مجمع اللغة العربية بدمشق
المؤتمر الثالث: قضايا المصطلح العلمي
2004/10/12-10

نحو معجم لمصطلحات علم التعمية

د. محمد مراياتي د. يحيى مير علم د. محمد حسان الطيان أ. سعيد الأسعد أ. مروان البواب

ملخص البحث:

علم التعمية (أو الشِّفرة) – بشقَّيْه: التعمية واستخراج المعمّى (أو التشفير وكسر الشِّفرة) – أحدُ العلوم المهمّة في عصر الحاسوب وثورة المعلومات والاتصالات؛ فهو يمارَس في نواحٍ عديدةٍ من الحياة كالإنترنت، والاتصالات المدنية والعسكرية، والتجارة، والأمن... وغيرها.

وكان علماؤنا العرب هم الذين أرسَوْا أسسَ هذا العلم، وصاغوا قواعده، وطوّروه، ومن ثَمَّ فهم الذين وضعوا مصطلحاته، وابتدعوا منهجياته ومبادئه؛ شهد بذلك النَّصَفَة من كتّاب علم التعمية يقدُمُهم كبير مؤرخي هذا العلم ديفيد كَهْن.

ولقد نشأتْ فكرةُ وضْع معجمٍ ثلاثيّ اللغة لمصطلحات علم التعمية نتيجة تحقيقنا مخطوطات عديدةً يعود أقدمُها إلى فيلسوف العرب يعقوب الكِندي (260 هـ). ومن هذه المخطوطات: مخطوطٌ للحسن بنِ طباطبا (322 هـ)، ولابنِ دنينير (627)، وابن عدلان (666 هـ)، وابن الدريهم (726 هـ)، والجُرْهُمِيّ... وتألَّفتْ نواة هذا المعجم من مجموع المصطلحات العلمية التي تضمنها الجزءان الأول والثاني من كتابنا ((علم التعمية واستخراج المعمّى عند العرب))، ومن ترجمتهما الإنكليزية التي صدر منها ثلاثة أجزاء من أصل تسعة.

يعتمد هذا المقال في حديثه عن علم التعمية على المصطلحات التي استعملتْها المدرسةُ العربية في علم التعمية، التي استمر عطاؤها العلمي أكثر من ستة قرون. يبدأ المقال بتعريف علم التعمية، وبيانِ أهميته في حياتنا المعاصرة، وأسبقيةِ العرب وريادتِهم فيه، ثم يعرض بإيجاز أهمَّ مخطوطات هذا العلم، معرِّفاً بأصحابها، ومبيِّناً ما اشتملت عليه من طرائق التعمية ومبادئ استخراج المعمّى. ثم يتحدث عن معجم مصطلحات علم التعمية، ويعرض نماذجَ مختارةً من هذه المصطلحات مقرونةً بمقابلاتها الأجنبية، يتبيّن لنا من تحليلها دقةُ هذه المصطلحات وغناها، وبراعةُ واضعيها.

أولاً: التعريف بعلم التعمية:

يقوم علم التعمية Cryptology (أو الشِّفرة) على ركيزتين أساسيتين؛ هما التعمية (أو التشفير)، واستخراج المعمّى (أو كسر الشيفرة).

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

وأما استخراج المعمّى (Cryptanalysis) فهو تحويل النصّ المعمّى إلى النصّ الواضح لِمَن لا يعرف طريقة التعمية المستعمَلة. فإذا ما عُلِمَتْ طريقةُ التعمية، فيسمّى تحويلُ النصّ المعمّى إلى النصّ الواضح بفكّ المعمّى Decipherment (أو فكّ الشيفرة).

ثانياً: أهمية علم التعمية:

تنبع أهمية علم التعمية من تطبيقاته الحيوية في النواحي المختلفة من حياتنا المعاصرة، ومن صلة هذا العلم بالعلوم الأخرى.

أما ما يتعلّق بتطبيقات هذا العلم، فليست محصورةً كما كان يُظَنّ بالعمليات الحربية والمؤسسات العسكرية، بل تتعدّى هذا النطاق إلى مجالاتٍ كثيرةٍ نذكر منها:

النظم الحاسوبية (Computer Systems Security): غدتْ حماية المعلومات المهمة والحساسة – سواءٌ المخزَّنةُ منها أو المتبادَلة عبر الشبكات – ضرورةً ملحَّة لمنع الوصول إليها ومعرفةِ مضمونها أو العبثِ بها أو تخريبها. وتصنَّف الأساليبُ المستخدَمة لتحقيق ذلك صنفين أساسيين هما: التعمية بالمفتاح الخصوصي Private Key Encryption، والتعمية بالمفتاح العمومي Public Key Encryption.

الإنترنت (Internet Security): إذا كانت الإنترنت مخزنَ العجائب، فإنها في الوقت نفسه أرضُ المخاطر الخفية. وقد بدأ الاهتمام جديّاً بمسألة أمن الإنترنت في عام 1988، وذلك بعد أن قام أحد طلاب جامعة كورنيل بنيويورك بإطلاق برنامجٍ خبيث أدّى إلى توقّف معظم المراسلات عبر الإنترنت لعدة أيام. وبالنظر إلى الخدمات الجُلّى التي توفِّرها الإنترنت كالتجارة الإلكترونية (E-Commerce)، والبريد الإلكتروني (E-mail)، وتبادل الملفات FTP (File Transfer Protocol)، والولوج إلى حاسوب آخر عن بعد (Telenet)، والمحادثة الفورية (Electronic Chat)، والبحث عن المعلومات (Searching)، والاتصالات الهاتفية عبر الإنترنت (Internet Phone)، والمؤتمرات المرئية (Video Conference)، والإعلانات الإلكترونية BBS (Bulletin Board Service)، وشبكة الأخبار (Network News) ... وغيرها، وبالنظر إلى وجود ثغرات أمنية مختلفة في شبكة الإنترنت، فقد وضع الخبراء عدداً من الحلول للتغلب على هذه الثغرات، حفاظاً على سرية المعلومات، وحمايتها من عبث

العابثين واحتيال المتطفلين. وتؤدي التعميةُ دوراً مهماً في الكثير من هذه الحلول.

قنوات البث الفضائية: تَعْمِد هذه القنواتُ إلى تعمية بعض برامجها التلفزيونية المبثوثةِ كيلا يشاهدها إلا المشتركون الذين يدفعون اشتراكاتٍ مقابل المفتاح الذي يَسمح لهم بفكّ التعمية ومشاهدة هذه البرامج المعمّاة.

المصارف: إن الحسابات المصرفية وتحويلاتِها واتصالاتِها والتحكمَ في عملياتها من بُعد، أظهر الحاجةَ الماسّة إلى تعميتها خوفاً من العمليات غير المشروعة في الحصول عليها.

الكشف عن اللغات القديمة البائدة: كان لطرائق استخراج المعمّى أكبرُ الأثر في كشف رموز اللغات الهيروغليفية في مطلع القرن الثامن عشر، ولا تزال تُستخدم في الكشف عن اللغات المسمارية كالحثيّة والفارسية والكلدانية.

وأما ما يتعلق بصلة علم التعمية بغيره من العلوم، فحسبنا أن نشير إلى صلته الوثيقة بعلوم اللغة العربية صوتاً وإحصاءً ونحواً وصرفاً ودلالةً وعَرُوضاً، وإلى صلته بعلوم الرياضيات، والإدارة، إضافة إلى صلته بحركة الترجمة.

ثالثاً: ريادةُ العرب وأسبقيتُهم في علم التعمية:

علم التعمية واحدٌ من علوم كثيرة تدين للعرب ولادةً ونشأةً وتطوّراً، وهو ليس كغيره من العلوم التي تَرجم العربُ بعضَ أصولها، ثم أغنَوْها وطوّروها كالرياضيات والفيزياء والفلسفة، وإنما هو علمٌ عربيُّ المولد، يعود الفضلُ إلى العرب في ابتكاره، ووضْع أسسه ومصطلحاته، وإرساء قواعده ومنهجياته، وتطويره إلى أن بلغ مرحلةً ناضجة. وغدا ما وضعوه فيه مرجعاً قَبَسَ منه المشتغلون بالتعمية من بَعْدُ. فالعرب أوّلُ من كتب في طرائق التعمية الرئيسية التي ما انفكّ العالَم يَستخدم بعضَها حتى يومنا هذا، وهم أوّلُ مَن وضع المنهجياتِ الأساسيةَ في استخراج المعمّى، ودوّنوا فيهما مصنفاتٍ مستقلةً على غاية من الأهمية منذ القرن الثالث الهجري، فسبقوا بذلك الغربيين نحواً من سبعة قرون.

ولقد اطَّلع ديفيد كَهْن الذي يُعدّ كبيرَ مؤرخي علم التعمية على بعض ما كتبه العرب في هذا العلم، فكتب يقول في الصفحة 284 من كتابه *Kahn on Codes*: ((لقد طوّر المسلمون معرفةً نظريةً في استخراج المعمّى تنِمّ عن ممارستهم العملية لاعتراض المراسلات واستخراج تعميتها، وذلك على الرغم من تشكيك بعض الباحثين في ذلك))، وقال في الصفحة 21 من الكتاب نفسِه: ((اطّلعتُ على مقالٍ نُشر في مجلة الدراسات الساميّة... بيّن المقال أن العربَ مارسوا استخراج المعمّى قبل الغرب بزمن طويل. ووفّر لي المقال ما أعُدُّه أكبرَ فتح تاريخي في كتابي كله))، ثم قال في الصفحة 41 من الكتاب نفسِه: ((كانت طريقةُ التعمية التي استعملها قيصر كافيةً لعصره، لأن أوائلَ مستخرجي التعمية لم يَظهروا إلا بعد عدة قرون منه. فالعرب هم الذين اكتشفوا مبادئ استخراج المعمّى، إلا أن معرفتهم تقلّصت مع أُفول

حضارتهم، ولم يَكتشف الغربُ استخراجَ المعمّى من جديد إلا في عصر النهضة)). وكتب يقول في الصفحة 93 من كتابه *The Codebreakers*: ((وُلِدَ علم التعمية بشِقَّيْه بين العرب، فقد كانوا أوّلَ من اكتشفَ طرق استخراج المعمّى ودوَّنَها)).

هذا ويمكن أن نوجز السَّبْقَ الذي حقّقه علماؤنا العربُ في هذا العلم بالنقاط الآتية:

1- الكندي هو 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 هو أوّل مَن فرّق بوضوح بين طريقتَي التعمية الأساسيتَين: الإبدال والقلب، أي قبل بورتا (Porta) بنحو سبعة قرون.

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

4- ابنُ عدلان هو أوّل مَن استخدم النصوص بدون فاصل، وأسماها المدمَج، وذلك قبل بورتا بثلاثة قرون.

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

6- ابن الدريهم هو الذي عرض طريقة التعمية باستعمال شبكة بسيطة، وذلك قبل كاردانو (Cardano) بقرنين أيضاً.

رابعاً: التعريف بأهم مخطوطات علم التعمية وأصحابها:

اشتمل الجزء الأول من كتابنا ((علم التعمية واستخراج المعمى)) على ثلاث رسائل مخطوطة في هذا العلم، واشتمل الجزء الثاني على ثماني رسائلَ مخطوطة. فبلغ مجموعها إحدى عشْرَةَ رسالة. وما زال العمل جارياً في تحقيق رسائلَ أخرى. وطلباً للاختصار سنوجز القول في أربعِ رسائلَ هي:

1- رسالة الكندي في استخراج المعمّى:

المؤلّف: فيلسوف العرب يعقوب بن إسحاق الكندي، عدّه كاردانو واحداً من أعظم الحكماء في تاريخ الإنسانية. ولد بالكوفة، وكان أبوه أميراً عليها في عهد الخليفة العباسي المهديّ، ونشأ بالبصرة، ثم انتقل إلى بغداد حيث حصّل جلَّ علومِه، فبرع بالطبّ والفلسفة والحساب والهندسة والفلك وغيرها. وقد أصاب منْزلةً عظيمة لدى خلفاء بني العباس، وتولّى بيتَ الحكمة. توفي سنة 260 هـ/873 م. خلّف ثروة فكرية هائلة في علوم شتى كالفلسفة والرياضيات والطب والسياسة والجغرافية والموسيقى والشعر واللغة والكيمياء والزراعة والحيوان، بلغتْ مئتين وتسعين مصنفاً.

الرسالة: رسالة الكندي هي أقدمُ ما وقع بين أيدينا من آثارٍ في التعمية واستخراج المعمّى، إذ يعود تأليفُها إلى القرن الثالث الهجري. وقد استكملتِ الرسالةُ أسبابَ التأليف العلميّ المنهجيّ في هذا الفنّ عمقاً وشمولاً، فأبرزتْه عِلماً قائماً بذاته، له أصولُه وطرائقُه المختلفة. ويمكن 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.

2- مقاصد الفصول المترجِمة عن حلّ الترجمة:

المؤلِّف: إبراهيم بن محمد بن إبراهيم المعروف بابن دنينير. ولد بالمَوْصل سنة 583 هـ/1187م، ونشأ فيها ونُسب إليها. برع ابنُ دنينير بالتعمية إضافةً إلى الشعر، ففي الشعر له كتابان؛ الأول: ديوانُه الشعري، والثاني: ((الكافي في علم القوافي)). وله في التعمية كتابان حسبما ذكر الصفدي أولهما: ((كتاب الشهاب الناجم عن علم وضع التراجم))، وثانيهما الرسالة التي أشرنا إليها آنفاً. توفي ابن دنينير في بانياس سنة 627 هـ/1229 م.

الرسالة: اعتمد ابن دنينير في رسالته هذه على الكندي اعتماداً كبيراً؛ فهو تارةً يشرح ما أوجزه الكندي، وأخرى يوجز ما بسط القول 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 معاً. وكان الموضوع الذي استغرق شطراً 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. أخذ النحوَ عن جماعةٍ يَقْدُمُهم أبو البقاء العكبري. كان أعجوبةً في الذكاء، رأساً في الأدب، شاعراً مُجيداً، حتى إن بعضهم عدّه من أذكياء بني آدم. وَضَعَ في علم التعمية ثلاثةَ كتبٍ هي: ((عقلة المجتاز في حلّ الألغاز))، و((المِعْلَم))، و((المؤلَّف للملك الأشرف)). ووضع كتاباً 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 المتشعبة، بل عرض فيها عشرين قاعدة في استخراج المعمّى، سبقتْها فاتحة، ولَحِقتْها 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 في سنة 712 هـ/1312 م بالموصل، ونشأ فيها. دَرَسَ على كثير من علماء عصره، وتنقّل تاجراً بين دمشق والقاهرة غيرما مرة. توفي سنة 762 هـ/1361 م. برع ابنُ الدريهم في كثير من العلوم، لكن شهرتَهُ ومهارته كانت في التعمية والأحاجي والألغاز وحلِّ المترجَم وخواصِّ الحروف ... وصنَّف في هذه العلوم كثيراً من الكتب والرسائل؛ منها: ((إيضاح المبهم في حلّ المترجَم))، و((غاية الإعجاز في الأحاجي والألغاز))، و((قصيدة في حلّ رموز الأقلام المكتوبة على البرابي))، و((مفتاح الكنوز في إيضاح المرموز)).

الرسالة: تعدّ هذه الرسالةُ أوسعَ ما عثرنا عليه من مخطوطات وأكثرَها تفصيلاً في هذا العلم، 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، ومنهجية حلّ الترجمة، ومقدمةٌ صرفية، وما لا بدّ منه لِمَن يعاني حلّ الترجمة، وختمها بمثالَيْن عمليَّيْن في حلّ الترجمة.

خامساً: طرائق التعمية:

سنوجز فيما يلي الكلامَ على أهم هذه الطرائق:

1- **التعمية بالقلب أو البعثرة** (Transposition):

وتكون بتغيير مواقع حروف النص الواضح وفق قاعدة معينة. وهناك أساليبُ كثيرةٌ تتفرع عن هذه الطريقة، نكتفي بذكر مثال واحدٍ بسيط منها:

النص الواضح: مجمع دمشق يرحب بضيوفه

النص المعمّى: جمعم مدقش ريبح ضبويهف

القاعدة: قلب (تغيير) موقعَيْ كلِّ حرفين من حروف النص الواضح؛ أي إن الحرفَ الأوّلَ يَحِلُّ محلَّ الثاني، والثاني محلَّ الأول، والثالثُ يحل محل الرابع، والرابع محل الثالث، وهكذا حتى ينتهي النص.

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

وتقوم على تبديل حروف النص الواضح، ووضع حروف أو رموز أخرى مكانها، ولهذه الطريقة كسابقتها أساليبُ كثيرةٌ تتفرع عنها، نكتفي بذكر مثال واحدٍ منها:

النص الواضح: مجمع دمشق يرحب بضيوفه

النص المعمّى: نحنع ذنصك ازخت تطايقو

القاعدة: إبدال كل حرف من الرسالة بالذي يليه في ترتيب حروف المعجم؛ أي نضع حرف الباء بدلاً من حرف الألف، والتاء بدلاً من الباء، والثاء بدلاً من التاء،... وهكذا.

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، نكتفي بذكر مثال واحدٍ منها:

النص الواضح: مجمع دمشق يرحب بضيوفه

النص المعمّى: ملجملع دملشق يرحبن بنضيوفه

القاعدة: زيادة حرف اللام بعد كل ميم، وحرف النون بعد كل باء.

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.

سادساً: مبادئ استخراج المعمّى:

وقفنا بعد تحقيقنا لمخطوطات عديدةٍ في استخراج المعمّى أنه 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 عموماً 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).

يبيّن الجدول الآتي دورانَ الحروف ونسبَها المئوية مرتبةً تنازلياً 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

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

المبدأ الثاني: استعمال الصفات الكيفية للحروف (Qualitative):

يقوم هذا المبدأ على معرفة أحكام بنية الكلمة (أو نَسْجها)، وما يكون من حروفها أصلياً أو زائداً، وما يقارِن غيرَه من الحروف وما لا يقارنه تقديماً وتأخيراً (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).

سابعاً: تعريف بمعجم مصطلحات علم التعمية:

هذا المعجم هو معجم لمصطلحات علم التعمية ثلاثيُّ اللغة (العربية والإنكليزية والفرنسية)، يتضمن في المقام الأول المصطلحاتِ العلميةَ التي وردتْ في الجزء الأول والثاني من كتابنا ((علم التعمية واستخراج المعمّى عند العرب))، ومن ترجمتهما الإنكليزية التي صدر منها ثلاثةُ أجزاءٍ من أصل تسعة. والعملُ جارٍ على إضافة ما يَستجدّ من مصطلحاتٍ تتحصّل لدينا نتيجة تحقيق الأجزاءِ التاليةِ من كتابنا المشار إليه.

لكلِّ مصطلح من مصطلحات المعجم عددٌ من الحقول؛ تتضمن: المصطلحَ العربي، وتعريفَه، وواضعَه، وتسمياتِهِ الأخرى، والكتبَ التي أوردتْه، وما يقابله في الإنكليزية والفرنسية، مع إيراد تعريفه بالإنكليزية.

ثامناً: نماذج مختارة من معجم 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 معروفاً في العالم الغربي، فبدا هذا المفهوم غايةً في الإبهام والتعمية، وصار مثلاً يُطلق على كلّ شيء مبهم.

هذا وقد سمّى 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 حروفاً من كلمات، أو تكونَ أرقاماً 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 طلباً للمبالغة في التعمية، فيصبح استخراجها عسيراً. 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.

تاسعاً: الخاتمة:

نأمُل أن يضيف معجم مصطلحات علم التعمية إلى مكتبتنا العربية معجماً مهماً ينضمّ إلى المعاجم العربية المتخصصة، يسدُّ حاجة المعنيين في واحد من الاختصاصات العلمية الحيّة التي تتنامى أهميتها في نواح عديدة من نشاطات حياتنا المعاصرة.

ولا بدّ في نهاية البحث من توجيه وافر الشكر والتقدير إلى كلِّ مَنْ أسهم في نشر المادة العلمية التي كانت أساساً لتحقيق هذا المعجم، يقدمهم الأستاذ الدكتور شاكر الفحام رئيس مجمع اللغة العربية بدمشق، والأستاذ الدكتور عبد الله واثق شهيد المدير العام لمركز الدراسات والبحوث العلمية لإصدارهما كتاب: ((علم التعمية واستخراج المعمّى عند العرب)). والشكر موصول كذلك لكلٍّ من: مركز الملك فيصل للبحوث والدراسات الإسلامية ممثلاً بأمينه العام معالي الأستاذ الدكتور يحيى محمود بن جنيد، ومدينة الملك عبد العزيز للعلوم والتقنية ممثلة برئيسها معالي الأستاذ الدكتور صالح بن عبد الرحمن العذل، لتفضلهما بتمويل ترجمة كتاب "علم التعمية واستخراج المعمّى عند العرب" إلى اللغة الإنكليزية، وطباعته وتوزيعه على المؤسسات العلمية في العالم. والشكر كذلك لنائب رئيس المدينة الأستاذ الدكتور محمد بن إبراهيم السويِّل وللأستاذ الدكتور إبراهيم بن عبد الرحمن القاضي على مشاركتهما في المراجعة العلمية للترجمة المذكورة.