة المحتمَلة probable word: إحدى طرائق استخراج المعمّى عن طريق استنباط الفواتح التقليدية الممكنة للرسائل وعبارات التمجيد الخاصة باللغة المستعمَلة في التعمية، كالسلام والبسملة والتحية ... وغيرها.

تواتر الحروف letter frequency أو frequency count: تردّد ورود كلّ حرف من حروف اللغة في نصٍّ ما. وهو من الأساليب الكمّية المستعملة في استخراج المعمّى.

تواترُ تقارن الحروف contact count: تردّد ورود كلّ زوجٍ من أزواج الحروف في نصٍّ ما. ويمكن أن يؤخذ ذلك بالنسبة إلى حرفٍ ما، فيُنظر إلى اقترانه بالتقديم أو اقترانه بالتأخير، كما يقول الكندي. وسمّاه غيره (ائتلاف الحروف وتنافرها). وهو من الأساليب الكيفية المستعملة في استخراج المعمّى.

المراجع

- **علم التعمية واستخراج المعمى عند العرب**، الجزء الأول، د. محمد مرياتي، د. يحيى مير علم، د. محمد حسان الطيان، مطبوعات مجمع اللغة العربية بدمشق، 1987.
- **علم التعمية واستخراج المعمى عند العرب**، الجزء الثاني، د. محمد مرياتي، د. يحيى مير علم، د. محمد حسان الطيان، مطبوعات مجمع اللغة العربية بدمشق، 1997.
- **من المكتبة العربية: علم التعمية واستخراج المعمى عند العرب**، عرض الدكتور محمد مكي الحسني الجزائري، مجلة مجمع اللغة العربية بدمشق، المجلد 83، الجزء 1، كانون الثاني 2008.
- **تاريخ مشرق لعلمٍ خفي، مراجعة كتاب «مستخرجو المُعمّى The Codebreakers»**، DAVID KAHN، مجلة العلوم، مؤسسة الكويت للتقدم العلمي، المجلد 15، 1999.
- **التعمية التطبيقية Applied Cryptography**، تأليف Bruce Schneier، ترجمة د. حاتم النجدي، د. أميمة الدكاك، مطبوعات الجمعية العلمية السورية للمعلوماتية، 2006.
- **إسهامات علماء التعمية في اللسانيات العربية**، د. يحيى مير علم، مجلة مجمع اللغة العربية بدمشق، المجلد 79، الجزء الثالث، ص 521–546.
- **إسهامات علماء التعمية في اللسانيات العربية**، على هامش الاحتفال بإصدار سلسلة الترجمة الإنكليزية لكتاب ((علم التعمية واستخراج المعمّى عند العرب)) وتكريم المؤلِّفين في مركز الملك فيصل للبحوث والدراسات الإسلامية بالرياض. جرى تقديم البحث في ندوة علمية متخصّصة في علم التعمية عقب حفل تدشين إصدار سلسلة ترجمة كتب علم التعمية عند العرب والمسلمين، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض 2003/10/19.
- **اكتشاف مخطوطات التعمية والجهود المبذولة فيها**، د. محمد حسان الطيان، أُلقي هذا المقال في حفل إصدار الجزء الأول من سلسلة كتب التعمية عند العرب بمدينة الملك عبد العزيز للعلوم والتقنية، الرياض، 17-19 تشرين الأول 2003. ثم نُشر في كتاب **تحت راية العربية**، د. محمد حسان الطيان، دار الثقافة والنشر، 2008.
- **التعمية واستخراج المعمى**، محمد مرياتي ومحمد وليد الجلاد، الموسوعة العربية، المجلد السادس، ط1، 2002.
- **علم التعمية واستخراج المعمى عند العرب**، د. موفق دعبول، د. محمد مرياتي، أ. مروان البواب، فعاليات الملتقى التونسي السوري، 23-24 نيسان، 2007.
- **نحو معجم لمصطلحات علم التعمية**، د. محمد مرياتي، د. يحيى مير علم، د. محمد حسان الطيان، أ. سعيد الأسعد، أ. مروان البواب، المؤتمر الثالث لمجمع اللغة العربية بدمشق، 2004.

- **ابن وحشية النبطي وريادته في كشف رموز هيروغليفية في كتابه: شَوْق المُسْتَهام في معرفة رموز الأقلام**، د. يحيى مير علم، مجلة مجمع اللغة العربية بدمشق، المجلد 79، الجزء الرابع، ص 735-764.

- **العلوم عند العرب**، قدري حافظ طوقان، مكتبة مصر، 1956.

- *Series on Arabic Origins of Cryptology*, Volume 1-6, M. Mrayati, Y. Meer Alam, M. H. Tayyan, Translated by S. al-Asaad, Puplished by KFCRIS & KACST, 2003-2007.

- *Kahn on Codes: Secrets of the New Cryptology,* David Kahn, Macmillan Publishung Comapny, New York, 1984.

- *THE CODEBREAKERS,* David Kahn, Macmillan Publishung Comapny, New York, 1976.