

التعمية في خدمة المجتمع

أ. د. أبو بكر خالد سعد الله

المدرسة العليا للأساتذة

القبة، الجزائر



" لم نجد في الكتابة السرية لدى كل الحضارات التي استعمرناها حتى الآن ... أي عمل والحق في استخراج المعنى ... وبالتالي فإن علم التعمية الذي يشمل علمي التعمية واستخراج المعنى لم يولد حتى هذا التاريخ [أي القرن 7م] في جميع الحضارات التي استعمرناها بما فيها الحضارة الغربية ... ولد علم التعمية بشقيه بين العرب، فقد كانوا أول من اكتشف طرق استخراج المعنى وكتبها ودونها. إن هذه الأمة التي انبثقت من الجزيرة العربية في الأعوام الستة والتي أشعت فوق مساحات من العالم المعروف، أخرجت بسرعة واحدة من أرقى الحضارات التي عرفها التاريخ حتى ذلك الوقت."

(مؤرخ علم التعمية ديفد كاهن David Kahn في كتابه The code breakers)

ملخص:

تُغنى التعمية cryptography بطرق إخفاء المعلومات ودراسة تطبيقاتها. وهي تعتبر في هذا العصر فرعاً من فروع الرياضيات وعلم الحاسوب. نتناول في هذا البحث موقوع التعمية وعلاقتها بشتى الميادين، أبرزها التجارة الإلكترونية والبطاقات البنكية ومختلف كلمات المرور الحديثة، الخ.

ونتناول في البداية الجانب التاريخي للتعمية ومنشأها كعلم تفوق فيه العرب والمسلمون فكانوا رواداً في هذا المجال. وقد تطورت التعمية قبل الحرب

العالمية الثانية، كما تواصل هذا التطور بعد الحرب باستخدام وسائل جديدة. ولذا قدمنا بعض التفاصيل حول هذا الجانب [2] لمن قائمة مرتبة زمنيا تضم أبرز المحطات التي مر بها علم التعمية.

ومن جهة أخرى، خصصنا حيزا من هذه الدراسة للتعمية العسكرية والجوسسة، كما ركزنا على تلك التي تمس المعلومات والوثائق ذات الطابع الاقتصادي والصناعي والاجتماعي، وقدمنا في ذلك نموذجين حديثين. وفي الأخير أشرنا إلى التعمية الكمومية quantum cryptography المبنية على مفاهيم ميكانيكا الكم وإلى آفاقها المذهلة، إذ من المتوقع أن تعوض التعمية الكمومية مستقبلا التعمية المؤسسة على نظرية الأعداد (الرياضيات) المتداولة الآن، وهو ما سيحدث ثورة عارمة في هذا المجال يسقط من جرائها الكثير من الضحايا (بشراً ومؤسسات).

كانت الدبلوماسية ومصالح الدفاع العسكري والتجهيزات الحربية تحتكر التعمية cryptography وأدواتها. ومنذ مطلع القرن العشرين بدأت الأمور تتغير في اتجاه آخر، وتمخضت التعمية عبر الرياضيات فولدت علم الحاسوب! والغريب أن هذا العلم الذي لا يتجاوز عمره عشرات السنين قد تمكن من احتواء علم يرجع تاريخه إلى أزيد من عشرين قرنا، ومنذ منتصف السبعينيات من القرن العشرين، امتد استعمال التعمية من مجال الاتصالات والمراسلات العسكرية والدبلوماسية والأمنية إلى عديد المجالات الأخرى، مثل الصناعة والاقتصاد والتجارة (للحفاظ على الأسرار المتعلقة بالابتكارات والتصاميم، وبالصفقات التجارية والأوراق المالية، الخ)؛ والبنوك والهيئات المصرفية (للحفاظ على حسابات الأفراد والودائع، وحمايتها من الاختلاس والتحايل).

وامتد أيضا هذا الاستعمال إلى شبكات الحواسيب الشخصية وغير الشخصية (للحفاظ على أمن المعلومات الحساسة، وحماية الملفات والمعلومات والحيلولة دون ولوج الغير إلى الشبكات عن طريق الرقم السري الخاص بالمستخدم؛ وإلى الاتصالات السلكية واللاسلكية المتعددة الأشكال لحمايتها من خطر التَّنصّت). كما نجد التعمية في البث التلفزيوني حيث يتم تشفير برامج بعض القنوات لمنع مشاهدتها باستثناء المشتركين.

ولعل الكثير من القراء لا يعرفون أن للتعمية دورا بارزا أيضا في مجال البحث عن اللغات القديمة والكشف عن أسرارها، فهي التي كشفت مثلا عن رموز اللغة الهيروغليفية منذ عشرات السنين ... ولا يزال هذا العلم يستخدم في الكشف عن خبايا اللغات المسماة القديمة. وهكذا تتضح الأهمية المتزايدة التي يكتسيها علم التعمية في كافة المجالات، ومن ثمّ فهو يستحق منا وقفة متأنية لتتعرف على مختلف جوانبه، سيما التاريخية والمستقبلية.

ما هي التعمية؟

يمكن أن نقول بإيجاز أن التعمية مجموعة من الأدوات التقنية التي تسمح بإخفاء معلومات بواسطة شفرة سرية، كأن تكتب نصا وتستبدل فيه كل حرف بحرف آخر، أو برقم وفق قاعدة معينة (كاستبدال كل حرف بالحرف الذي يليه في الترتيب الأبجدي). وينظر البعض إلى التعمية على أنها "علم السرية".

والواقع أن هناك نوعين من التعمية، هما تعمية المعاني بالتورية التي تعتمد على خبرة المتراسلين وعلاقاتهم فيما بينهم، وهذا النوع بعيد عن التعمية الحديثة، ولا يهمننا في هذا المقام. أما النوع الثاني، فهو يعني بتعمية الحروف،

يغض النظر عن معنى الكلمات والجمل، ولذا فهو يخضع لقواعد دقيقة جعل من التعمية علما قائما بذاته.

وتستخدم التعمية الآن، كما كان حالها في الماضي، وسائل لغوية وأدوات من المنطق الرياضي والرياءيات ذاتها، فصارت التعمية الحديثة تمس العديد من المظاهر الاجتماعية. وأصبحت بذلك وطيدة الصلة بكافة المجالات العلمية. ومن ثم ساد استعمال أحدث الوسائل التكنولوجية، وأصبحنا في أمس الحاجة إلى سن قوانين جديدة تنظم سير هذا العلم وتماشى مع نظرة الأفراد والمسؤولين لمفهوم "السرية".

ويرى بعض المؤرخين أن التعمية بدأت فنا ثم صارت تقنية، ولم تلبث طويلا حتى أصبحت علما مستقلا بقواعده وأدواته المختلفة. وقد عاشت التعمية هذه المراحل الثلاث غير المتساوية المدة، وانتقلت من مرحلة إلى أخرى عبر انقطاعات وقفزات نوعية أوصلتها إلى عصرها الحالي، وهو يمثل بدون شك عصرها الذهبي. لنستعرض الجانب التاريخي لعلم التعمية مبتدئين بما أسهم به أجدادنا العرب والمسلمون في هذا الباب لأنهم أهل لهذا التبجيل كما سنرى أدناه.

التعمية عند العرب والمسلمين:

لا شك أن القارئ غير المختص سيستغرب عندما يطلع على رأي ثلاثة خبراء ومؤرخين عرب لعلم التعمية، وهم محمد مرياتي ويحيى مير علم ومحمد حسان الطيان حين يقولون : "خلصنا من بحثنا هذا إلى أن علم التعمية واستخراج المعنى علم عربي الأصل والنشأة والتطور، فالعلماء العرب هم أول من كتب في طرائق التعمية الرئيسية التي مازال العالم يستخدم بعضها حتى اليوم. وما كان لنا أن نصل إلى هذه الحقيقة لولا اكتشافنا مخطوطات عربية مهمة

في هذا الباب، منها ما هو موغل في القدم يعود إلى القرن الثالث للهجرة، ومنها ما كان في حكم الضائع المفقود ... " (مرياتي، 1992 : ص 27).

وهذه شهادة أخرى لأحد الغربيين تؤكد رأي المؤرخين العرب السابقين في أسبقية أجدادنا في اكتشاف طرق استخراج المعنى وتأليفهم في هذا النوع. يقول مؤرخ علم التعمية ديفد كاهن David Kahn : " لم نجد في الكتابة السرية لدى كل الحضارات التي استعملناها حتى الآن ... أي عمل والحق في استخراج المعنى ... وبالتالي فإن علم التعمية الذي يشمل علمي التعمية واستخراج المعنى لم يولد حتى هذا التاريخ 1 في جميع الحضارات التي استعملناها بما فيها الحضارة الغربية ... ولد علم التعمية بشقيه بين العرب، فقد كانوا أول من اكتشف طرق استخراج المعنى وكتبها ودونها. إن هذه الأمة التي انبثقت من الجزيرة العربية في الأعوام الستة والتي أشعت فوق مساحات من العالم المعروف، أخرجت بسرعة واحدة من أرقى الحضارات التي عرفها التاريخ حتى ذلك الوقت." 2 (مرياتي، 1992 : ص 30).

وتأكيداً على ما ذهب إليه هؤلاء الخبراء جميعاً، نتعرف على بعض العرب القدامى الذين كتبوا في علم التعمية وانشغلوا به خلال نحو ثمانية قرون :

1- الخليل بن أحمد الفراهيدي (100هـ/718م-170هـ/786م) : ينسب إليه كتاب في التعمية لم يعثر عليه المؤرخون، بل هناك من اعتبر هذا العالم أول من وضع علم التعمية وكتب فيه.

2- جابر بن حيان (توفي 200هـ/810م) : ألف كتاب "حل الرموز ومفاتيح الكنوز".

3- ثوبان بن إبراهيم ذو النون المصري (توفي 245هـ/859م) : ألف كتاب "حل الرموز وبرء الأسفام في أصول اللغات والأقلام".

4- سهل بن محمد بن عثمان السجستاني (توفي 248هـ/862م) : قال فيه ابن النديم في "الفهرست" أنه كان "يتبحر في الكتب ويخرج المعنى، حاذق في ذلك، دقيق النظر فيه."

5- يعقوب بن إسحاق الكندي (توفي 260هـ/873م) : من مؤلفاته في التعمية رسالة في استخراج المعنى.

6- أحمد بن علي بن وحشية (توفي بعد 291هـ/914م) : من مؤلفاته في علم التعمية "شوق المستهام في معرفة الأقلام". وقد ترجم الكتاب إلى الإنكليزية عام 1806.

7- محمد بن أحمد بن كيسان (القرن 3هـ/9م) : قال ياقوت الحموي في "معجم الأدباء" أن "له في العروض والمعنى كتابا."

8- داود بن الهيثم بن إسحاق التنوخي (228هـ/843م-316هـ/928م) : كان نحوياً لغوياً حسن المعرفة بالعروض واستخراج المعنى.

9- محمد بن أحمد بن محمد بن طباطبا (توفي 322هـ/934م) : من مؤلفاته رسالة في استخراج المعنى.

10- محمد بن سعيد البصير الموصللي (القرن 4هـ/10م) : كان رائداً في استخراج المعنى والعروض.

11- إسحاق بن إبراهيم بن وهب الكاتب (نحو القرن 4هـ/10م) : من مؤلفاته في علم التعمية كتاب "البيان والتبيين".

12- أحمد بن عبد العزيز الشنتمري (كان حياً عام 553هـ/1158م) : كان ذائع الصيت في العروض وفك المعنى.

13- أسعد بن مهذب بن مماتي (554هـ/1149م-606هـ/1209م) : من مؤلفاته في علم التعمية كتاب "خصائص المعرفة في المعانيات."

- 14- إبراهيم بن محمد بن دُنيير (583هـ/1187م-627هـ/1229م) : من مؤلفاته في علم التعمية كتاب "مقاصد الفصول عن حل الترجمة".
- 15- علي بن عدلان النحوي المترجم (583هـ/1187م-666هـ/1268م) : من مؤلفاته في علم التعمية كتاب "المؤلف للملك الأشرف في حل التراجم" وكتاب "المُعَلِّم".
- 16- علي بن محمد بن الدريهم (712هـ/1312م-762هـ/1359م) : من مؤلفاته في علم التعمية "مفتاح الكنوز في إيضاح الرموز" و"إيضاح المبهم في حل المترجم" و"مختصر المبهم في حل المترجم" ونظم لقواعد فن المترجم و^[2]وابطه وقصيدة "في حل رموز الأقلام المكتوبة".
- 17- علي بن محمد بن أيدير الجلودي (توفي 742هـ/1341م) : من مؤلفاته في علم التعمية "كنز الاختصاص ودرة الغواص في معرفة أسرار علم الخواص".
- 18- أحمد بن علي القلقشندي (756هـ/1355م-821هـ/1418م) : نجد فصلا كاملا في موسوعته "صبح الأعشى في صناعة الإنشا" المكونة من 14 جزءا يتناول مو^[2]لوع التعمية.
- 19- أحمد بن محمد أبو القاسم العراقي 3 : من مؤلفاته في علم التعمية "حل الرموز وفتح أقفال الكنوز".
- 20- محمد بن الحسن أبو الحسن الجرهمي 4 : له شرح حول طريقة حل تعمية الشعر.

وما دام الأمر هكذا فمن حقنا أن نتساءل : ما الذي جعل العرب والمسلمين يهتمون إلى هذه الدرجة بعلم التعمية بوجه عام؟ يجيب المؤرخون عن هذا السؤال بملاحظتين هما : ظهرت التعمية، بمعنى "تشفير النصوص" في القرنين الثاني والثالث للهجرة، وهذا راجع لمتطلبات ترجمة كتب الحضارات الأخرى، علما أن بعضها كان معمى. ثم إن الحاجة السياسية إلى التعمية، سيما

في منطقة الشام ومصر، ابتداءً من القرن السادس للهجرة ساعدت على تطور هذا العلم، وصار الملوك يستعملون التعمية في مراسلاتهم، وامتد ذلك إلى دواوينهم المختلفة. كما يلاحظ المؤرخون في هذا الباب أنه لولا التقدم الذي عرفته مختلف العلوم عند العرب في ذلك الوقت، وبوجه خاص الرياضيات وعلم اللغة لما بلغ علم التعمية ذلك المستوى المتقدم على أيديهم.

وهكذا نرى أن الحاجة الأمنية هي التي دفعت علم التعمية إلى الأمام مستغلا تطور العلوم الأخرى. فابتداءً من القرن الرابع نجد العديد من العاملين في الدواوين والإدارات يستعملون التعمية حتى صار أمناء السر ملزمين بالإلمام بهذا العلم.

التعمية قبل الحرب العالمية الثانية:

لقد ظهرت التعمية، بمعناها البسيط، منذ العصور الغابرة إذ عثر علماء الآثار عما يثبت استعمالها في عهد الفراعنة. ويُذكر بوجه خاص أن اليهود قديماً كانوا يخفون معاني بعض النصوص بقلب أحرف الأبجدية (وهو ما يسمى التعمية بالقلب)، أي باستبدال آخر حرف في الأبجدية بأول حرف فيها واستبدال ثاني حرف بالحرف قبل الأخير، وهكذا دواليك. ويمكن أيضاً أن تقلب حروف كل كلمة على حدة في النص، فنكتب مثلاً "دحم لآخ دلاخ" بدل "محمد خال خالد".

وهناك أيضاً طريقة التعمية بالإبدال التي تتمثل في الاتفاق على استبدال كل (أو بعض) الأحرف بأحرف أو رموز وفق قاعدة معينة. وعلى سبيل المثال كان يوليوس قيصر يستعمل (القرن 1 ق.م). شفرة سرية في مراسلاته حيث كان يسحب مثلاً جميع الحروف بأربع مراتب : الألف يصبح ثاء والباء جيها

والتاء حاء، الخ. ويتفرع عن علم التعمية علمٌ يسمى "استخراج المعْمَى"، وهو يستخدم علم اللسانيات (خصوصيات اللغة التي تكتب بها الرسائل المشفرة) والرياضيات والإحصاء.

وقد امتدت هذه المرحلة إلى الفترة التي تفصل الحرب العالمية الأولى عن الثانية. ومن المعلوم أن بعض الطرق التقليدية والميكانيكية قد تواصل استخدامها حتى فترة الحرب العالمية الثانية. ويرى المتتبعون أن هذه المرحلة (العصر الفني كما يصفه البعض) هو الذي جلب الأنظار أكثر من أي وقت مضى.

ويفرّق المختصون بين فرعين للتعمية : cryptology (علم التعمية) الذي يهتم بعلم المراسلات السرية وبين cryptography (فن التعمية) الذي يعني مجموعة الطرق والتقنيات التي تضمن السرية. لكن هذا التمييز بين المصطلحين لا زال حديث العهد ولم ينتشر استعماله بين الناس، ولذا سوف نهمل هنا هذا التمييز.

وكان الاهتمام خلال العصر الفني منصباً على كفاءات التشفير، أي تحويل نص ^[٢] إلى نص غامض المعنى. وبعدها تأتي عملية إزالة التشفير (استخراج المعْمَى)، أي ردّ النص الغامض إلى نص مقروء ^[٣] واستناداً إلى القواعد التي تم بها التشفير. وهنا يميّز المختصون بين إزالة التشفير وإزالة التعمية حيث يكمن الفرق بينهما في كون الأولى تعتمد على قواعد وآليات تم بها التشفير. أما الثانية (إزالة التعمية) فتتم دون معرفة مسبقة لتلك القواعد، كما يفعل القراصنة. وسنستعمل هنا - قصد التيسير، ولأننا لا نحتاج إلى المبالغة في التدقيق - مصطلح "التعمية" للدلالة على المصطلحين بما في ذلك التعمية في حد ذاتها (التشفير) وفك (أو استخراج) المعْمَى (كسر الشفرة، أو كسر مفتاح التعمية).

لقد تطورت وتحسنت الطرق التقليدية من عهد الفراعنة وقيصر الروم إلى الحرب العالمية الأولى ببطء شديد. ورغم ذلك ظلت التعمية تستخدم أدوات

بسهولة وسهولة الاختراق. ويرجع ذلك إلى ضعف الوسائل التكنولوجية وإلى كون الجانب النظري لم يتحرر عن الجانب العملي، فلم تظهر مفاهيم نظرية بارزة إلا بعد مرور فترة نضج دامت قرونا.

وكان ظهور مفتاح التشفير قد مكّن من بروز مبدأ آلية تعمية التغيرات بشكل دوري. والملاحظ أن ظهور هذا المفتاح قد واكب "تكميم" أفواه الرياضيين: كان جلّ رجال التعمية خلال الفترة الممتدة من القرون الوسطى إلى عصر النهضة الأوروبية من المختصين في الرياضيات. وتغيّر الأمر فيما بعد وحلّ العسكريون ورجال الأمن محلّ الرياضيين لأن الطابع السري لهذا النوع من الأبحاث يتطلب هذا الخيار.

وعند انتهاء الحرب العالمية الأولى ظهرت آلات تشفير أدت إلى الاستغناء عن كثير من اليد العاملة وحسنت إمكانيات التشفير، ومن ثمّ ظهرت الحاجة إلى تطوير الجانب النظري. فنودي مجدداً إلى الرياضيين، لكنه لم يكن من السهل، بالنسبة للعسكريين وزملائهم الأمنيين، إعادة الرياضيين إلى مجال التعمية لأنها أصبحت تعتبر سلاحاً مرتبطاً بالجهد الحربي والأمني درجة سريته تتطلب توخي الحيلة والحذر الشديدين.

وفي هذا الجو المتقلب، لا نستغرب أن نرى العالم آينشتاين وزملاءه منهمكين في صناعة القنبلة الذرية بلوس ألاموس Los Alamos الأمريكية خلال الحرب العالمية الثانية في الوقت الذي كان فيه الرياضي البريطاني آلن تورينغ Turing (1912-1954) يطور في الريف الإنكليزي آلة كولسوس Colossus التي تعتبر أول آلة إلكترونية حاسبة قابلة للبرمجة. إنها بداية عصر جديد بالنسبة للتعمية، إنه "عصر التقنية". لكن ما علاقة آلة كولسوس بالتعمية؟

لقد كان مشروع كولسوس - الذي أشرفت عليه مصلحة الشفرة البريطانية - جزءاً من برنامج يهدف إلى إزالة التعمية للاتصالات التي يقوم بها الألمان. وليس من محض الصدفة أن نجد الآلة، التي تسمى آلة تورينغ، تمثل في الواقع نموذجاً للجهاز سمي فيما بعد الحاسوب (أو الكومبيوتر)! وهكذا نرى أن التعمية كانت من وراء صناعة الحاسوب وظهور علم الحاسوب. هل نستغرب بعد ذلك من صلة علم التعمية بعلم الحاسوب؟! من هنا بدأت المرحلة الثالثة للتعمية ودخلت عصرها الذهبي من بابه الواسع.

ولم يكن تورينغ وحده في مجال البحث عن إزالة التعمية. ففي مخبر بيل Bell الأمريكية كان كلود شانون Shannon قد وُلق أسس ما يسمى بـ: "نظرية السرية" حتى إن كانت هذه النظرية قد خيّبت آمال البعض. لكن ذلك لم يمنع الأمريكيين من اختراق الشفرة اليابانية آنذاك، وساهم ذلك في انتصار الحلفاء على جيوش هتلر خلال الحرب العالمية الثانية. ومهما يكن من أمر فإن العسكريين ورجال الأمن ساهموا خلال قرون عديدة في تطوير التعمية، ولا يزالون.

والجدير بالذكر هنا أن الاتصالات الألمانية خلال الحرب العالمية الثانية كانت تتم بالراديو عبر الشفرة الشهيرة إنigma Enigma. ولعل أبرز حدث عرفه علم التعمية من الناحية الأمنية هو نظام إنigma الذي ابتكره الألمان قبل الحرب العالمية الثانية. وهو يتمثل في آلة كهروميكانيكية تقوم بتشفير وفك تشفير البرقيات المتعلقة بقوات الحلفاء.

وكانت آلة إنigma لـلخمة لكنها تحمل إلى جبهة القتال على عجالات. والغالب أن الألمان كانوا واثقين من استحالة اختراق هذا النظام، والمؤكد أنهم لم يكونوا على علم من أن هذا النظام كان قد اخترق من قبل الحلفاء قبل اندلاع

الحرب العالمية الثانية بفضل آلة كولسوس، كما أسلفنا. وهذا ما مكّن الحلفاء من فك شفرة نحو 80 % من برقيات الألمان. وقد خصص الحلفاء لهذا العمل التجسسي خلال الحرب أزيد من عشرة آلاف موظف في مركز سري بضواحي لندن. سنعود أدناه ببعض التفاصيل إلى دور التعمية في الجوسسة.

التعمية بعد الحرب العالمية الثانية:

ليس من الغريب أن يكون المدير العلمي، آلن تورينغ، لفريق الباحثين الأنكليز الذين تمكنوا من كسر شفرة آلة إنغما رياضي التكوين. فقد أدت الآلة التي تحمل اسمه إلى ابتكار أول حاسوب في العالم عام 1948. وظل هذا الابتكار طي الكتمان عشرات السنين.

والواقع أن تطور المعلوماتية عرف قفزة نوعية منذ السبعينيات فجعل علم التعمية يتقدم بسرعة فائقة بفضل الرياضيات التي أتاحت حلولاً نظرية لقضية تبادل المعلومات بين عدة أطراف بصفة سرية وذلك بناء على مفهومين جديدين هما مفهوم "المفتاح العمومية" ومفهوم "التوقيع الرقمي".

هناك طريقتان رئيسيتان للتشفير: نظام يقوم على مفتاح متناظرة تسمى "المفتاح السرية" ونظام يقوم على مفتاح غير متناظرة تسمى "المفتاح العمومية". إذا استخدم شخصان "المفتاح المتناظرة" في تبادل الرسائل ينبغي عليهما اقتسام سر يدعى المفتاح السرية. تسمح هذه المفتاح بتشفير الرسالة عند الإرسال، ثم إزالة تشفيرها عند الاستلام. ومن نقائص هذه التقنية وجوب إرسال المفتاح. ولذا يتعين أن تكون قناة المراسلة قناة آمنة.

ولنضرب هنا مثالا نوّح به كيف يمكن الاعتماد على أدوات رياضية في مجال التعمية بالمفتاح السرية: هب أن عليا وأحمد أرادا تبادل برقيات سرية.

عليهما أن يتفقا على استعمال مفتاح سرية... يمكنهما مثلا أن يقررا تبني مفتاحا تستخدم عددا يتكوّن من 19 رقما. ينبغي أيضا أن يتفقا على استعمال صيغة رياضية تسمح بتعمية (تشفير) البرقية، ثم باستخراج المعنى (كسر الشفرة). حتى يرسل علي برقيته يستعمل المفتاح المتفق عليها والصيغة الرياضية، فتصبح بذلك مشفرة غير مقروءة من طرف أي كان. وعندما تصل البرقية إلى أحمد يستخرج المعنى باستعمال نفس المفتاح ونفس الصيغة الرياضية.

فما من شك أن هذا النوع من التشفير قد ساعد على تطوير علم التعمية المعلوماتية، لكن عيبه الرئيسي يتمثل في كونه لا يصلح إلا إذا كان عدد المعنيين بالبرقية لا يتجاوز بضعة أشخاص. ذلك أن تطور شبكة الأنترنت وكثرة زبائنها لا يسمح باستخدام هذا النوع من التعمية على نطاق واسع. والحل ربما يكمن في إيجاد مفتاح سرية لكل شخصين اثنين. غير أنه يستحيل تسيير شبكة الأنترنت بهذا العدد من المفاتيح : فإذا كان عدد المفاتيح اللازمة لخمسة أشخاص هو 10 مفاتيح فإن عدد المفاتيح المطلوبة لألف شخص سيكون نصف مليون مفتاح لتأمين سرية جميع المراسلات.

وحتى تُحل مسألة تعدد المفاتيح السرية تمّ عام 1975 إدخال مفهوم المفتاح العمومية. ويستعمل هذا المفهوم نفس المبدأ المبين في المثال السابق إلا أننا ندخل متغيرا للتشفير وآخر لفك التشفير : تتكوّن المفتاح من جزأين لهماوظيفتان مختلفتان: جزء (مفتاح) سري وجزء (مفتاح) عمومي. وعلى كل شخص أن يعلن للآخر عن مفتاحه العمومية ويحافظ على مفتاحه السرية. ويتم التشفير بواسطة المفتاح العمومية التي يمتلكها مستلم الرسالة ويزال التشفير بواسطة المفتاح السرية لهذا الأخير. وهكذا فكل من يملك المفتاح العمومية يمكنه تشفير رسائله، علما أن مستقبل الرسالة سيستعمل مفتاحه الخاصة لفك الشفرة.

لقد طور الريا^{٢٦}ليون عام 1977 هذه الطريقة وسَمَّوها طريقة RSA (وهي الأحرف الأولى للريا^{٢٦}يين الثلاثة الذين ابتكروها⁵) بناء على نظرية الأعداد مستخدمين الأعداد الأولية التي سنشير إليها لاحقاً. والواقع أن الحاجة إلى التعمية تجاوزت آنذاك المجالات التقليدية (العسكرية والدبلوماسية، الخ). إذ أصبحت حاجة عمومية تمس الحياة اليومية للمؤسسات بكافة أشكالها وكذا الأفراد. وهكذا صارت التعمية الحديثة، بفضل خدمات الحاسوب، اختصاصاً تابعا لمجال البحث العمومي - إتفاقة إلى البحث العسكري والأمني - في المعلوماتية النظرية.

ويتفق الخبراء على القول بأن التعمية الحديثة قد برزت بظهور بحث الأستاذين ديفي Diffie وهلمان Hellman عام 1976⁶. وهم يؤكدون أن ظهور الحاسوب قلب المفاهيم الأساسية للتعمية، ذلك أنه وفّر قوة حسابية فائقة لفئة الباحثين، سيما في مجال إزالة التعمية.

ومن العوامل التي طورت التعمية منذ نشأتها حدة "المواجهة" بين فئة الباحثين في مجال حماية المعطيات وولعها في تأمين من القرصنة وبين فئة الباحثين في طرق إزالة التعمية وكسر الحماية. وأدى تطور هذه المواجهة ببعض المسؤولين إلى رفع طابع السرية على الكثير من الخوارزميات المستخدمة.

ومنذ الثمانينيات أصبحت الحاسوبات الشخصية تزداد قوة بحيث صار باستطاعتها استخدام أنظمة تعمية كانت في السابق حكراً للأجهزة العسكرية ... بل انقلبت الأمور اليوم وصارت أفضل خوارزميات التشفير وأفضل أنظمة التعمية تكتشف داخل مخابر الريا^{٢٦}ليات التطبيقية بعيداً عن عيون العسكريين ورجال الأمن الذين تحولوا أحياناً إلى زبائن يشترون برامج التشفير والتعمية من القطاع المدني لسد بعض حاجياتهم.

أما التوقيع الرقمي فيسمح، خلافا للمفتاح العمومية، بتوقيع برقية بصيغة رقمية تماما كما نوقع عقدا أو رسالة عادية. ويستعمل هذا النوع من التوقيع عكس فكرة المفتاح العمومية : إذا كان أحدهم يمتلك مفتاحا خاصة ومفتاحا عمومية فإنه يتم القيام بسلسلة حسابات انطلاقا من المفتاح السرية ومن البرقية التي ستحمل التوقيع فيرفق التوقيع بالبرقية. وسيتمكن مستقبل البرقية من التأكد من التوقيع انطلاقا من المفتاح العمومية ومن التوقيع وذلك حتى يتحقق من أن الأمر يتعلق بالتوقيع المناسب.

ومن جهة أخرى فإن ظهور الإنترنت والبريد الإلكتروني في نهاية القرن العشرين طرح مسائل أمنية عويصة سارع المختصون إلى البحث عن الحلول المناسبة لها من خلال تطوير وسائل التعمية. والسؤال المطروح في هذا السياق هو : هل هناك ^[7]ممانات أمنية عندما نستخدم البريد الإلكتروني، أو الهاتف الخليوي، أو عندما نرسل برقم بطاقة التأمين (التمويل) عبر الإنترنت؟ والواقع يقول إنه لا وجود لضمانات أكيدة في هذا الباب لأن القراصنة قادرون على تحويل تلك المعلومات باستخدام الوسائل التكنولوجية الحديثة وتطور المعلوماتية.

والتعمية تُستخدم أيضا في إبرام الصفقات التجارية والمبادلات البنكية لتأمين مثل هذه العمليات المالية. وقبل ذلك كانت (ولا تزال) معظم الاتصالات بين البنوك خاضعة للتشفير. كما أصبحت الآن التوقيعات الرقمية مقبولة لدى العديد من البنوك، وهو ما يجعل هذا الميدان عرضة لكل المخاطر. ولذا فإنه يحتاج إلى ^[8]لوابط أمنية كبيرة حتى لا يتمكن القراصنة من الاختراق وتحويل الصفقات والأموال إلى غير وجهتها، أو تغيير قيم المبالغ المحولة أو الأمر بتحويل مبالغ بدون علم أصحابها، الخ.

ولذلك فالسعي إلى المزيد من تأمين البطاقات البنكية ونحوها لا زال حثيثا، ولن يتوقف لأن بقدر ما تشدد القيود الأمنية بقدر ما يزيد بحث القراصنة عن اختراقها، فهي في نهاية المطاف معركة دائمة في هذا القطاع بين طرفين، هما : طرف أصحاب البنوك ورجال الأعمال، وطرف القراصنة والمحتالين. والملاحظ أن التعمية "المدنية" ظهرت، شيئا فشيئا، بعد أن تبنت الولايات المتحدة الأمريكية مقياسا تجاريا للتشفير، عام 1977، يمكن أن يكون مرجعا لكل رجال الصناعة وهو مقياس "ديس" (Data Encryption Standard) DES. ولا زال هذا المقياس لم يفقد إلى اليوم أهميته.

إن التحول من الطابع "العسكري" إلى الطابع "المدني" لم يتم دون ظهور مستجدات على صعيد البحث العلمي في مجال التعمية. ففي حقل الصفقات التجارية، لوحظ مثلا وجود معطيات قد لا تعتبر سرية، وهو ما أضاف مهام جديدة للتعمية (قد نكون حريصين مثلا في تعاملنا التجاري على عدم كشف هوية الشريك أو فحوى وثيقة لا غير).

ومن بين المبتكرات الحديثة في البطاقات البنكية أن التعرف على البطاقة ورقمها السري يتم من خلال حسابات تجرى داخل البطاقة ذاتها ولا تجرى داخل النظام المعلوماتي للمؤسسة التي يتعامل معها صاحب البطاقة. وهذا يعني أن البطاقة لا تترك أثرا في أجهزة المؤسسة التي من الجائز أن تخترق من قبل القراصنة ويطل الضرر في تلك الحالة صاحب البطاقة. وهذا ما يزيد في تأمين التعامل بالبطاقات البنكية. وقد قطعت التعمية الحديثة شوطا معتبرا جعلها تهتم حتى بالفنون الجميلة والصور حيث يمكن تشفير صورة موزعة على شبكة الإنترنت. وهذا يساعد مثلا على الكشف عن مهربي اللوحات الفنية ونحوها، وليس فقط عن مبيضي الأموال والمتعاملين معهم.

محطات تاريخية بارزة:

استكمالا للمعلومات التاريخية المقدمة آنفا، نستعرض في ما يلي ملخصا يتبع التسلسل الزمني، ويشير لأبرز المحطات التي عرفها تاريخ التعمية منذ العهود الغابرة حتى نهاية القرن العشرين⁷. ولم نواصل تقديم أحداث القرن الحادي والعشرين لكثرتها وتشعبها، ولأننا سنشير إلى بعض منها في بقية هذا البحث.

* حوالي 1900 قبل الميلاد : كانت هناك كتابات هيروغليفية غير مطابقة للغة المتداولة آنذاك. ولذا اعتبر بعض المؤرخين أنها تمثل أول كتابة معمّاة.

* 1500 قبل الميلاد : هناك لوح من آسيا الصغرى يحتوي على صيغة مشفرة لصنع دهن برّاق لطلاء الأواني الطينية.

* 600-500 قبل الميلاد : مخطوطات عبرية استعملت التشفير.

* 487 قبل الميلاد : استعمل اليونانيون وسيلة في التشفير وفكّ التشفير تتمثل في عصا تُلفّ حولها قطعة من الجلد، ويكتب عليها نص الرسالة. ثم تستخدم هذه القطعة كحزام لحامل الرسالة. وعندما يصل المبعوث إلى الشخص الذي ينبغي أن يقرأ الرسالة يلفها هذا الأخير حول عصا في حوزته فيستخرج المعنى وتصبح الرسالة مقروءة.

* حوالي 150 قبل الميلاد : اكتشاف في اليونان ساعد فيما بعد العديد من المهتمين بمجال التعمية.

* 60-50 قبل الميلاد : استخدم القيصر (100-44 ق.م.) طريقة الإبدال في التعمية فأزاح حروف الأبجدية بمقدار معين في مراسلاته. كما عوّض أحيانا الأحرف اللاتينية بالأحرف اليونانية. وكان هذا كافيا للتعمية في ذلك الوقت، سيما أن الأمية كانت منتشرة بين الناس.

* القرن الثامن الميلادي : دخول العهد العربي الإسلامي والتعمية العربية. ومن أبرز الكتابات فيها كتاب ابن وحشية "الشوق المستهام في معرفة رموز الكلام" وكتاب الكندي الذي يوضح طرق استخراج المعنى، وهو أقدم نص يكتب في هذا الموضع حسب المؤرخين، من بينهم سيمون سينغ Singh Simon. وقد ظل العرب والمسلمون متفوقين على الأوربيين خلال عدة قرون في مجال التعمية.

* 1226م : ظهرت انطلاقا من هذه السنة تعمية ذات طابع سياسي نجدها في أرشيف مدينة البندقية.

* حوالي 1250م : وصف روجيه باكون Roger Bacon عدة طرق للتعمية موضحا "أن الإنسان الذي يعبر عن سر بشكل غير ذلك الذي يحوره لحيولة دون تمكن الآخرين من الإطلاع عليه إنسان مجنون".

* 1379م : قدم غابرييل دي لافيند Gabriel de Lavinde عدة مفاتيح تشفير بسيطة إضافة إلى أبجدية تشفير. ويعتبر عمل دي لافيند أول نموذج لكيفية دام استعمالها قرابة أربعة قرون في أوروبا وأميركا.

* 1392م : لم جوفري شوسر Geoffrey Chaucer إلى أحد كتبه الخاصة بتشغيل آلة فلكية نصوصا توضح بعض قوانين التعمية.

* 1412م : قدم أحمد بن علي القلقشندي (756هـ/1355م-821هـ/1418م) في موسوعته "صبح الأعشى في صناعة الإنشا" المشكلة من 14 جزءا مجمل ما توصل إليه العرب والمسلمين في ذلك الوقت في مجال التعمية. ومما نجد في هذه الموسوعة كيفية إخفاء المعلومات السرية من خلال الحروف.

* 1466م : ابتكر ليون باتيستا ألبرتي Leon Battista Alberti أول طريقة تشفير متعددة الأبجديات. ويبدو أن طريقته في التعمية لم تكسر حتى القرن التاسع عشر. وكانت هذه الطريقة أكثر أماناً من طريقة دي لافيند التي كانت مستعملة بوجه خاص في الشؤون الدبلوماسية. ولم يتم إدخال اختصارات على هذه الطريقة إلا في نهاية القرن التاسع عشر.

* 1474م : ألف سيكو سيمونيتا Sicco Simonetta كتاباً في التعمية "كتاب الشفرة" (Liber Sifrorum) خدمة لدوق ميلانو الإيطالية.

* 1506 : كان جيوفاني سورو Giovanni Soro من أبرز علماء التعمية الأوروبيين. فقد كان مسؤولاً عن التشفير في البندقية بدءاً من عام 1506م. وكان بابا الفاتيكان قد اختبر شفرته لدى سورو فأرسل إليه نصوصاً معبّاة طالباً منه كسر تعميته، فأجاب سورو بأنه لم يتمكن من ذلك. لكن البعض يشكك في صدق سورو ... فلعله ادعى ذلك حتى يواصل الإطلاع على أسرار الفاتيكان.

* 1518 : كتب جون تريثم Jean Trithème أول كتاب مطبوع حول التعمية. وابتكر طريقة تعمية نجد فيها كل حرف ممثلاً بكلمة. كما جاء بتشفير متعدد الأبجديات و[٢٢]حها في جداول.

* حوالي 1550 : ابتكر جيروم كاردان Jérôme Cardan شبكة سميت باسمه. وتستعمل هذه الشبكة التي تظهر فيها نوافذ فارغة وأخرى داكنة كما يلي : يكتب المشفر نصه بشكل طبيعي عبر النوافذ الفارغة، ثم يسحب الشبكة ويملاً الفراغات بنصوص وهمية (أي نصوص عشوائية). وعندما يصل النص إلى صاحبه فما عليه سوى و[٢٣]ع شبكة كاردان على النص فيظهر له النص المفيد دون غيره فيدرك مغزى الرسالة.

* 1553 : ألف جيوفن باتيستا بيلازو Giovan Batista Belaso كتابا أول² فيه طريقة تعمية بالإبدال متعددة الأبجديات. وأدخل عليها عبارة "كلمة السر". ومن المعلوم أن هذه الفكرة تعتبر أساس ما يستعمل حاليا في بعض أنظمة التعمية.

* 1563 م : ألف جيوفاني باتيستا ديلا بورتا Giovanni Battista Della Porta أربعة كتب حول تاريخ التشفير قبل عهده وخلالها. كما تناول فيه المميزات اللغوية التي تساعد على التشفير. والملاحظ أن أفكاره لا زالت معتمدة لحد الآن في مجال التعمية. ومن تلك الأفكار كيفية استبدال حرفين برمز واحد.

* 1578 : ألف مارينس Marins الذي كان أحد موظفي التعمية في جمهورية البندقية كتابه "من عالم استخراج المعنى" (Del mondo di extrazar le cifre).

* 1585 : ألف بليز دي فيجينير Blaise de Vigenère كتابا حول التشفير² منه جدولا مهما في مجال التعمية يحمل اسمه. وقد ساد الاعتقاد بأن طريقته في التعمية يستحيل كسرها. والحقيقة أنها كسرت في نهاية القرن التاسع عشر... وهذا لم يمنع مجلة علمية راقية - وهي مجلة Scientific American - من أن تؤكد عام 1917، أي بعد أزيد من مائة سنة من كسر هذه الشفرة، بأنها "شفرة مستحيلة الكسر".

* 1623 : ابتكر فرنسيس باكون Francis Bacon نظام تعمية جديد. ويعتقد البعض أن هذا الشخص هو في الواقع وليم شكسبير.

* 1691 : أعد أنتوان روسينيول Antoine Rossignol بمعية ابنه مؤلفا سماء "الشفرة الكبرى" (Grand Chiffre) حول التعمية أهداه للملك لويس الرابع

عشر. لكن قراءته كانت صعبة بحيث عجز المختصون عن قراءته حتى نهاية القرن التاسع عشر.

- قبل مواصلة استعراض هذه الومضات التاريخية نشير إلى أن ظهور التقنيات الجديدة خلال المرحلة الموالية في مجال الاتصال (النقل، الصحف، التلغراف، ...) كان حافزا قويا أدى إلى تقدم علم التعمية. كما أن الحروب والصراعات بين الدول دفعت في نفس الاتجاه.

* 1790 : ابتكر تومس جفرسون Thomas Jefferson اسطوانة مشفرة متميزة، مما جعلها تظل مستعملة - رغم التقدم التقني السريع - حتى بعد قرن ونصف من ابتكارها. وبعد أن أهمل هذا الابتكار خلال فترة معينة أعيد إحيائه عام 1891 من قبل الضابط إتيان بازييري Etienne Bazeries الذي حاول بدون جدوى أن يتبناه الجي 2 الفرنسي. والغريب أن الجي 2 الأمريكي قد ابتكر نظاما يكاد يكون مطابقا لاسطوانة جفرسون عام 1922.

* 1854 : كان شارل ويتستون Charles Wheatstone من رواد التلغراف الكهربائي. وقد ابتكر طريقة تعمية متميزة.

* 1857 : بعد وفاة الأميرال فرنسيس بوفور Francis Beaufort نشر أخوه شفرة تحمل اسمه.

* 1854 : قام شارل باباج Charles Babbage بكسر شفرة دي فيجينير، لكن هذا الإنجاز ظل مجهولا لأنه لم ينشر مضمونه. ولم يتم تسليط الضوء عليه إلا في القرن العشرين حين درس المؤرخون مجموعة مؤلفات وبحوث باباج.

* 1861 : نشر فردريك كازس Friedrich Kasiski كتابه "الشفرات وفن التشفير" (Die Geheimshriften und die Dechiffrierkunst) الذي قدّم

أول حلّ عام لمسألة استخراج المعمّي إذا كان النص مشفرا وفق الطريقة المتعددة الأبجديات ذات المفاتيح الدورية. وبذلك أي على كسر شفرة دي فيجينير التي ظلت صامدة خلال عدة قرون.

* 1891 : ابتكر الضابط بازييري (المشار إليه آنفا) اسطوانة تعمية. وكانت هذه الأسطوانة تتكوّن من 20 قرصا يحمل كل منها 25 حرفا. لكن الجي ² الفرنسي لم يستخدم هذه الأسطوانة.

* 1917 : ابتكر جليبر فيرنام Gilbert Vernam، الذي كان يعمل لدى شركة "آي تي تي" AT&T، آلة تشفير متعددة الأبجديات وسهلة الاستعمال. لم يستعمل هذا التشفير عسكريا، لكنه استخدم من قبل الدبلوماسيين الألمان عام 1921.

* 1918 : استعمل الألمان في نهاية الحرب العالمية الأولى نظام التشفير، المسمى ADFGVX، الذي يمثّل في حد ذاته امتدادا لنظام آخر رمز إليه بـ ADFGX. وقد اخترقه أحد الضباط الفرنسيين مبكرا.

* 1919 : قام آرثر شريبوس Arthur Scherbius بتسجيل براءة اختراع آلة التشفير الشهيرة إنigma 8. لكن الثمن الباهظ الذي طلبه صاحبها لم يشجع على استعمالها، علما أن هناك مبتكرين آخرين في بلدان مختلفة كانوا قد عر ²لوا في نفس الفترة آلات مماثلة.

* 1925 : اقترح بوريس هجلين Boris Hagelin للجي ² السويدي الآلة "ب-21" (B-21) التي كانت خلال عقد من الزمن أصغر آلة قادرة على طباعة برقيات مشفرة. وكان الحلفاء قد صنعوا خلال الحرب العالمية الثانية آلة من نفس الطراز تسمى "سي-36" (C-36) في أوروبا و"إم-209" (M-209) في الولايات

المتحدة. وأنتجوا منها 140 ألف نسخة. وبعد الحرب العالمية أسس هجلين في سويسرا شركة تعتبر لحد الآن من أبرز المؤسسات المصنعة لتجهيزات التعمية.

* 1929 : نشر لستر هيل Lester Hill مقاله "التعمية في الأبجدية الجبرية" (Cryptography in an Algebraic Alphabet) الذي يصف فيه طريقة تشفير تحمل الآن اسمه. وهو تشفير متعدد البيانات يستعمل أدوات رياضية مثل الأشعة والمصفوفات.

* 1931 : نشر هربرت ياردلي Herbert Yardley كتابه "الغرفة السوداء الأمريكية" (The American Black Chamber)، الذي يعتبر من أشهر كتب علم التعمية. فقد نجح مثلاً في كسر عدة شفرات، منها شفرات يابانية.

* 1933-1945 : لم تعرف آلة إنigma نجاحاً تجارياً، لكن الألمان تبَنّوها وحسنوها واتخذوها آلة تشفير عسكرية خلال الحرب العالمية الثانية. وقد قام بكسر تشفيرها الرياضي البولندي مريان رجفس Marian Rejewski الذي اعتمد على نص مشفر وقائمة مفاتيح تم الحصول عليها عبر أحد الجواسيس. وكانت البرقيات العسكرية الصادرة خلال الحرب عن إنigma تُفكّ شفرتها في أنكلترا من قبل آلن تورينغ Alan Turing وغوردن ولشمن Gordon Welchman وآخرين، وذلك باستخدام أولى الحواسيب.

* 1940 : نجح وليم فريدمان William Friedman في كسر شفرة آلة تشفير يابانية، وهي آلة "بوربل" PURPLE. ويعتبر فريدمان أب التعمية في أمريكا. وكان يرأس فريقاً يختص في التعمية، كما أنه استعمل هذا العلم لكسر شفرة المهربين خلال فترة تحريم الخمر في أمريكا.



- وبعد بروز الحاسوب خلال السبعينيات وظهور شبكة الإنترنت قفزت التعمية إلى مرحلة راقية بأدوات جديدة، هذه أهم محطاتها :

* 1970 : طور هوست فيستل [Horst Feistel](#) خلال السبعينيات مشروع بحث لدى شركة "آي بي إم" IBM أدى إلى ابتكار شفرة "لوسيفير" Lucifer التي كانت بدورها من وراء ابتكار شفرات متعددة.

* 1976 : نشر ويتفيلد ديفي Whitfield Diffie ومارتن هلمن Martin Hellman بحثا بعنوان "اتجاهات جديدة في التعمية" (New Directions in Cryptography) ادخلا فيه فكرة التعمية بالمفتاح العمومية. وقدّما حلا جديدا لمسألة تبادل المفاتيح السرية.

وفي نفس السنة ظهرت شفرة "معيّار تشفير البيانات" (Data Encryption Standard) المنبثقة عن شفرة لوسيفير. وقد اعتبرت هذه الشفرة صعبة الاختراق إلى درجة أن وزارة الدفاع الأمريكية تبنتها وراقبت في ذات الوقت تصديرها. ومن ثم نالت شهرة واسعة.

* 1977 : ابتكار نظام "آر أس أي" [RSA](#) (وهذه التسمية تمثل الأحرف الأولى لأسماء المبتكرين ريفست وشمير وأدرمان Rivest, Shamir & Adleman). يعمل هذا النظام بالمفتاح العمومية، وهو يسمح بالتأكد من البيانات إضافة إلى تشفير النصوص. وقد ذاع صيته عبر أرجاء العالم في كل الأوساط التي تبحث عن تأمين اتصالاتها.

* 1978 : نشر خوارزمية نظام "آر أس أي" RSA.

* 1990 : نشر مقال لـ كسوجيا لاي Xuejia Lai وجيمس ماسي James Massey يقدم خوارزمية جديدة سميت IDEA (اختصارا لـ International

البيانات". وقد أثبت هذا النظام جدارته حيث لم يتم اختراقه اختراقا كلياً لحد الآن.

* 1990 : نشر شارل بنيت Charles Bennett وجيل براسارد Gilles Brassard نتائجهما التجريبية حول التعمية الكمومية. وهذا نوع من التعمية يستخدم ما يعرف في الفيزياء بالفوتونات. يعتبر هذا الاكتشاف بالغ الأهمية لأنه يوفر سرية الاتصال، كما يكشف عن المخترقين المحتملين. أما عيب التعمية الكمومية فيتمثل في أنها تتطلب وجود واصل من الألياف البصرية بين المتراسلين.

* 1991 : كانت وكالة المخابرات الأمريكية "الآف بي آي" قد تحدثت عن احتمال طلب السماح لها بالنفوذ إلى أية مراسلة في أمريكا فأصدر الباحث فيليب زيمرمن Philip Zimmermann نظام تعمية مجانيا يقي المستخدم من اختراق مراسلاته. وصار هذا النظام بعد ذلك معياراً دولياً.

* 1995 : قام نيكولا جزين Nicolas Gisin بتجربة حول التعمية الكمومية في سويسرا مستعملاً واصلًا من الألياف البصرية طوله 25 كلم.

* 1999 : استطاعت شبكة من الحاسوبات المنتشرة في 11 موقعا داخل ستة بلدان أن تفكك عددا من 155 رقما إلى عوامل أولية. وقد دقّ هذا الحدث ناقوس الخطر لأنه يشكل تهديداً أمنياً على التجارة الإلكترونية في العالم إذ كان استخدام هذا العدد في أنظمة التعمية المعتمدة على شفرة "آر أس أي" RSA وارداً.

* أول يناير 2000 : أحدث الانتقال من القرن العشرين إلى القرن الحادي والعشرين تعطلاً في الأنظمة الأرضية التي تقوم بمعالجة المعلومات المرتبطة بأقمار الجوسسة.

الحاسوب والتعمية:

دعنا نتحدث قليلا في البداية عن الحاسوب بمعزل عن دوره في التعمية. فمن بين الإنجازات الكبرى التي حققتها التقنيات الإلكترونية صناعة جهاز الحاسوب. والحاسوب صنع، في بداية الأمر، لمساعدة الباحث الرياضي في دراسة مسائله الحسابية التي لا يكفيه الوقت لحلها يدويا نظرا لطول العمليات فيها. وعلى هذا الأساس قدّر أحد الرّيا [2]لين في نهاية الأربعينات أن الولايات المتحدة الأمريكية سوف لن تحتاج إلى أكثر من ثلاثة أو أربعة أجهزة حاسوب لتغطية كافة حاجياتها المستقبلية! وكم هو عدد هذه الأجهزة الآن في أمريكا والعالم؟ إنه يعدّ بالملايين!

وفيما يخصّ مجال الرّيا [2]ليات بالذات، يخطر الكثير من الناس في التصور أن الحاسوب هو الآن قادر على حل جميع (أو جلّ) المسائل التي يبحث فيها الرّيا [2]يون. ورغم كثرة استعمال هذا الجهاز لدى الباحثين في الرّيا [2]ليات فإن المسائل التي يحلها الحاسوب في هذا الحقل لا يساوي عددها شيئا بالمقارنة مع عدد المسائل التي يحلها الرّيا [2]ليون بدون تدخل الحاسوب!

وفي الفروع العلمية الأخرى، مثل الفيزياء والكيمياء والجيولوجيا والهندسة ...، فإن الحاسوب أصبح من الأدوات العادية التي يستخدمها يوميا العاملون في هذه الميادين، وهذا رغم أن عمر الحاسوب حوالي نصف قرن. ولم يقتصر هذا الجهاز على التدخل في الاختصاصات العلمية فحسب بل نجده يصلح ويحول في العلوم الإنسانية والاجتماعية، وفي الطب والصيدلية والاقتصاد، وفي اللسانيات وعلم النفس ... والباحث اليتيم، اليوم، هو ذلك الباحث الذي يشتغل دون حاسوب بجانبه مهما كان مجال اختصاصه.

وكان أول حاسوب يزن أكثر من ثلاثين طنا وينجز حوالي 5000 عملية في الثانية. واستطاع الجيل الثاني من الأجهزة أن يرفع عدد العمليات إلى 200.000 عملية في الثانية. وعندما وصل الجيل الثالث تضاعف هذا العدد عشر مرات. وأما الجيل الرابع فبإمكانه إنجاز مئة مليون عملية في الثانية ... وكل جيل جديد يأتي لنا بمضاعفة هذا العدد آلاف المرات.

لقد أصبح، اليوم، عدد أجهزة الحاسوب المستعملة في مختلف القطاعات مقياسا لتقدم الدول وميزانا لقدراتها. وفي حين كان الحاسوب يستخدم للسرعة في إجراء عمليات حسابية بسيطة صار يقدم العديد من الخدمات الأخرى. ويمكن تلخيص مهامه الحالية في ثلاثة محاور، والملاحظ أن كلاً منها يدعم تطوير التعمية دعماً أكيداً:

1. إنشاء أنظمة بحث جديدة ومعالجة المعلومات من أجل كسب سرعة أكبر والتوصل إلى ابتكار تقنيات جديدة. كما أن تجميع المعلومات في ما يسمى ببنوك المعلومات يسمح بالاستعمال الأمثل للحلول التقنية المتوفرة.

2. إنشاء أنظمة اتصال قادرة على توصيل جملة كبيرة من المعلومات (مثل شبكة الأنترنت والشبكات الداخلية "الأنترانت")، إذ أن الاستعمال المكثف للحاسوب في العالم طرح مسألة «الاتصال». وهناك بحوث جارية منذ سنوات من أجل تطوير الاتصال بين الإنسان والحاسوب، ليس كتابياً فحسب بل صوتياً أيضاً. وهذا الأمر بالغ الأهمية لأنه يسمح للشخص المراقب في المصنع، مثلاً، أن يصدر أوامره شفويًا للحاسوب خلال عملية الإنتاج قصد إجراء تعديل سريع أو تدارك خطأ آني. كما يتيح للطبيب الجراح تتبع عملية جراحية يقوم بها الحاسوب مع إمكانية إعطاء أوامر شفوية (حتى عن بعد) خلال إجراء العملية



فينفذها الجهاز الجراح فوراً، وقس على ذلك إذا ما فكرت في عمليات أمنية محضة يقوم بها الجيـ [٢] أو رجال الأمن.

3. « تأليل » المراقبة وتصميم نماذج رياضية. وسنهتم هنا بجانب من جوانب تصميم النماذج.

وخلاصة القول إن تطوير الحواسيب سمح لعلم التعمية بالابتعاد عن المعالجات التقليدية المرتبطة باللغات المتداولة : فالرسالة أو البرقية في مفهوم التعمية الحاسوبية ليست سوى سلسلة من الأرقام المتكونة من الرقمين 0 ، 1 .

الأعداد والتعمية:

يقوم مبدأ المفتاح العمومية على خواص الأعداد الطبيعية. من لا يعرف تلك الأعداد التي لا تقبل القسمة على عدد سوى على 1 وعلى نفسها؟ إنها الأعداد الأولية، وهي : 2 ، 3 ، 5 ، 7 ، 11 ، 13 ، 17 ، 19 ، 23 ، ...

يعلم الرياضيون من قديم الزمان أن قائمة هذه الأعداد غير منتهية. ويتساءل تلاميذنا دائماً لماذا يطلب منهم، في التمارين الحسابية، تفكيك عدد طبيعي إلى عوامل أولية مثل : $15 = 3 \times 5$ ، $36 = 2 \times 2 \times 3 \times 3$ ، $38 = 2 \times 19$. إنهم لا يعلمون أن فكرة تفكيك الأعداد الطبيعية إلى عوامل أولية هي أساس المفتاح العمومية في التعمية ! بل إن دراسة خواص هذه الأعداد تعمقت منذ 1980 بعد أن تم اكتشاف دورها الفعال في تقنيات التعمية. وهكذا ندرك مرة أخرى أن الرياضيات الأكثر تجريداً يمكنها أن تكون أساساً لتطبيقات ملموسة.

كيف يتم استعمال هذه الأعداد في التعمية؟ من المعلوم أنه كلما كان العدد الطبيعي كبيراً كلما صعب تفكيكه إلى عوامل أولية. تصوّر مثلاً أنك

سئلت عن تفكيك عدد طبيعي يبلغ عدد أرقامه 1500 رقم. نحن نستطيع عادة القيام بهذه العملية اعتمادا على الطرق التقليدية، مستنجرين بالحاسوب إذا كان عدد أرقام العدد المطلوب لا يتجاوز كثيرا 15 رقما. وباستعمال وسائل [خمة] مثل استخدام آلاف الحاسوبات، المنتشرة عبر العالم والمتراطة فيما بينها من خلال شبكة الإنترنت، وعبر شبكات داخلية مؤمنة، تمكن الريا [يون] منذ بضع سنوات من تفكيك عدد صعب المعالجة يبلغ عدد أرقامه 129 رقما. ولذلك فإن مسألة تفكيك الأعداد الكبيرة تمثل بالنسبة للمختصين في نظرية الأعداد تحديا حقيقيا.

تعتمد فكرة استخدام الأعداد الأولية في مجال التعمية - وبصفة خاصة في المراسلة بواسطة المفتاح العمومية - على ملاحظتين:

- إنه من السهل إيجاد عددين أوليين كبيرين أ ، ب ثم حساب جدائهما $J = A \times B$.

- إنه من الصعب جدا اتباع المسلك المعاكس، أي تحديد العددين أ ، ب انطلاقا من معرفتنا للعدد الكبير ج. هذه الصعوبة، بل هذه "الاستحالة" العملية، هي التي تضمن استحالة استخراج المعنى في المراسلات بالمفتاح العمومية من طرف الجواسيس حتى ولو علموا بقيمة العدد ج.

لا بد من أن نشير في هذا السياق، بخصوص الأعداد الأولية، إلى أن دور نظرية الأعداد في مجال التعمية يطرح أمام الريا [يين] قضايا تخص أدبيات مهنتهم. فعلى سبيل المثال، إذا اكتشف أحدهم طريقة أكثر فعالية من الطرق السابقة، تمكن من تفكيك الأعداد الطبيعية إلى عوامل أولية، ماذا عليه أن يفعل؟ هل يبعث بها إلى أعلى سلطة في البلاد أو يعر [لها] أمام الجمهور في ندوة

عالمية حتى لا يستغلها أحد [٢] الآخرين؟ أو يبيعها إلى من يدفع أكثر؟! ذلك جزء من بعض التساؤلات التي يطرحها تطور علم التعمية على الباحثين في هذا الحقل.

التعمية العسكرية:

ما من شك أن التعمية وسيلة قوية لدعم الأمن العسكري وجهده خلال الحروب، في الدفاع وفي الهجوم. وقد كانت التعمية تعنى في البداية بالاتصالات على مستويات معينة بين القادة. ولذلك كانت تدرّس قديما في بعض الكليات، سيما العسكرية لدى الإغريق، وكانت محلّ تقدير رفيع لدى قادة الجيوش في العصور الغابرة.

وقد تخيّل العسكريون في الماضي، وابتكروا طرقا مختلفة كي تصل الأوامر السرية للقادة إلى أبعد الحدود وتحفظ تعليماتهم وتكون في مأمن من استخبارات الأعداء. ويذكر المؤرخون أن الإقدام على استخدام حروف أو رموز سرية يعتبر في المحاكم الإنكليزية أمرا لا يخفف العقوبات بل يزيد في ثقلها، وظل الأمر كذلك حتى القرن السابع عشر.

كما أن الملك الفرنسي هنري الرابع (1553م-1610م) قد اخترق بعض الرسائل المشفرة كانت موجهة إلى الحكومة الأسبانية في عهده فأمر الرياضي الشهير فيات Viète بالبحث عن كيفية كسر شفرتها. وتمكن فيات من تلبية طلب الملك، وهو ما أتاح التعرف على نوايا الأعداء خلال سنتين كاملتين.

أما في عهد الدوق الفرنسي ريشليو Richelieu (1585م-1642م) فكان فنّ فكّ تشفير الكتابات السرية قد بلغ درجة عالية حتى اعتبر علما ينبغي على الحكومات الاعتناء به. وكانت لوزارة الشؤون الخارجية آنذاك كلية يدرّس فيها هذا الفن. وتواصل هذا الاهتمام بالتعمية على أكثر من صعيد، سيما العسكري.

وعلى الرغم من أن مؤرخي تلك الحقبة (القرن 16م) لم يعثروا على آثار مراسلات عسكرية استعملت فيها التعمية فإنهم واثقون بأن الأوامر الموجهة لقادة الجيوش على جبهات القتال في القرن الثامن عشر كانت لا ترسل إلا لمن نصوص مشفرة.

ثم أصبحت المراسلات المشفرة أكثر استعمالاً بين العسكريين. فالمؤرخون⁹ يؤكدون أن في عهد نابليون الأول (1769-1821) كان الإمبراطور يشفر مراسلاته خلال الحرب¹⁰ لد روسيا في بداية القرن التاسع عشر. وفي الحرب الأسبانية كان أحد الأسبانيين قد عثر على مفتاح شفرة سهّل مهمّة بلده في استعادة بعض أرا¹¹ ليها. ومن المعلوم أن استعمال التعمية قد عم لدى قادة الجيوش الأوروبية قبل نهاية القرن التاسع عشر.

وفي نهاية القرن التاسع عشر كان العسكريون الألمان يعتبرون أن المراسلات المشفرة ينبغي أن تعمم على جميع المستويات في الجي¹². وهكذا كانت البرامج المقررة في كلياتهم العسكرية تتضمن دروساً وتدريباً على كتابة النصوص المشفرة وقراءة المراسلات المشفرة. بل تتطلب تلك البرامج إلمام الطالب بالمبادئ النظرية لفنّ التشفير. أما في الجي¹³ الفرنسي فالملزمون آنذاك باستخدام التشفير في المراسلات هم كبار القادة. وكانت المساعي جارية لبلو ز ما بلغه الألمان في هذا المجال، وكذا التمكن من التراسل باستعمال التعمية على كل المستويات في زمن الحرب كما في زمن السلم. وكان القادة العسكريون يرون بأنه لا بد من تدريب الضبا ر على استعمال الشفرة خلال زمن السلم لأن ذلك غير ممكن خلال الحروب.

غير أن امتلاك شفرة خاصة بالمراسلات السرية ليس كافياً إذ من الضروري أن يضمن درجة مقبولة من السرية وعدم الاختراق. وهذه هي نقطة¹⁴ لعف أنظمة التشفير عموماً. ويروى مثلاً خلال الحرب التركية الروسية

(1877-1878) أن السلطات الفرنسية استلمت ذات يوم من أحد ملحقها العسكريين المتابعين لهذه الحرب برقية مشفرة. لكن مسؤول مكتب التشفير كان غائباً فـ [7]طر الوزير الذي كان يجهل مفتاح التشفير إلى اللجوء لأحد الضباط ليحاول فك شفرة البرقية. وقد تمكن الضابط من ذلك بعد بضع ساعات، وهذا يدل على هشاشة التشفير المستخدم.

ثم ازدادت التعمية العسكرية أهمية في الحروب منذ مطلع القرن العشرين، حتى أن الخبراء وصفوا كلا من الحربين العالميتين الأولى والثانية بأنهما كانتا "حرباً تعمية". ولعل أبلغ دليل على ذلك قرار حكومة تشرشل خلال الحرب العالمية الثانية بخصوص المعارك التي دارت رحاها في صحراء شمال إفريقيا المتمثل في ترك الألمان يدمرون قاعدة عسكرية بريطانية بأكملها رغم علم تشرشل بتفاصيل الخطة الألمانية وتوقيتها عن طريق كسر تعمية الألمان وقراءة رسائلهم. وهكذا [7]لحقى البريطانيون بقاعدة من قواعدهم حتى لا يكتشف الألمان بأن الحلفاء تمكنوا من كسر شفرتهم.

وعلى كل حال فإن القادة العسكريين كانوا واعين منذ القرن التاسع عشر بضرورة التمييز بين نظام كتابة مشفرة و [7]لعه صاحبه من أجل تبادل ظرفي لرسائل بين أشخاص منعزلين، وبين طريقة تعمية تهدف إلى و [7]لعه قواعد لمدة زمنية غير محدودة تضمن سرية التواصل بين قادة الجي [7]. ذلك أن هؤلاء القياديين لا يستطيعون تغيير شفرتهم بكل حرية في أي وقت. ثم إنهم مطالبون دائماً بعدم حمل أشياء أو كتابات تتضمن معلومات تفيد العدو حول المراسلات السرية. لذلك فنظام التعمية، كما كانت تراه في الماضي القيادات العسكرية، لا بد أن تتوفر فيه بعض الشروط الأساسية منها:

1- يجب أن يكون النظام منيعاً من الناحية الأمنية حتى لا يخترق، أو يخترق بصعوبة كبيرة.

2- ينبغي ألا يشكل خطراً حتى لو سقط في أيدي العدو.

3- يجب ألا يتطلب تبليغ مفتاح الشفرة أو تذكرها نصوصاً مكتوبة. كما يجب أن يتمكن مستعملوها بتغييرها عند الحاجة.

4- يجب ألا يتطلب تشغيله اللجوء إلى عدة أشخاص.

5- يجب أن يكون استعمال هذا النظام يسيراً، وألا يتطلب جهداً فكرياً مركزاً.

والواقع أن هناك أسراراً عسكرية (أو غير عسكرية) لا يهم أن تعرف بعد وقت معين (ساعات أو أيام) كأن تكون حاملة لخبر هجوم مرتقب بعد ساعات، بينما تتطلب معلومات أخرى أن تظل سرية خلال سنوات عديدة. ولذا وجب التمييز بين أنواع الأسرار. ففي الحالة الأولى يكفي لنظام التعمية ألا يتمكن العدو من فك شفرته قبل ساعات .. لكن هناك من يعارض هذه الفكرة ويبرر معارضة²ته بافتراض أن هناك رسالتين تحملان معلومتين وشفرة بنفس الطريقة، وتم إرسالهما الواحدة تلو الأخرى، وقد استطاع العدو الحصول عليهما وقضى وقتاً في فك الشفرة الأولى وفاته اعتراض مفعولها. لكنه سوف ينجح في التصدي لمفعول الرسالة الثانية لأن فك الشفرة الأولى سيسمح له بفك الشفرة الثانية في لحظات.

تلك هي بعض انشغالات التعمية العسكرية قصدنا من خلال استعرا³ها الإشارة إلى تنوع الرنى والاستعمالات عبر العصور.

الجوسسة والتعمية

حتى تتضح لدينا أهمية التعمية بشتى أنواعها وفي كل المجالات، نقدم فيما يلي نموذجين من الهيئات الأمنية التي تعمل في مجال الجوسسة العسكرية

وغير العسكرية، هما "مركز أمن الاتصالات" 10 في كندا وشبكة إشلون Echelon العالمية 11. وقد اخترنا هذين الجهازين لكون حقل انشغالهما تجاوز التوقعات، ووصل حدود التجسس الاقتصادي والتجاري على الأصدقاء والحلفاء.

النموذج الأول : مركز أمن الاتصالات الكندي

تسعى بعض الدول سعيًا منقطع النظير من أجل حماية مجمل الاتصالات التي تحمل طابعًا سريًا (عسكريًا، حكوميًا، اقتصاديًا، ...) كما سنرى ذلك في حالة كندا. هناك في كندا مركز قومي يسمى "مركز أمن الاتصالات" مهمته الإشراف على التعمية في كندا بهدف دعم الحكومة ومختلف هيئاتها في هذا المجال بما في ذلك أجهزة الاستخبارات. كما يقدم خدمات تضمن أمن المعلومات والاتصالات الإلكترونية. أما شعار المركز فهو "الحفاظ على أمن كندا عبر تفوقها في مجال الاتصال"، وهو يوظف في مقره المركزي بالعاصمة الكندية نحو 1500 موظف.

وقد رأى هذا المركز النور منذ بداية الحرب العالمية الثانية. وكان قد تمكن خلال تلك الحرب من اختراق رسائل عديدة ذات صلة بالاستعلامات العسكرية الألمانية في أمريكا الجنوبية وفك شفرتها. كما استهدف المركز مصالح البحرية والسلك الدبلوماسي لحكومة فينلاند الفرنسية (حليفة هتلر آنذاك).

وبعد أن وقعت الحرب العالمية أوزارها درست السلطات الكندية مدى فائدة الإبقاء على هذا المركز. ومما أقنع الحكومة بأهمية الحفاظ عليه حينذاك تصريحات خبير التعمية السوفييتي الشهير إغور غوزنكو Igor Gouzenko التي أكد فيها وجود خلايا تجسس سوفيتية نشطة في كندا. وفي 1947 أصبح أمن

الاتصالات في كندا أحد الأهداف الرئيسية للمركز. وصار اسمه "مديرية الاتصالات لدى المجلس القومي للبحوث". وبعد ذلك نشط المركز وربط علاقات وطيدة مع الولايات المتحدة وبريطانيا وأستراليا وزلندا الجديدة، وعاد التعاون بين جميع هذه الهيئات إلى ما كان عليه خلال الحرب العالمية، بل زادت وتيرته وصارت تلك الدول تتقاسم الكثير من المعلومات الأمنية والدبلوماسية والتجارية. ثم تدعم أكثر فأكثر نشا ر هذا التعاون بوسائل تقنية وتكنولوجية إبان الحرب الباردة بين المعسكرين الشرقي والغربي، وتواصل أيضا بعد تلك الفترة.

وقد أعادت الحكومة الكندية عام 1974 الاسم القديم للمركز بدل "مديرية الاتصالات لدى المجلس القومي للبحوث". حدث هذا التغيير في التسمية إثر حصة تلفزيونية بثتها قناة أمريكية كشفت فيها عن الدور التجسسي لهذه المديرية. لكن المركز ظل يقوم بمهمته الأولى ولم يحد عنها.

وبعد سقوط حائط برلين عام 1989، وانهار المعسكر الشرقي تقشفت الحكومة الكندية في ميزانية المركز وقلصت عدد موظفيه، وهو ما أثر في أدائه التجسسي خلال التسعينيات. لكن تلك الحقبة عرفت ثورة عارمة في مجال تكنولوجيات الاتصالات وتنوعت وسائلها بسرعة مدهشة، سيما بعد ظهور شبكة الأنترنت. ثم جاءت أحداث 11 سبتمبر 2001 في نيويورك وما تلاها من تداعيات. وهكذا أعيد الاعتبار للمركز في ديسمبر 2001 وخولت له صلاحيات واسعة لضمان أمن تكنولوجيات الاتصالات والمضي قدما في تطوير أنظمة التعمية في كندا.

ويعلن المركز لآاحة بأنه يسعى إلى التحكم في البنية القاعدية العالمية للاتصالات، وهو مجال بالغ التعقيد، ويشكل في نظر المركز أكبر خطر على البلاد. وعلى سبيل المثال يقوم المركز بجمع المعلومات حيثما وجدت، سيما تلك

التي تفيد الحكومة في باب التوجهات الاستراتيجية واتخاذ القرارات الحاسمة والتقييم اليومي لوسائل ونوايا الدول الأخرى. ويرجع نجاح المركز في هذه المهمة إلى تحكمه في أبرز تكنولوجيات البنية القاعدية العالمية لمجال الاتصالات ... وفي ذلك تعاون كبير مع الدول الأربع المشار إليها آنفا.

وبعد أن كان الاتحاد السوفييتي هو محط نظر المركز خلال الحرب الباردة تحول اهتمامه إلى قطاعات أخرى تَمَسُّ السياسة والصناعة والاقتصاد والتجارة وأمن الكنديين في الداخل والخارج، سيما من ظاهرة الإرهاب. وقد تطلّب منه ذلك توظيف عدد كبير من محلي المعلومات والمختصين في مختلف اللغات والمترجمين ومحرري التقارير والمهندسين المصممين للبرمجيات ومختبرين للتكنولوجيات الحديثة في مجال الاتصال والتعمية. وهكذا وظّف المركز ربا²لين لتطبيق الريا²ليات في مجال التعمية وفي قطاعات أخرى مرتبطة بتكنولوجيات الاتصالات. كما وظّف معلوماتيين ومبرمجين لتطوير أنظمة وبرمجيات تعنى بمجالات عملية مختلفة : أمن المعلومات، استخراج المعمى، الدعم التقني، القطاعات المرتبطة بالاتصالات.

وغطى المركز أيضا حاجياته من الفيزيائيين للبحث في مجال تطوير الرادارات والاتصالات وتحليل الإشارات الرقمية. ويشمل حقل بحوث هؤلاء الفيزيائيين أمن مختلف الاتصالات الحكومية وسبل إيجاد طرق جديدة لاكتساب المزيد من المعطيات والتحليل اعتمادا على الأدوات المعلوماتية والتجهيزات التكنولوجية الراقية. وامتدت حاجة المركز إلى الإداريين والمختصين في الصيانة بمختلف أنواعها، وكذا الشؤون المالية والمحاسبية وتسيير المنشآت، والمخططين ومسيري المشاريع، والمختصين في مجال الاتصال وفي الموارد البشرية.

وهكذا نرى بأن المركز الكندي لم يغفل أي قطاع وأنه لا يتوانى في التجسس على كافة المشاريع، وقد تزود بكل الوسائل التكنولوجية الحديثة والموارد البشرية اللازمة من علماء وباحثين وتقنيين وإداريين كي يكون رائداً في مجال التعمية حرصاً منه على أمن الاتصالات مهما كانت طبيعتها. فكيف لا يكون هذا المركز نموذجاً يحتذى به في بلدان أخرى؟

النموذج الثاني : شبكة التنصت العالمية "إشلون"

إشلون شبكة تجسس أمريكية الأصل، لكنها توسعت فيما بعد إلى أربعة بلدان أخرى، وهي تقوم بمراقبة كافة الاتصالات العالمية من مكالمات هاتفية أرّاقية ونقالة، ورسائل عبر الفاكس وبريد إلكتروني. وهناك حسب تقديرات صحفية حوالي 175 محطة تنصت رئيسية أمريكية منتشرة في نحو 140 دولة، غير أنها لا تنتمي بالضرورة كلها إلى إشلون. وهذا دون الإشارة إلى المحطات التقليدية مثل السفارات والقنصليات والمحطات والأقمار الصناعية المتحركة بحراً وجواً.

تستطيع شبكة إشلون تحليل مليوني مكالمة في الدقيقة الواحدة. وهي تقوم باختراق نحو 4.3 مليار اتصال يوميا، وهذا يعادل تقريبا نصف الاتصالات اليومية عبر العالم المقدرة بـ 10 ملايين اتصال. ومن المعلوم أن هذه الشبكة التنصتية تقوم بمهامها آليا، ولا تبلغ الجهات المعنية إلا بالاتصالات التي تتضمن كلمات مفتاحية معينة سبق تزويد الشبكة بها. ولا تخضع لاطلاع الفعلي المباشر (قراءة النصوص أو الاستماع إلى الأصوات أو مشاهدة الصور المسجلة عبر الشبكة) من قبل الأشخاص المكلفين بالمراقبة إلا التسجيلات التي تتضمن تلك الكلمات المفتاحية. وبعد ذلك يقوم المراقبون الأمنيون بعملية

انتقاء على مستوى المعطيات المتوفرة، ويرسلونها إلى الحكومة الأمريكية. ومن ثم ترسل المعلومات إلى الجهات المعنية في الداخل والخارج، من مصالح أمنية ودبلوماسية وعسكرية وخاصة، دون أن ندرك المؤسسات الاقتصادية والتجارية.

وقد جندت الشبكة نحو 120 قمرا اصطناعيا تجسسيا وعدة غواصات لاختراق البرقيات والرسائل التي تنقلها الأقمار الاصطناعية والكوابل في قاع المحيطات والبحار (حيث تلصق تجهيزات إلكترونية على تلك الكوابل في أماكن محددة داخل الماء لتلتقط الحقول المغناطيسية المارة في تلك الكوابل ثم ترسل تلقائيا إلى الجهات المختصة).

إليك بعض المحطات التاريخية تعرفنا بنشأة هذه الشبكة العالمية السرية:

* 1948/1947 : تمديد صلاحية الميثاق المعروف باسم يوكوزا UKUSA (هذا الاسم مركب من UK وUSA، وهما الرمزان اللذان يدلان على المملكة المتحدة والولايات المتحدة الأمريكية). وقد وقّع هذا الميثاق السري خلال الحرب العالمية الثانية بين الولايات المتحدة وبريطانيا، وكان يهدف إلى تنظيم التعاون بين مصالح الاستخبارات بين البلدين في مجال الجوسسة على الاتصالات وتبادل المعلومات. وبعد ذلك انضمت إلى هذا الميثاق كندا 12 وأستراليا وزلندا الجديدة. وكان الهدف الرئيسي لهذه الشبكة آنذاك هو الاتحاد السوفيتي والمعسكر الاشتراكي.

* 1952 : إنشاء وكالة الأمن القومي National Security Agency في الولايات المتحدة [٢]من هيئة المخابرات الأمريكية لتختص في التجسس الكهرومغناطيسي (أي الاتصالات عبر الراديو والرادار والاتصالات الهاتفية ونحوها)، والعمل على تصميم أنظمة تعمية تضمن سرية الاتصالات الحكومية والدبلوماسية والعسكرية الأمريكية. والوكالة تستخدم في أمريكا وحدها

نحو 4000 موظف يعالجون المعلومات المخترقة بواسطة شبكة من أقوى الحواسيب، وميزانيتها تقدر بنحو 4 ملايين دولار.

* 1966 : تولت وكالة الأمن القومي الأمريكية التحكم في قاعدة منويد هيل Menwith Hill بشمال أنكلترا، وكانت القاعدة قبل هذا التاريخ تحت رقابة الجي ٢ الأمريري ر فصار ت أ ٢ خم محطة اختراق للاتصالات في العالم.

* 1987/1985 : قيام مشروع إنشاء شبكة عالمية لمراقبة الاتصالات كشف عنه الصحفي دونكن كمبل Duncan Campbell. أما فكرة المشروع فتتمثل في ربط قواعد اختراق المعلومات التي نشرها أعضاء ميثاق يوكوزا في مختلف بلدان العالم (عبر حواسيب قوية). هذا المشروع هو مشروع إشلون.

* 1989 : أدى سقوط جدار برلين إلى إعادة النظر في المهام الإستراتيجية للولايات المتحدة. فصار غزو الأسواق الاقتصادية والتجارية العالمية هو الهدف الأول، واندرجت هذه الأولوية في عمل مشروع إشلون.

* 1996 : كشف الخبير النيوزلندي نيك هيجر Nicky Hager في كتابه "السلطة السرية" (Secret power) عن وجود أكبر شبكة تجسس حول الاتصالات في العالم، وذكر أنها سميت إشلون.

* 1998 : أكدت دراسة قام بها البرلمان الأوروبي على وجود مخاطر يتسبب فيها نشا ر هذه الشبكة على بلدان الاتحاد الأوروبي ومؤسساته. وفي نفس السنة قامت وكالة الأمن القومي الأمريكية بإحالة عدد كبير من موظفيها على المعاش المسبق حتى يتم توظيفهم في الشركات الخاصة، وتستغلهم كعملاء للوكالة. وفي نفس الوقت قامت الوكالة بتوظيف عدد معتبر من المواهب الشابة.

* 1999 : قدم البيت الأبيض برنامج تصميم حواسيب المهدف منه حل مسألة التعمية والسرعة في معالجة الاتصالات المخترقة، على أن ينجز المشروع عام 2004.

وقد عبرت لجنة برلمانية أوروبية سميت لجنة "أنظمة المراقبة والاختراق الإلكتروني التي يمكن أن تعرض الأمن القومي للخطر" عام 2000 عن مدى جهل الدوائر السياسية الأوروبية بالرهانات الجديدة في مجال الاختراق الإلكتروني. وقضت هذه اللجنة سبعة أعوام في أداء مهمتها لتصل إلى ما وصل إليه المختصون منذ سنين. وطالب أعضائها باتخاذ سلسلة إجراءات من شأنها تحرير التعمية والحفاظ على أمن المواطن الأوروبي كما هو الحال في الولايات المتحدة.

وما يزعج الأوروبيين بوجه خاص في هذا الباب هو أن الجوسسة التي راحوا [7]لحيتها من طرف حلفائهم لم تكتف بالاتصالات المختلفة (سيما ذات الطابع العسكري) بل ذهبت إلى أبعد من ذلك وصارت تهتم بالجانب الصناعي والاقتصادي والتجاري. ثم إن شبكة إشلون لا تقوم بنقل تلك المعلومات إلى سلطات الولايات المتحدة وحدها بل تنقلها إلى حلفاء آخرين (دول ومؤسسات). وقد ثبت لدى الأوروبيين أن مؤسسات أوروبية لم تفز بصفقات تجارية دولية في مجالات عديدة (كالطيران والرادارات) بسبب العمل التجسسي لإشلون وفازت بها مؤسسات أمريكية.

وهكذا عبّر المتحدث باسم اللجنة الأوروبية عن قلقه، كما وصفت رئيسة البرلمان الأوروبي آنذاك قضية إشلون بالفضيحة. أما وزير الخارجية البلجيكي فكان أكثر حدة حين اعتبر الو [7]لع غير مقبول وهدد باستخلاص "ما ينبغي استخلاصه في مجال السياسة الخارجية". كما طالب وزير فرنسي سابق بتنصيب لجنة تحقيق أوروبية حول المو [7]لوع. وقد أدت مثل هذه التصريحات

برئيس الحكومة البريطاني الأسبق توني بلير إلى التأكيد بأن بلده لم يسبق له أن خان حلفاء الأوروبيين بتعاونه مع الولايات المتحدة.

وتؤكد وكالة الأمن القومي الأمريكية أن لا يعينها من وراء المعلومات المستقاة سوى أمن المواطن الأميركي. غير أن الأوروبيين يشككون في هذا القول ويعتقدون أن الوكالة تقوم عبر شبكة إشلون بعملية جوسسة اقتصادية وصناعية لصالح الولايات المتحدة وغيرها من الحلفاء المقربين، كما أنها تخترق الاتصالات الخاصة الأوروبية.

والواقع أن شبكة إشلون لم تزعج الأوروبيين وحدهم بل أقلقّت أيضاً اليابانيين. فقد جاء في الصحافة اليابانية أن نظام إشلون راقب خلال عشرين سنة المكالمات الهاتفية للدبلوماسيين اليابانيين. كما تقوم إشلون بمراقبة العديد من الجمعيات غير الحكومية، مثل الصليب الأحمر الدولي وجمعيات الخضر (كمنظمة "غرينيس")، ومنظمة العفو الدولية، الخ.

ومما زاد في تخوفات الأوروبيين أن لجنة التحقيق الأوروبية في موفوع إشلون كانت قد طلبت مقابلة المسؤولين في وكالة الأمن القومي الأمريكية التي كانت من وراء نشا ر إشلون. لكن الوكالة رفضت الطلب. كما ألغيت معظم اللقاءات الأخرى التي كانت مبرمجة مع مسؤولين أمريكيين. زد على ذلك أن بريطانيا تنتسب في آن واحد إلى الاتحاد الأوروبي وإلى شبكة إشلون.

ولنقدم أدلة وقرائن وأحداث ذات علاقة بشبكة إشلون تدعم الشكوك والتخوفات الأوروبية في المهام الحقيقية لشبكة إشلون :

1. لقد قام الصحفي البريطاني دونكن كمبل - المختص في المسائل المرتبطة باستخدام التكنولوجيات الحديثة في مجال الاستخبارات - بتحقيق حول

شبكة إشلون فتبين أنها تخترق يوميا كل الاتصالات الإلكترونية والهاتفية والمراسلات عبر الفاكس في أوروبا، وذلك من خلال أقمار تجسسية ومحطات أر[ق]لية تابعة للشبكة موزعة في الولايات المتحدة وبريطانيا وكندا وأستراليا وزلندا الجديدة وبلدان أخرى كثيرة.

ويضيف الصحفي أن هناك ما يثبت أن بعض تجهيزات إشلون تستهدف القطاع التجاري وليس العسكري. وذكر بعض المؤسسات الاقتصادية التي كانت محل اهتمام الجوسسة الصناعية من قبل إشلون خلال السنوات الأخيرة، منها شركة تصنيع الطائرات الأوروبية إيربوس Airbus ومؤسسة الصناعة الإلكترونية الفرنسية تومسون Thomson (التي فقدت صفقة تقدر بنحو مليار ونصف مليار دولار). ويبدو أن طريقة عمل الوكالة في هذا الباب، وهي تهتم بكل ما يبرم من عقود تجارية في مجال صناعة الطيران والأقمار الاصطناعية، أنها مثلا تزود شركة بوينغ بمعلومات عندما تعتبر الوكالة أن تلك المعلومات تفيد الشركة.

2. 1990 : اختراق الاتصالات بين مؤسسة يابانية تختص في صناعة الأقمار الاصطناعية وأندنوسيا حول إبرام صفقة بمئات ملايين الدولارات. وقد تدخل الرئيس بوش الأب شخصا لتقتسم الصفقة المذكورة بين اليابانيين والأمريكيين. وفي نفس السنة دشنت الصين المقرر الجديد لسفارتها بأستراليا، فتم اكتشاف أن خلال تشييد هذا المقرر قام رجال أمن أمريكيون بول[ق]ع تجهيزات مجهرية تجسسية متعددة وأنظمة مراقبة الاتصالات في جل جدران مبنى العمارة. وكانت الاتصالات المسجلة تتجه تلقائيا عبر أقمار إشلون إلى مركز الوكالة بالولايات المتحدة.

3. 1991 : مصادرة 12 طنا من الكوكايين بفضل اختراق الاتصالات التي تتم بين بارونات المخدرات في أمريكا اللاتينية.

4. 1992-1993 : التجسس على اتصالات السلطات المكسيكية عندما كانت تتفاوض مع الولايات المتحدة وكندا حول اتفاق التبادل الحر في شمال أمريكا.

5. 1993 : و^[2] مع تجهيزات قادرة على التنصت على قادة 15 دولة دعاهم الرئيس بيل كلنتون إلى الاجتماع في الولايات المتحدة. ويذكر أن بعض المعلومات المستقاة قد تم نقلها إلى مؤسسات كانت قد مولت الحملة الانتخابية لبيل كلنتون.

6. 1994 : كانت شبكة إشلون قد استخدمت بقوة من قبل الأمريكيين خلال مفاوضات الغات GATT بين الولايات المتحدة والاتحاد الأوروبي. واستخدمت الشبكة، بوجه خاص، من أجل التجسس على موقف كل بلد من بلدان الاتحاد الأوروبي البالغ عددها آنذاك 15 دولة، وللتعرف أيضا على استراتيجية اللجنة الأوروبية. وهذا ما جعل المسؤولين الأوروبيين يعطون حينئذ تعليمات لموظفي الاتحاد الأوروبي في بروكسل تقضي بعدم استعمال البريد الإلكتروني.

7. 1994-1996 : ابتكر أحد المهندسين ينتسب لشركة غير أمريكية جهازا ذا تكنولوجيا عالية لإنتاج الكهرباء. فتجسست عليه شبكة إشلون وأرسلت بمضمون أعماله إلى مؤسسة تكنولوجية أمريكية التي سارعت إلى تسجيل براءة ابتكار حول الجهاز. وكانت العدالة قد حكمت فيما بعد لصالح المهندس، لكن شركته تضررت، ولم تتمكن من دخول السوق الأمريكية بسبب هذا الاختراق.

8. 2000 : كشفت وثائق سرية للغاية، بعد أن رفع عنها طابع السرية بشكل رسمي، عن وجود برنامج إشلون. وفي نفس السنة نشرت الصحافة الألمانية مقالات تفيد بأن محطة في ألمانيا تابعة لشبكة إشلون تقوم بأعمال تجسسية على مؤسسات سويسرية وألمانية اقتصادية وتجارية.

9. 2001 : استخدام شبكة إشلون لرصد تحركات منظمة الباسك الإسبانية واختراق اتصالاتها.

وفي نفس السنة تم تصميم برنامج من قبل الولايات المتحدة لتصنيع شبكة من 24 قمرا صناعيا للتجسس ليلا ونهارا، ومهما كانت أحوال الطقس. وقدرت تكلفتها بـ 25 مليار دولار على أن تكون عملية بدءا من 2005.

كما كشفت الصحافة الألمانية عن اختراق أجهزة وزارتي الخارجية والدفاع عبر نظام مايكروسوفت التي تعمل به الحواسيب المستعملة في الوزارتين. ثم اكتشفت السويد نفس الظاهرة التجسسية في مؤسساتها. ومن المعلوم أن ألمانيا قررت بعد ذلك إزالة هذا النظام واستبداله بنظام آخر طلبت من مؤسساتها القومية (مثل شركة سيمنس Siemens) تصميمه.

10. 2002 : ظهور ما يسميه البعض بمشروع "إشلون 2".

لكن هناك من يبرر هذا التصرف من قبل الأمريكيين بسببين، أولهما أن الأوروبيين، سيما الفرنسيون، يطورون تدابير تجارية غير متفق عليها، وأن هناك قدرات اختراق لدى دول أوروبية (مثل ألمانيا وفرنسا) مماثلة لما يقوم به إشلون. وثانيهما أن التجسس على المؤسسات الاقتصادية والتجارية يندرج في إطار مكافحة الفساد المالي ودفع الرشاوى من قبل مجموعات ومؤسسات أوروبية لحكومات وهيئات مختلفة. ثم إنه من الصعب أحيانا تحديد "جنسية" مؤسسة اقتصادية أو تجارية إن كانت فروعها منتشرة عبر العالم.

ونتيجة لكل هذه الأحداث وتداعياتها قرر الاتحاد الأوروبي عام 2004 تخصيص 11 مليون يورو لتطوير التعمية الكمومية من أجل [?]مان أمن الاتصالات فوق أرا [?]يه. والهدف من هذا المشروع هو ابتكار نظام تعمية

يحول دون اختراق أية معلومات تنقل من خلاله متحديا بذلك نظام إشلون واختراقاته السافرة. وهذا ما جعل الأوربيين يقررون اللجوء، دون تردد، لنظام التعمية الكمومية (انظر أدناه)، وهو مشروع تشارك في إنجازه العديد من البلدان الأوربية الغربية، بما في ذلك روسيا.

التعمية الكمومية:

إذا اعتبرنا أننا بلغنا درجة مقبولة من الأمن بفضل التعمية المبنية على الأعداد الأولية لأنه لا توجد لحد الآن طريقة سريعة تمكن من تفكيك الأعداد الكبيرة إلى أعداد أولية، فماذا يحدث لو تمكن العلماء من اكتشاف طريقة سريعة التفكيك للأعداد الطبيعية إلى أعداد أولية؟ هذا هو السؤال المحير الذي يؤرق اليوم العلماء. ولو حدث ذلك لذهب نظام التعمية الحالي أدراج الرياح ولبات الو²ع الأمني في عدة قطاعات حيوية مأساويا في جميع الدول المتقدمة والنامية.

من هذا الباب الواسع دخلت الفيزياء في مجال التعمية مستخدمة فرعها المسمى بالفيزياء الكمومية، لتحلّ بذلك محلّ الريا²ليات. وهذه الفيزياء هي علم يعنى بالمجهرات فيدرس الجسيمات الأولية، مثل البروتونات والنيوترونات والإلكترونات، كما يدرس الفوتونات والذرات والجزيئات الكيميائية.

تقوم التعمية الكمومية بتشفير المعلومة التي نريد إرسالها بالتأثير على الجسيمات الأولية (باستقطابها مثلا) بحيث يستحيل على أي جاسوس اختراقها. والجميل في هذه الطريقة لا يتمثل في كون الجاسوس لن يتمكن من بلو زهدفه فحسب، بل إن كل محاولة اختراق ستحدث ا²طرابا في الجسيمات سرعان ما يكتشفها صاحب المعلومة.

والواقع أن نظام التعمية الكمومية يكتفي بإرسال مفتاح الشفرة ولا يشفر النص. وهذا راجع لخصوصيات الفيزياء الكمومية. وقد وُضعت أسس هذه التعمية عام 1984 بفضل عدة أبحاث منها بحوث شارل بنيت وجيل براسارد. أما الأفكار الأولى فظهرت خلال الستينيات من القرن الماضي في أعمال ستيفن ويسنر Stephen Wiesner ... والغريب في هذه الأعمال أنها لم تقبل للنشر وقتئذ رغم قيمتها العلمية.

وهناك الآن محاولات وبحوث عديدة في هذا الاتجاه لتصميم أجهزة تجريبية لهذا النوع من التعمية. وإذا ما نجحت هذه التجارب في التعمية الكمومية فإن الخبراء يرون فيها "الأمن المطلق" بعد أن يتم التخلص بسلام من التعمية "العديدة". وسيكون نظام التعمية الجديد ناجعا، بالدرجة الأولى، على مستوى أمن الدول والهيئات العالمية قبل أن "ينزل إلى الأسواق".

يقارن بعض الخبراء علم التعمية بشبكة الإنترنت، فكلاهما ترعرع لدى العسكريين ورجال الأمن. وعندما فكَّ هؤلاء الحصار عليهما وجعلهما في متناول "المجتمع المدني" تطورا بشكل مدهش^[2]، وقدّما خدمات لا تضاهي للمدنيين والعسكريين وللناس أجمعين.

اهم المراجع

أولا : بالعربية

1. سعد الله، أبوكر خالد (2005). عالم الريا [٢]يات. الجزائر : دار هومة.
2. مرياتي، محمد؛ مير علم، يحيى؛ حسان الطيان، محمد (1992). علم التعمية واستخراج المعنى عند العرب : أبحاث الندوة العالمية الرابعة لتاريخ العلوم عند العرب، ج 1. حلب : معهد التراث العلمي العربي. ص 27-58.

ثانيا : بالإنكليزية والفرنسية

1. Cerf N. & Gisin N. (2000). "Les promesses de l'information quantique", La Recherche, 327 : 46-53.
2. Diffie W.& Hellman M.E. (1976). New directions in cryptography. In IEEE Transactions on information theory, Vol. IT-22 : 644-654.
3. Kahn D. (1980). La guerre des codes secrets. Paris: InterEditions.
4. Kerckhoffs A. (1883, January). "La cryptographie militaire". Journal des sciences militaires, Vol. 9 : 5-38.
5. Rivest, R. (1999). Pour la libéralisation de la cryptographie, Pour la Science, 260 : 101-106.
6. Rivest, R.; Shamir, A. & Adleman L. (1978, February). "A method for obtaining digital signatures and public key cryptosystems". Communications of the ACM. : 120-126.
7. Singh S. (1999). Histoire des codes secrets. Paris : LC Lattès.

ثالثا : مواقع على شبكة الإنترنت

1. موقعان حول إشلون Echelon :

<http://www.echelonwatch.org>

http://reseau.echelon.free.fr/reseau.echelon/documents/stoa/vol1_fr.pdf

2. موقع "مركز أمن المعلومات" الكندية

<http://www.cse-cst.gc.ca>

الهوامش

- ¹ - يقصد القرن السابع الميلادي.
- ² - جاء هذا النص في كتاب لديفيد كاهن عنوانه The code breakers يتضمن 1164 صفحة.
- ³ - لم يتمكن المؤرخون من معرفة سنة ولادته أو وفاته.
- ⁴ - لم يتمكن المؤرخون من معرفة سنة ولادته أو وفاته.
- ⁵ - هؤلاء الرياليون هم رون ريفست Ron Rivest وأدي شامير Adi Shamir ولين أدلمان Len Adleman المنتسبون لمعهد التكنولوجيا لماسشوستس الأمريكي MIT (Massachusetts Institute of Technology).
- ⁶ البحث هو
- Diffie W., Hellman M.E. (1976). New directions in cryptography. In IEEE Transactions on Information Theory, Vol. IT-22. pp. 644-654.
- ⁷ - للمزيد من التفاصيل، انظر الموقع التالي على شبكة الإنترنت :
<http://www.apprendre-en-ligne.net/crypto/index.html>
- ⁸ - يرجع تاريخ إنغيما في الواقع إلى سنة 1919 عندما سجّل المهندس الهولندي هوغو ألكسندر براءة اختراع آلة تشفير كهروميكانيكية. وبعد ذلك قام الدكتور آرثر شرييوس بالتأمل في أفكار صاحب البراءة، وأنشأ في برلين شركة تصنيع آلة تشفير مدنية سهاها إنغيما. غير أن هذه الشركة أفلس في الوقت الذي أثارت هذه الآلة اهتمام العسكريين الألمان فتبنوها.
- ⁹ انظر مثلاً المرجع الهام الصادر في نهاية القرن التاسع عشر :
Kerckhoffs A. (January 1883). La cryptographie militaire, Journal des sciences militaires, Vol. 9. pp. 5-38.
- ¹⁰ - انظر موقع هذا المركز على شبكة الأنترنت :
<http://www.cse-cst.gc.ca>
- ¹¹ - انظر الموقع على شبكة الأنترنت :
<http://www.echelonwatch.org>
- ¹² - وبطبيعة الحال فقد كان لمركز أمن الاتصالات الكندي، الذي تعرفنا عليه في النموذج الأول، باع طويل في هذه الشبكة.