

نظام التشفير العربي علاقة بين الحروف والأرقام أمثلة ونماذج وثائقية مغاربية.

*The Arabic cryptography system is a relationship between
letters and numbers
Examples of sample documents Maghreb history.*

جمال عناق.

جامعة العربي التبسي؛ تبسة (الجزائر).

البريد الإلكتروني: djamel.annak@univ-tebessa.dz

تاريخ الإرسال: 22/03/12؛ تاريخ القبول: 22/05/20؛ تاريخ النشر: 22/06/01

المخلص:

يأتيك أحيانا على جهازك المحمول رسالة كهذه: "بفضل خاصية التشفير التام بين الطرفين، يتم تأمين رسائلك بقفل أمان، ويكون المفتاح اللازم للإطلاع على هذه الرسائل معك أنت ومستلم الرسالة فقط". هذه أحد التبيهات أو الإشارات التي قد نجدها في أجهزتنا الإلكترونية (كالمحمول مثلا) عبر وسائل التواصل الاجتماعي. ستحاول هذه الورقة إعطاء بعض النماذج والاستعمالات التشفيرية الأولى في الوثائق والمخطوطات العربية بوصفها ممارسة خصوصية وشخصية بين المتراسلين.

الكلمات المفتاحية: التعمية؛ التشفير؛ حساب الجمل؛ وثائق؛ أرقام.

Abstract:

Many times on your mobile device, you get a message like this: "because with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have

the special key needed to unlock and read them. All of this happens automatically".

This is one of the alerts or signals that can find me and you on our devices (such as cell phones) through social media. This study will attempt to give the first cryptographic models and uses that were used on Arab and Maghreb documents and manuscripts as a private and personal practice among correspondents .

Key words: Aldjummel; Cryptology ;Maghreb ; numeration-Hissab.

مقدمة:

لا شك أن احتكاك العرب بأمم كثيرة كالفرس والهند والروم، نتيجة للتعاملات التجارية والعلمية، وحاجتهم إلى الحساب قد أخذوا منهم علم الأرقام والتشفير، واستمر العمل بهذا النظام لكن بطريقة مبتكرة إلى عهود قريبة على أقل تقدير إلى غاية القرن التاسع عشر الميلادي، وهو ما تشبهه الكثير من الوثائق والمخطوطات التاريخية بإعتمادها على نظام حساب الجُمَّل، وقيام من يعلمون بهذا الحساب بعمليات التشفير في تعاملاتهم السرية.

يهدف الموضوع إلى العمل على إبراز العلاقة بين الحرف والرقم في نظام الجُمَّل واستعمالاته في الحضارة العربية والمغاربية خاصة؛ بوصفه ضرورة تجارية واقتصادية، واستعملات علم الحساب في عمليات التشفير السرية التي كانت تتم في مختلف المعاملات الخاصة بين المتراسلين من خلال بعض النماذج.

إشكالية الموضوع: يفترض على هذه الدراسة الإجابة عن الأسئلة الآتية: ماهي العلاقة التي بين الأرقام والحروف في التراث العربي؟ وما هو حساب الجُمَّل؟ وما هي الطريقة لحساب الجُمَّل في الوثائق

والنصوص التاريخية المغاربية؟ ما هو نظام التشفير وعلم اخفاء المعلومات المغاربي؟ وكيف يتم استعمال نظام التشفير؟ هذه إذا بعض الأسئلة التي سنحاول الإجابة عنها معولين في ذلك على مجموعة من الأمثلة الأنموذجية.

وسنعمد في هذه الدراسة على المنهج التاريخي والتحليلي، معتمدين في ذلك على بعض النصوص التراثية لتحديد طرق حساب الجُمَل وكيفياته، واستعمال نظام التشفير من خلال بعض النماذج الوثائقية.

أسس نظام التشفير والتعمية:

إن كلمة التشفير كلمة وردت من اللغة اللاتينية *Cipher* التي أخذت من كلمة الصفر العربية الذي أدخل في النظام العددي، (Ibrahim, 2010, p. 102) وهذا ما لم تعرفه الأرقام اللاتينية التي لا وجود للصفر في نظامها الرقمي، فدرج استعمال كلمة التشفير بدلا عن كلمة التعمية التسمية الحقيقية لهذا النظام، والمقصود منها تحويل نص واضح إلى نص غير مفهوم باستعمال طريقة محددة، يستطيع من يعرفها أن يعود ويفهم النص (محمد، 1987، ص: 28)، وقد عرّف التعمية محمد الصغير المراكشي مؤرخ الدولة السعدية بالآتي: وهو: "أن تذكر الاسم وتريد المسمى أو تذكر المسمى وتريد الاسم، وأعلم أنهم لا يشترطون في استخراج التسمية بطريق التعمية حصولها بحركاتها وسكناتها بل اكتفوا بحصول الكلمة من غير ملاحظة لهيئاتها الخاصة فإذا وقع ذلك في الشعر فيكون عندهم من المحسنات ويسمى العمل التذييلي" (الصغير، 1880، ص: 141- 142).

فالتعمية إذا بشرح بسيط تعتمد على استعمال مجموعة من الحروف الأبجدية العربية التي قد تعبر عن أسماء مقصودة لأسماء أشخاص مقصودين لكن بأسلوب خفي (initi, 1894, p. 215) سنحاول إعطاء بعض النماذج عن التعمية، لكن قبل ذلك يجب أن يعلم القارئ أن هذه العملية تركز بالأساس على الحساب بنظام الجُمْل، بتحويل الحروف إلى أرقام معلومة باستعمال حساب أبجد هوز، وللعلم فإن في بلاد المغرب الإسلامي يستعمل أهله نظاما أبجديا مخالفا لما هو موجود في المشرق، فإلى جانب استعمال حساب أبجد هوز يوجد نوع ثالث يستعملونه في تأريخ المنتسختات، وترقيم أوراق المخطوطات، وفي عمليات وثائق المحاكم الشرعية، وصار يعرف بالقلم الفاسي (قاسم، 2001، ص: 214)، ليتطور هذا النظام وليصبح أداة للتشفير بوصفه طريقة بديلة في إخفاء المعلومات في أدبيات المراسلة والترسل.

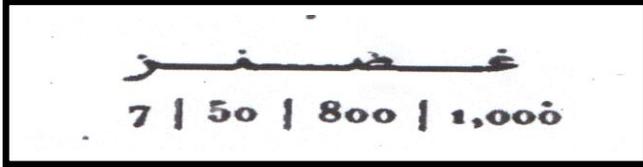
الحساب بنظام الجُمْل:

الحساب لغة: العَدُّ، يقال: عن الشيء؛ حَسَبَهُ حَسَبًا وحُسْبَانًا بالضم، وحُسْبَانًا وحِسَابًا وحِسْبَةً وحِسَابَةً، بكسرهن؛ عَدَهُ والمعدود محسوب (الفيروزآبادي مجد الدين محمد بن يعقوب، 2005، ص: 74). وفي اللسان: حَسِبْتُ الشيء أَحْسَبُهُ حِسَابًا، وحَسَبْتُ الشيء أَحْسَبُهُ حِسْبَانًا وحُسْبَانًا، وحَسَبَ الشيء يَحْسَبُهُ، بالضم، حَسِبًا وحِسَابًا وحِسَابَةً: عَدَهُ، والحُسبان: الحساب وهو العَدُّ والمَعْدُودُ مَحْسُوبٌ (منظور، 1955، ص: 865).

أما إصطلاحا فقليل في تعريفه: ضرب من الحساب يجعل فيه لكل حرف من الحروف الأبجدية عدد من واحد إلى الألف على ترتيب خاص (التميمي، 2011- 12- 01، ص: 16- 17).

سنعطي أمثلة على حساب الجُمَّل لكي تتضح الصورة فمثلا

كلمة غُضُنز نقسمها حسب أرقامها الى:



فتعطينا في المجموع: 1857. مثلا آخر فلو كان اسمك: سيف يوسف وأنت من مواليد 1983، وتريد أن تعرف مجموع أرقام إسمك وتتستر على تاريخ ميلادك فتكون العملية بعد تقطيع حروف الكلمة كالآتي:

س/ي/ف/10/80+ي/10/ و/6/س/60/ف=80 فنجمع

س=60/ي=10/ف=80+ي/10/ و=6/س=60/ف=80 فنجمع الحاصل وهو: 306 هذا بالحساب المشرقي، أما بالحساب المغاربي فالاختلاف هنا هو في الحرف السين الذي مقداره: 300 و60 و240 ونضربها إلى الحساب السابـاق:

وهو: 486=80+60+06+10+80+10+240

أما اذا أراد ان يعطي لتاريخ ميلاده صيغة حرفية فسيكون الآتي: 1000=غ+900=ظ+80=ف+03=ج.

فنجعم الحروف فنتحصل على كلمة: غظفج.(حساب المشرق)
 وأما بالحساب المغاربي فالخلاف في حرف:
 $ش = 1000 + 900 + 80 + ف = 03 = ج$. فنجمع الحروف فنتحصل على
 كلمة: شفغج. (حساب المغارب) - (Woepcke.M.F., 1863, pp. 472-
 473) ويشير الباحث بريسنيه، الذي كان أستاذ اللغة العربية في
 المدرسة الجزائرية، في كتابه المعنون: "دورة عملية ونظرية في اللغة
 العربية"، إلى أن سكان بلاد المغرب يتبعون نظاماً آخر لتصنيف
 الحروف الرقمية، يتشاركونها في تسع كلمات تقنية، وفقاً لترتيب
 الأرقام التي تشير إلى عدد الوحدات، والعشرات، الخ. (L-Bresnier
 (J), 1915, p. 343) وفيما يأتي هذه الكلمات التقنية التسع التي أشار
 إليها:

| | |
|-------------------------------------|---------------------------------|
| أيفش <i>dyqach</i> , 1-10-100-1,000 | وج <i>was'akh</i> , 6-60-600 |
| بكم <i>bakar</i> , 2-20-200 | زعة <i>za'adz</i> , 7-70-700 |
| جلس <i>djalas</i> , 3-30-300 | حبة <i>h'afaz'</i> , 8-80-800 |
| دمن <i>damat</i> , 4-40-400 | طصغ <i>t'ad'ough</i> , 9-90-900 |
| هنن <i>hanats</i> , 5-50-500 | |

جدول رقم: 01

المصدر: (Pihan,(A. P), *Notice sur les divers genres d'écriture*)

ويسمى هذا التصنيف بتصنيف: (أيقش) (*dyqach*)، وهي
 الكلمة التي نتجت عن مزيج من الحروف الواردة في المجموعة الأولى
 (Pihan.A.P, 1860, p. 213).

نظام التعمية والتشفير العربي:

لقد تطرقنا في العنصر الأول من هذه الدراسة الى كيفية حساب الجمل بتحويل الحروف الى أرقام معلومة باستعمال حساب أبجد هوز، سنقوم بالطريقة نفسها لكن سنستعمل الحروف اللاتينية لتبسيط الأمر ومعرفة نظام التشفير بشكل اسهل أو كما تعرف بشفرات الاستبدال البسيط بالاعتماد على هذه المعادلة الرياضية:

حيث: ع = س + 13 أي كلما أعطينا قيمة لحرف س نجد قيمة ع

لاحظ الجدول:

| | | | | |
|----|----|----|----|-------|
| 4 | 3 | 2 | 1 | قيم س |
| 17 | 16 | 15 | 14 | قيم ع |

الجدول 02

ثم لنحول هذه الحروف اللاتينية الى أرقام لاحظ الجدول 03:

| | | | |
|-------|-------|-------|------|
| 25= Y | 17= Q | 9= I | 1= A |
| 26= Z | 18= R | 10= J | 2= B |
| | 19= S | 11= k | 3= C |
| | 20= T | 12= L | 4= D |
| | 21= U | 13= M | 5= E |
| | 22= V | 14= N | 6= F |
| | 23= W | 15= O | 7= G |
| | 24= X | 16= P | 8= H |

جدول 03

مجال الحروف [Z....A] ومجال الأرقام [1....26]

الآن نعود إلى المعادلة السابقة : ع = س + 13

| | | | | |
|----------------------------|----------------------------|----------------------------|----------------------------|--------------------------------|
| <input type="checkbox"/> D | <input type="checkbox"/> C | <input type="checkbox"/> B | A | <input type="checkbox"/> س قيم |
| <input type="checkbox"/> Q | <input type="checkbox"/> P | <input type="checkbox"/> O | <input type="checkbox"/> N | <input type="checkbox"/> ع قيم |

الشرح : أي عندما أعطينا لي س القيمة A تحصلنا على قيمة ع وهي

$$\begin{aligned} \text{ع} &= \text{س} + 13 \\ \text{N} &= \text{A} + 13 \\ 14 &= 1 + 13 \end{aligned}$$

N لاحظ جدول 13.

س : يمثل الحرف الأصلي

ع : يمثل الحرف المشفر

أي الحرف A يصبح N بعد عملية التشفير:

الآن نريد تشفير كلمة JAMEL باستعمال المعادلة السابقة :

عندما نعطي لي س الحرف J نجد أن ع تصبح قيمتها R

عندما نعطي لي س الحرف A نجد أن ع تصبح قيمتها N

عندما نعطي لي س الحرف M نجد أن ع تصبح قيمتها Z

عندما نعطي لي س الحرف E نجد أن ع تصبح قيمتها E

عندما نعطي لي س الحرف L نجد أن ع تصبح قيمتها Y

أي عند تشفير كلمة JAMEL بالمعادلة السابقة نجد: **RNZE**

بمعنى اننا نظيف للرقم 13 قيمة الحرف بعد N

ملحظ مهم: فك التشفير يكون بإدخال النص المشفر إلى المعادلة

$\text{س} = \text{ع} - 13$ على فكرة هذه المعادلة هي المعادلة المستعملة في خوارزمي

التشفير ROOT13 (file:///C:/Users/win8/Downloads/Noor-)

(Book.com) (باير، 2016، ص: 28) (Delastelle.F, 1902, p. 08).

فهذه إذا أسهل الطرق لعمليات تعمية أو تشفير الحروف، وقد

كان للمسلمين دور كبير في علم التعمية، فهذا المؤرخ الأمريكي

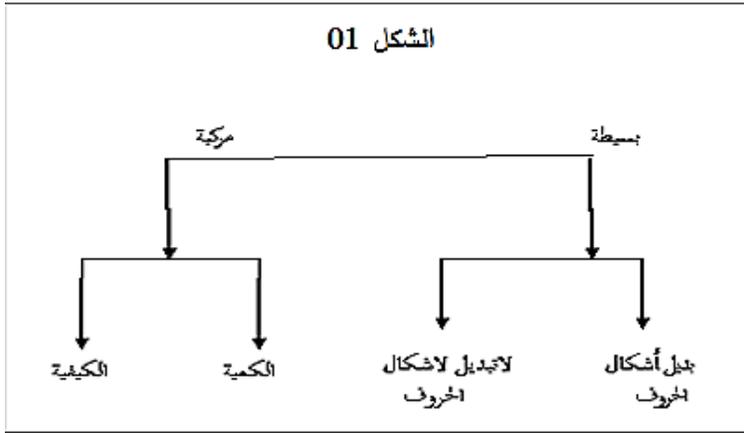
المعروف *David Kahn* الذي أرّخ لعلم التعمية في كتابه: *The Codebreakers* بعد أن استعرض كل الحضارات حتى القرن السابع الميلادي يقول: "ولد علم التعمية بشقيه بين العرب، فقد كانوا أول من اكتشف طرق استخراج المعّمى وكتبها ومن دونها" ومن بين ما يذكره استعمال أبجدية بديلة كلاسيكية أخرى في وقت متأخر من عام 1775م، في رسالة تجسس إلى وصي العرش في الجزائر العاصمة. عُرف هذا النص في تركيا باسم "المصري" (Kahn, 1968, p. 93) ومن أشهر علماء المسلمين الذين كتبوا وتبحروا في هذا المجال نجد:

- ✓ جابر بن حيان، وله كتاب (حل الرموز ومفاتيح الكنوز).
 - ✓ يعقوب بن اسحاق الكندي له رسالة سماها (رسالة في استخراج المعّمى).
 - ✓ علي بن محمد بن الدريهم كتابه الذي سماه (مفتاح الكنوز في إيضاح الرموز).
 - ✓ إبراهيم بن محمد بن دنينير له رسالة (مقاصد الفصول المترجمة عن حل الترجمة) (Ibrahim, 2010, pp. 49-52).
- وغيرهم كثير لا يسعنا أن نذكرهم جميعا... فقط نأخذ المثال للاعتبار.

نظام التعمية والتشفير عند الكندي يعقوب بن اسحاق:

يمكن القول إن البدايات الأولى في تكوين علم الحساب المرتبط بعلم التعمية عند المسلمين، وحسب الكثير من الآراء (Singh, 2000, pp. 32-33) كانت إنطلاقا من القرن الثالث الهجري (التاسع الميلادي)، وبالتحديد بداية مع محاولات الكندي يعقوب بن اسحاق، وتلميذه احمد البلخي وابن الدريهم الموصلية.. وبالرغم من أسبقية أقوام

الهند واليونان والفرس في علوم الحساب والتعمية أو التشفير، إلا أن العرب والمسلمين خاصة المغاربة استطاعوا أن يبرعوا فيه، ويجدوا العديد من الحلول للمسائل الحسابية والفلكية التي كانت تشغلهم، سنحاول تقديم بعض الأمثلة لنظام التعمية عند الكندي بشكل مبسط حيث يقسم الطرق الأساسية للتعمية الى قسمين كما يوضحه الشكل 01:



فالبسيطة يقسمها بدورها الى قسمين:

1 - بتبديل اشكال الحروف ويتفرع عنها :

- بتغيير مواضع الحروف وخلطها مثال: لاحظ الجدول 04:

| | | | | | |
|---|----|---|---|----|------------------|
| أ | ب | ج | د | هـ | حروف النص المرتب |
| د | هـ | أ | ج | ب | حروف النص المشفر |

الجدول 04

- اتخاذ رموز مبهمه لحروف مرتبة هكذا في الجدول 05:

| النص الواضح | من | منا | أمتن | المتن |
|-----------------------------|----|-----|------|-------|
| الإمكانية الأولى للتعمية | ⊞ | ⊞ | ⊞ | ⊞ |
| الإمكانية الثانية | ⊞ | ⊞ | ⊞ | ⊞ |

الجدول 05

وقد أشار الكندي إلى طريقة أخرى وهي إمكانية أن يوضع لكل ثنائية كثيرة الوجود رمزا أو شكلا واحدا مثل ثنائيات: لا - من - أل - أو - ما. (لاحظ الجدول 06):

| حروف النص المرتب | أ | ب | ج | د | هـ | و |
|------------------|---|---|---|---|----|---|
| حروف النص المشفر | ⊞ | ⊞ | ⊞ | ⊞ | ⊞ | ⊞ |

الجدول 06

لنصل الى المستطيل (07 X 04) عند الكندي وقد تضمن عدد الحروف الكامل أو المربع 87 فتُعَمِّي (نشفر) كلمة محمد هكذا:

⊞ ⊞ ⊞ ⊞

لاحظ كيف تم تعمية أو تشفير اسم محمد في الجدول 07 (محمد، 1987، ص: 49-52).

| الشكل الثاني الأول | ١ | ٢ | ٣ | ٤ | ٥ | ٦ | ٧ |
|-----------------------|----|----|----|----|----|----|----|
| أ | ب | ت | ث | ج | د | هـ | و |
| ١ | ٢ | ٣ | ٤ | ٥ | ٦ | ٧ | ٨ |
| ٩ | ١٠ | ١١ | ١٢ | ١٣ | ١٤ | ١٥ | ١٦ |
| ١٧ | ١٨ | ١٩ | ٢٠ | ٢١ | ٢٢ | ٢٣ | ٢٤ |

الجدول 07

نماذج من أنظمة التشفير:

سنحاول تقديم بعض الأمثلة على التشفير في بلاد المغرب، والأساليب الأخرى للتشفير والإخفاء التي استعملها المغاربة بين القرنين السابع عشر والتاسع عشر خاصة، وسنلاحظ استعمالا مكثفا لحساب الجمل ولتشفير الأرقام تم استعمال شبكة مليئة بالأبيات الشعرية على شكل رقعة شطرنج لكتابة رسالة معينة، وبالرغم من قلة الكتابات الأكاديمية المغربية حول علم التشفير أو التعمية، لكن هناك بعض الكتب في التاريخ أو الرحلات الاستكشافية أو علم الفلك التي تقدم أفكاراً في علم التشفير تنسب إلى مغاربة وأندلسيين كابن سبعين أو عبد الواحد بن مسعود عنون. وتأتي هذه الندرة من حقيقة أنه لا يزال هناك عدد من الأرشيفات السرية التي لم يتم اكتشافها بعد في الكتب والمخطوطات القديمة التي تم تجاهلها في المكتبات العائلية القديمة أو التي لا تزال مفقودة.

لكن ومع ذلك فيمكن الاستفادة من بعض الدراسات التي استفدنا منها كأبحاث عبد المالك عزيزي الذي نشرها في مجلات

مختلفة وان كنا قد نجد تكرارا للمعلومات نفسها ! (Azizi.A, 2013, p. 334). وكما قلنا سابقا فإن أهل بلاد المغرب كانوا يستعملون نظاما أبجديا مخالفا لما هو موجود في المشرق، فإلى جانب استخدام حساب أبجد هوز، يوجد نوع ثالث يستعملونه في تأريخ المنتسخات، وترقيم أوراق المخطوطات، وفي عمليات وثائق المحاكم الشرعية، وصار يعرف بالقلم الفاسي (Colin.G., 1933, pp. 211-212) بالمغرب الأقصى، ليتطور هذا النظام وليصبح أداة للتشفير، وبوصفه طرقا بديلة في إخفاء المعلومات في أدبيات المراسلة والترسل، فقد مارس المغاربة عدة أساليب في استعمال الشعر، فأخفوا بشكل خاص الرسائل أو المفاتيح أو التوقيعات السرية بين أحرف واحدة، أو عدة أبيات في قصيدة واحدة، سنستدل بالعديد من طرق التشفير التي تم إدخالها في القصائد، مثل طريقة السلطان المنصور الذهبي وهو أول مثال على التشفير الحسابي الذي تم تقديمه في أواخر القرن السادس عشر (Azizi.A, 2013, p. 329). سنقدم أمثلة أخرى على إخفاء المعلومات والتشفير المستعمل في بلاد المغرب والأندلس:

المثال الأول: علاقة الحروف بالأبيات:

يتعلق برسالة كتبها الملك المعتمد بن عباد صاحب إشبيلية بالأندلس أرسلها إلى زوجته إعتاد كانت قصيدة حب أعطاها اسم زوجته؛ قام بتأليف القصيدة بحيث تشكل الأحرف الأولى من كل بيت اسم إعتاد (الشكل الشكل 02) (Azizi.A, 2013, p. 330).

ا غائبة الشخص عن ناظري
 ع ليك السلام بقدر الشجون
 ت ملكتي مني صعب المرام
 م رادي لقياك في كل حين
 ا قيعي على المهدي ما بيننا
 د ست اسمك الحلو في ظي شري
 وحاضرة في هميم الفؤاد
 ودمع الشجون وقدر السهاد
 وصادقت ودي سهل القيادة
 فياليت اتي اعطي مرادي
 ولا تستحيل لطول البعاد
 وألقت فيه حروف « اعتاد »

الشكل 02

المثال الثاني: التشفير عبر قطعة الشطرنج:

في عام 1736م، كتب المهدي الغزال -الذي كان قبل هذا التاريخ مبعوثاً للسلطان مولاي إسماعيل (1672- 1727) إلى إسبانيا، وكان مكلفاً بشكل خاص للتفاوض بشأن استعادة مكتبة مولاي زيدان من إسبانيا، كتب قصيدة دينية بعنوان "اليواقيت الأدبية في الأمداح النبوية"، وقد وقع عليها بطريقة رائعة، فكان توقيعه يتمثل في إدخال الحروف التي يتكون منها اسمه داخل بيت من القصيدة، وكانت حروف اسمه: المهدي غزال هي الأحرف الثانية من كل كلمة مؤلفة في بيت القصيدة (Azizi.A, 2013, p. 332)

واغفر إلهي لمن له مدح فيه بغرب وزنه ذا الكرم
 أ ل م د د ي غ ز ال
 وفي ظهور يمن لها ظهرت تزهو بأمداح سيد الأمم

الشكل 03

المثال الثالث التشفير باستعمال أبيات القصيدة:

كما رأينا في الطريقة التي استعملها المهدي الغزال عندما وقع شعره الديني، فطورها وعمّمها ابنه أحمد، الذي كان أيضاً مبعوثاً للسلطان محمد الثالث (1757- 1790) إلى ملك إسبانيا. فأخذ قصيدة من ثماني أبيات، وقسم كل بيت إلى ثمانية أجزاء. ثم اعتبر شبكة بها ثمانية أسطر وثمانية أعمدة، ووضع البيت الأول في السطر الأول من الشبكة مرتبة كجزء 1 في العمود 1، والجزء 2 في العمود 2، وهكذا دواليك. وبالمثل، وضع البيت الثاني في السطر الثاني، البيت الثالث في السطر الثالث، وهكذا... ثم استخدمها واختار حروف الجملة التي أراد أن يبينها (الشكل 04):

حمدا مرشد عبده ، لثائه وحده . ونسّم على سيّدنا محمّد وبنيه ،
والصّحب ومحبّيه . أمّا بعد .

وجملة حروف الحمد والتّصلية وأمّا بعد أربع وستون حرفاً ؛ وكيفية أخذها من الجدول نعتا ووصفا ، أن تأخذ :

- حرفه الأول من أول سابع الأول .
- 2 ، وهو الرابع في رابع السابع .
- 3 ، هو الرابع في ثالث الرابع .
- 4 ، هو [995] الأول في خامس الثالث .
- 5 ، الأول في سابع الثاني .

(الشكل 04)

- لبيت الأول نحب إلى الخط السابع في الحرف الأول من الكلمة نجد الحرف: ح ←
- لبيت السابع نحب إلى الخط الرابع في الحرف الرابع من الكلمة نجد الحرف: م ←
- لبيت الرابع نحب إلى الخط الثالث في الحرف الرابع من الكلمة نجد الحرف: د ←
- لبيت الثالث نحب إلى الخط الخامس في الحرف الأول من الكلمة نجد الحرف: أ ←
- لبيت الثاني نحب إلى الخط السابع في الحرف الأول من الكلمة نجد الحرف: ل ←

الشكل 05

وبيانه كالتالي (لاحظ الشكل 05) ثم نجمع الحروف لنجد بيان كلمة: حمدا ل...وهكذا لبقية حروف الحمدلة والتصلية لنحصل على شبكة في شكل رقعة شطرنج كما هو مبين في (الجدول 08).

| | | | | | | | | | |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| 49 د 42 د 29 د | 27 ح 19 ح 4 ح | 58 ر 32 ر 28 ر | 7 ر 32 ر 28 ر | 45 ي ذكي 52 ي | 16 ب 43 ب 27 ب | 46 ز 48 م 51 م | 51 ل 34 ل 63 ل | 44 ن 34 ن 34 ن | 13 م 40 م 38 م |
| 45 غ 32 غ 33 غ | 4 ل 5 ل 3 ل | 53 أ 59 أ 24 أ | 59 أ 39 أ 5 أ | 62 م منيب 39 م | 15 م 56 م 41 م | 47 أ 64 أ 21 أ | 2 ل 50 ل 23 ل | 50 م 2 ل 62 ل | 49 ل 64 ل 47 ل |
| 41 د 24 د 18 د | 57 ر 25 ر 7 ر | 14 ا 37 ا 40 ا | 37 ا 20 ا 20 ا | 18 ا 29 ا 26 ا | 56 م 58 م 3 م | 3 ر 53 ر 3 ر | 41 ع 52 ع 42 ع | 41 د 41 د 42 ع | 48 ا 43 ا 30 ا |
| 7 د 27 ر 35 ر | 50 ن 22 ن 30 ن | 28 د 35 د 7 د | 35 د 22 د 44 د | 17 ا 29 ا 8 ا | 21 ر 20 ر 17 ر | 8 م 3 د 2 م | 19 ل 14 ل 25 ل | 3 د 19 ل 46 ل | 31 ل 44 ل 16 ل |
| 38 د 16 د 11 د | 23 ن 11 ن 12 ن | 12 ن 26 ن 15 ن | 26 ن 12 ن 22 ن | 10 ع 60 ع 13 ع | 13 ا 61 ا 45 ا | 34 ن 55 ن 9 ن | 11 د 23 د 36 د | 34 ن 55 ن 36 د | 33 ر 63 ر 41 د |
| 10 ا 18 ر 8 ي | 33 ل 28 ل 9 ل | 61 ج 60 ج 56 ج | 60 ج 22 ج 51 ج | 38 م 22 م 19 م | 6 د 9 د 39 د | 37 ب 51 ب 24 ب | 31 ر 8 ر 15 ر | 37 ب 51 ب 24 ب | 29 م 20 م 60 ي |
| 32 د 19 د 50 د | 34 ح 39 ح 14 ح | 35 م 15 م 47 م | 15 م 35 م 26 م | 54 م 62 م 53 م | 17 ر 2 م 22 ر | 26 م 55 م 45 م | 30 م 52 م 40 م | 26 م 55 م 45 م | 21 ح 24 ح 37 ح |
| 42 ع 30 ع 43 ع | 5 ع 57 ع 5 ع | 59 ع 63 ع 10 ل | 63 ع 59 ع 10 ل | 47 ر 47 ل 57 ل | 54 م 6 م 49 م | 9 ر 40 ر 38 ر | 25 ن 36 ن 61 ن | 40 ر 25 ن 61 ن | 12 د 36 د 44 د |

(Azizi.A, 2013, pp. 332-333)

(الجدول رقم: 08)

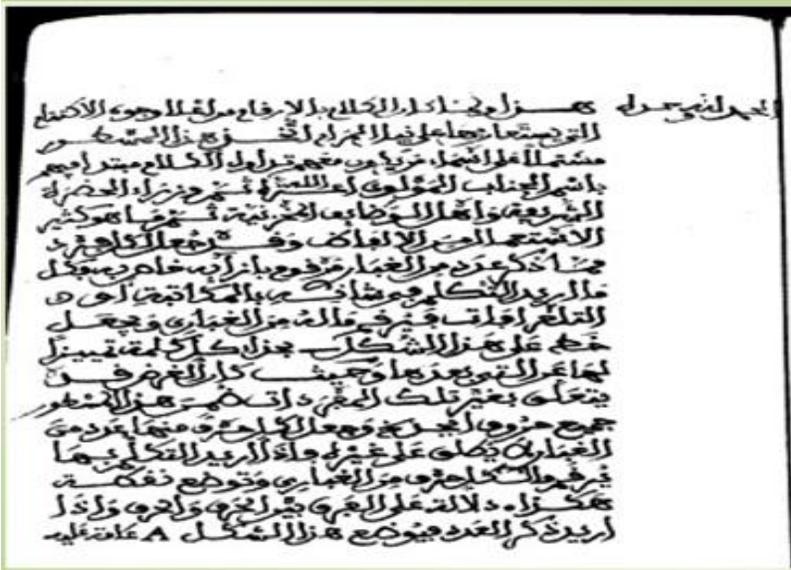
وما بين القرن السادس عشر والتاسع عشر، كان هناك استعمال مكثف لوظيفة التجزئة "بحساب الجمل" من خلال تشفير الأرقام بالحروف ولتشفير الكلمات بالأرقام من أجل ضمان الأفعال المالية والقانونية كما في شهادات الميراث أو الزواج التي تطورت اليوم باستعمال تقنيات الكمبيوتر الجديدة؛ ومع ذلك، هناك بلا شك العديد من الأفكار الأخرى، التي يمكن العثور عليها، في الوثائق والمخطوطات القديمة.

المثال الرابع التشفير باستعمال العدد:

يعتمد نظام تشفير المعلومات وإخفائها على طريقة لا يفهمها إلا أصحابها لأنه يتخذ السرية في المعاملات المختلفة، الذين لهم مصلحة في إخفاء معلوماتهم المهمة.

وعلى الرغم من قلة الباحثين في هذا العلم الذي قالت عنه الوثيقة أنه من أعلا وجوه الاكتناه فقليل من يدركه (قاسم، 2001، ص ص: 17- 18- 20)، لذا فإننا سنحاول في هذه الورقة تبسيطه، وهذا بالاعتماد على احدى الوثائق (الشكل 06) التي لم يذكر تاريخها إلا أنه (الشكل رقم: 06) من الممكن أن نؤرخها بأوائل القرن 20م حوالي سنة 1904م من خلال استعمال هذه الوثيقة لمصطلح التلغرافات، وقد نشرها عبد المالك عزيزي (Azizi.A, 2013, p. 334) ونحن نعيد نشرها لكن مع شرحها بشكل مبسط للقارئ الكريم، وبطريقة أوضح في شرح طريقة التشفير.

تبتدأ الوثيقة بما يأتي:



- السطر 01: الحمد لله وحده هذا ولما كان الكلام بالأرقام من أغلا وجوه الاكتتام
- السطر 02: التي يستعين بها على نيل المرام اتخذ هذا المسطور
- السطر 03: مشتملا على أسماء من يكون معهم تداول الكلام مبتدأ (مبتدئا) فيهم
- السطر 04: باسم الجناب المولوي أعزه الله ثم وزراء الحضرة
- السطر 05: الشريفة وأهل الوضاييف(الوظائف) المخزنية ثم ما هو كثير
- السطر 06: الاستعمال من الألفاظ وقد جعل لكل فرد
- السطر 07: مما ذكر عدد من الغبار مرقوم بازايه(بإزائه) خاص به فكل
- السطر 08: ما أريد التكلم في شأنه بالمكاتبة أو
- السطر 09: التلغرافات فيرقم ماله من الغباري ويجعل
- السطر 10: خط على هذا الشكل — بجذا (بجنب) كل كلمة تمييزا
- السطر 11: لها عن التي بعدها وحيث كان الغرض قد لا
- السطر 12: يتعلق بغير تلك المفردات ضمن هذا المسطور
- السطر 13: جميع حروف أبجد(...) وجعل لكل حرف منها عدد من

السطر14: الغبار لا يطلق على غيره فاذا أريد التكلم بها

السطر15: يرقم ما لكل حرف من الغباري وتوضع نقطة

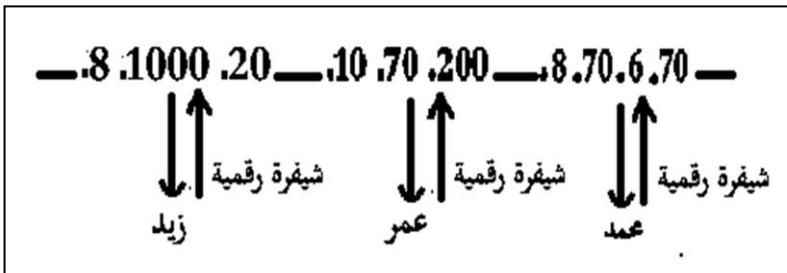
السطر16: هكذا (•نقطة) دلالة على الفرق بين الحرف والحرف واذا

السطر17: أريد ذكر العدد فيوضع هذا الشكل (A) علامة عليه

الشرح:

من خلال ما جاء في هذه الوثيقة فإن صاحبها يعلل بأنه وبسبب كثرة الوزارات والوظائف، وأيضا كثرة المستعملين في مختلف دوائر الحكم، والمُلك في بلاد المغرب الأقصى وعددهم، فإن ذكر أسمائهم وأسماء آبائهم مع كثرة الألفاظ، ولكي لا يقع الخلط، والسقط فإنه استُعِيض عن ذلك باستعمال حساب الجُمَّل بحيث أن خصَّ كل فرد من هؤلاء بعدد غباري يعوض حروف اسمه دون سواه، ومثال ذلك من خلال ما جاء في الوثيقة ولكي نبسط الأمر:

سنأخذ مثلا ثلاثة أسماء وهم: محمد - عمر - أسامة .
ونحسب قيم كل حرف من أسمائهم (باستعمال نظام حساب الجُمَّل):
وبعدها نفرق هذه الأعداد كما قال صاحب الوثيقة (في السطر العاشر) يخط للدلالة على التفرقة بين اسم وآخر، وهكذا توزع أرقام الحروف، وكذا أسماء الأفراد المخفية بشيفرة رقمية هكذا:

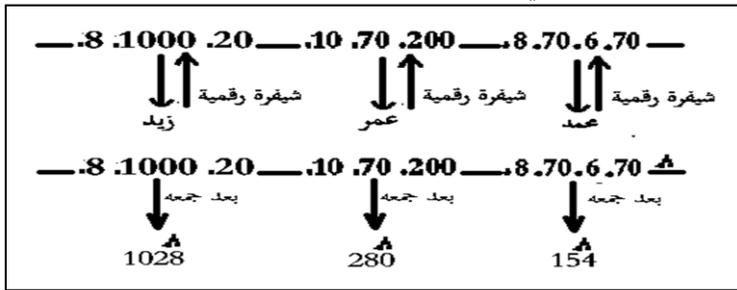


ودرءاً لكل لبس أو خلط بين الأرقام فقد اقترح صاحب الوثيقة استعمال هذا الشكل: (A) والغاية منه التفريق في الصفحة الواحدة بين الأعداد الأفقية والعمودية بعد جمع الأرقام، لتتحصل في الأخير على شيفرة لكل اسم هكذا:

محمد شيفرته هي: 154A

عمر شيفرته هي: 280A

زيد شيفرته هي: 1028A



خاتمة:

وفي الأخير ومما سبق نستطيع القول أن البدايات الأولى في تكوين علم الحساب المرتبط بعلم التعمية عند المسلمين وحسب الكثير من الآراء كانت انطلاقا من القرن الثالث الهجري (التاسع الميلادي)، وبالتحديد بداية من عهد الكندي يعقوب بن اسحاق وتلميذه أحمد البلخي وابن الدريهم الموصلية، وبالرغم من أسبقية أقوام الهند واليونان والفرس في علوم الحساب والتعمية أو التشفير إلا أن العرب والمسلمين خاصة المغاربة في بلاد المغرب الإسلامي استطاعوا أن بيرعوا فيه ويجدوا العديد من الحلول للمسائل الحسابية والفلكية التي كانت تشغلهم.

ويمكننا الخروج من خلال هذه الدراسة بمجموعة من النتائج
نلخصها في ما يأتي:

- 1 - كان أهل بلاد المغرب يستعملون نظاماً أبجدياً مخالفاً لما هو موجود في المشرق.
- 2 - أسهم العرب المغاربة في بلورة حساب الجُمَّل وتطويره.
- 3 - يتبع أهل بلاد المغرب نظاماً آخر خلافاً للمشاركة في تصنيف الحروف الرقمية.
- 4 - ابتكر المغاربة طرقاً أخرى في إخفاء المعلومات والتعمية بوصفها أسلوباً للتشفير الرقمي، واعتمد هذا النظام على إخفاء المعلومات على طريقة لا يفهمها إلا أصحابها، لأنه يتخذ السرية في المعاملات المختلفة، والذين لهم مصلحة في إخفاء معلوماتهم المهمة.
- 5 - ضرورة الاهتمام بالتاريخ الهجري والعودة إلى العمل والتأريخ به.
- 6 - علم الاكتناه هو علم يختص بدراسة المخطوطات وتمحيصها وتأريخها بدقة. ولا يُعنى بعلم دراسة فحسب، بل هو اشتقاق جديد للباحث من اكتنه الشيء إذا تعرف عليه، واستتبط منه نتائج علمية، فهو معرفة ما وصل إلينا من تراث مكتوب أو منقوش أو مرسوم ثم دراسة المواد التي دخلت في صناعة كل ذلك واستنباطه.

قائمة المصادر والمراجع:

- 1 - بايير ميريفي شون. (2016). علم التشفير. (محمد سعد طنطاوي، المترجمون) القاهرة: مؤسسة هنداوي للتعليم والثقافة.
- 2 - التميمي حاتم عبد الرحيم. (2011 - 12 - 01). حساب الجُمَّل في كتب التفسير (مقالة منشورة). مجلة كلية الشريعة الكويت.
- 3 - السامرائي قاسم. (2001). علم الإكتناه العربي الإسلامي (الإصدار ط1). الرياض: مركز الملك فيصل للبحوث والدراسات الإسلامية.

- 4 - الفيروزآبادي مجد الدين محمد بن يعقوب. (2005). القاموس المحيط. بيروت: مؤسسة الرسالة.
- 5 - بن قربة، صالح. (2011). أبحاث ودراسات في تاريخ وآثار المغرب الاسلامي وحضارته. الجزائر: دار الهدى.
- 6 - المراكشي محمد الصغير. (1880). نزهة الحادي بأخبار ملوك القرن الحادي.
- 7 - المرياتى محمد. (1987). علم التعمية واستخراج المعنى عند العرب. دمشق: مطبوعات مجمع اللغة العربية.
- 8 - ابن منظور. (1955). لسان العرب. بيروت: دار المعارف.
9. Azizi.A. (2013). *Instances of Arabic Cryptography in Morocco II*. Cryptologia; Taylor And Francis. 334 ،
10. Bresnier(L-J). (1915). *Cours Pratique Et Théorique De Langue Arabe*. Alger: 2eme id.
11. Colin.G. (1933). *de l'origine grecque Des Chiffres De Fès*. Hespéris. 211 .
12. Delastelle.F. (1902). *Cryptographie*. Paris: Gauthier-villars.
13. Ibrahim, A.-k. (2010). *Origins of Cryptology: The Arab Contributions*. Cryptologia, 97-126.
14. Kahn, D. (1968). *The Codebreakers*. New York: The Macmillan Company.
15. Pihan.A.P. (1860). *Notice sur les divers genres d'écriture* . Paris.
16. Singh, S. (2000). *The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Andjor Books.
17. un initi. (1894). *Cryptographie occultes*. Ch;XIV . Mystères des sciences ،Paris. ،france.
18. Woepcke.M.F, 1. (1863). *La Propagation Des Chiffres Indiens*. *Journal Asiatique*, 472-473.

