العالم المسلم أبو يوسف الكندي رائد علم التشفير

كتبه محمد كريم | 12 أبريل ,2020

أبو يوسف يعقوب بن إسحاق الكندي (801-873) الملقب بأبو فلاسفة العرب، يعد واحدًا من أوائل فلاسفة المسلمين والعراقيين، ولد في مدينة الكوفة الذي كان والده واليًا عليها، وتلقى تعليمه الابتدائي هناك، ثم ارتحل إلى بغداد ليكمل مسيرته العلمية في زمن الخليفة المأمون، ونتيجة فطنته وعكفه على قراءة الكتب الفلسفية والعلمية، عينه المأمون مشرفًا إلى جانب الخوارزمي في بيت الحكمة على كتابة وترجمة الكتب الأجنبية إلى العربية، ثم جعله الخليفة المعتصم في زمن خلافته معلمًا لابنه أحمد.

كان للكندي دور كبير في ترجمة الكتب الفلسفية القديمة في بيت الحكمة، لا سيما الكتب الفلسفية الإغريقية لمشاهير فلاسفتهم كأفلاطون وأرسطو، ونتيجة لهذا العمل، لقب بـ"المعلم الثاني" لمكانته العالية في الفلسفة ولتوسيعه فلسفة أرسطو الملقب بـ"المعلم الأول"، وكان تابعًا لمدرسة المشائية التي أوجدها أرسطو.

اشتهر ابن الكندي بنباهته في علم الفلك، فساهم باكتشاف النجوم ووضع نظريات فيه، واخترع مقياسًا لمعرفة مدى فعالية الدواء على المرضى من خلال أطوار القمر، وهو أول من أدخل علم الرياضيات إلى الطب والعلوم الأحيائية، وقدم الكندي كتابًا عن أسس الطب الذي أصبح كتابًا أساسيًا تابعًا في كل الدول الأوربية آنذاك.

وفي مجال الكيمياء، وصف الكندي طريقة تقطير العطور واخترع أكثر من 107 أنواع من العطور، أما في علم الطقس، فقد فسر الظواهر الجوية كالرياح وظاهرة المد والجزر، ثم قدم للإسلام الكثير من النصوص التي شرح فيها أصول الدين والفقه.

ساهم الكندي كثيرًا في نظرية الموسيقى ووضع قواعد جوهرية لها، ويعد من أوائل علماء العرب الدراسين للموسيقى والعلاج الموسيقي، وهو أول من أدخل كلمة "موسيقى" إلى اللغة العربية، ومنها انتقلت إلى الفارسية والتركية، من أجل كل تلك المعارف والإنجازات في مختلف العلوم والفنون، يستحق ابن الكندي لقب "الفيلسوف" من غير مجاملة أو مدح.

كتب الكندي ما لا يقل عن 260 كتابًا ورسالة في مختلف المجالات العلمية والفلسفية والدينية والفنية، منها كتاب الحث على تعلم الفلسفة، ورسالة في أن لا تنال الفلسفة إلا بعلم الرياضيات، ورسالة في أنواع الحجارة وأنواع السيوف والحديد، ومقالات عديدة عن الحساب الهندسي والشفاء من السموم، لكن أهم من تلك الكتب والرسائل هي مخطوطته عن علم التشفير التي وجدت في الأرشيفات العثمانية معنونة بـ"مخطوطة في فك رسائل التشفير"، فهذا العمل الإبداعي من الكندي هو العلم الأساسي الذي جعله مشهورًا في عالمنا اليوم.

علم التشفير أو ما يسمى بعلم التعمية هو علم يدرس النصوص بأنواعها وذلك لغرض تشفيرها وجعلها غير مفهومة لبعض الأشخاص غير المرغوب بمعرفتهم محتوى تلك النصوص (تعمية العدو)، وجعل تلك نصوص خاصة فقط لمن يملكون المفتاح أو المعلومات في كيفية إرجاع ذلك النص المشفر إلى أصله. يستخدم علم التشفير في التقنيات الإلكترونية، وذلك لغرض تشفير معلومات مهمة مثل الأرقام السرية للحسابات البنكية أو لإنشاء محادثات آمنة بين الأشخاص المتحدثين في الإنترنت.

> وجد ابن الكندي أول طريقة لاستخراج المعمى أو فك شفرة النصوص المشفرة

أما علم التحليل المشفر أو استخراج المعمى فهو علم يهتم بدراسة النصوص المشفرة ومحاولة فكها وفهم محتواها من خلال إجراء تقنيات إحصائية ورياضية عليها للحصول على مفتاح أو معلومات كافية لإرجاع النص إلى أصله المفهوم، وهو علم مقابل لعلم التشفير وكل منهما يكمل الآخر، فالأول يشفر من أجل الإخفاء، والآخر يحاول فك الشفرة من أجل الإظهار، ويستخدم علم تحليل المشفر في العمليات العسكرية والإجرامية لمحاولة فك الرموز الغامضة من الرسائل المشفرة التي تتداول بين القيادات العسكرية أو النصوص المشفرة بين المجرمين والمافيات.

وجد ابن الكندي أول طريقة لاستخراج المعمى أو فك شفرة النصوص المشفرة، وهو بذلك أعطى شرف السبق للعرب في قيامهم بفك شفرة النصوص. يعتبر ابن الكندي اليوم واضع ومؤسس الأول لعلم التعمية والتحليل.

كانت الشفرات القديمة تستخدم طريقتي الاستبدال وتحويل الترتيب، وطريقة الاستبدال هي

تبديل حروف النصوص الأصلية إلى حروف أخرى في الأبجدية، مثلًا، يمكننا القيام بتشفير النص الآتي:

"علي سوف يقوم بالهجوم اليوم" إلى "غمأ شيق أكين تبموحين بمأين"، حيث استبدلنا الحروف الأصلية في النص بالحروف التي تليها في الأبجدية، كما نرى تغير النص وتحول حرف الياء فيه إلى ألف، وحرف الألف إلى باء، وهكذا.

وإن أردنا إعادة النص إلى أصله غير المشفر، فما علينا إلا استبدال الحروف في النص المشفر بالحروف التي تسبقها في الأبجدية، فنبدل حرف الـ(غ) في أول الكلمة بـ(ع) إلى آخره، حتى يعود النص مفهومًا للقارئ، وهذه المعلومة التي علمت فيها أن النص مستبدل بالحروف التي تليه في الأبجدية تسمى بالمفتاح، لأن في معرفتها ينجلي الأمر للمحلل في كيفية إرجاع النص إلى أصله، والمفتاح ممكن أن يكون مختلفًا عما أعطيناه في المثال هنا، فمن الممكن أن تستبدل الحروف الأصلية في النص بالحروف التي تبعد عنها بستة أحرف في الأبجدية، كتبديل حرف (أ) بـ(د) وهكذا.

بدأ ابن الكندي دراسة النصوص غير المشفرة أولًا، واستنتج بأن هناك حروفًا يتكرر استعمالها بشكل شائع عند تكوين الجمل، مثلًا في اللغة العربية يتكرر حرفا (أ – ل) كثيرًا للغاية، بينما وجود حرفي (ض – ظ) نادر في النص، مما دفع الكندي إلى استنتاج تقنية يقدر من خلالها على فك شفرة النصوص التقليدية ومعرفة المفاتيح المستخدمة فيها.

هذه التقنية تعرف اليوم بالتحليل الترددي وهي تقنية يستخرج بها المحلل (الراغب في فك شفرة) الرموز الأكثر تكرارًا في النص المشفر، ويحاول استبدال تلك الحروف بحروف أكثر تكرارًا في لغة العدو، فبذلك عاجلًا أم آجلًا، سوف يكتشف المحلل المفتاح الذي يفك النص المشفر، ولا تقتصر هذه التقنية على الحروف فقط، بل يمكن تحليل النصوص المشفرة بالبحث عن الكلمات الأكثر شيوعًا في اللغة.

وفي وقت ابن الكندي، كانت الكلمات الأكثر تنقلًا في الرسائل المشفرة هي كلمات ذات صلة بالدين (الله، إسلام، مسلم، إلخ) وكانت أغلبية الرسائل تفتتح بالبسملة وتحتوي على الأقل على آية قرآنية واحدة أو حديث نبوي واحد، مما يسهل أمر فك الشفرات للمطلع على ثقافة الإسلامية والعالم بالأسلوب المتبع في كتابة الرسائل.

> وجد ابن الكندي طريقة مثالية في تحليل وفك شفرة النصوص الكلاسيكية، واستخدمت هذه التقنية بعده بشكل واسع في عدة حروب

يعتمد التحليل الترددي على بعض الشروط المقيدة التي لا يمكن إجراء العملية دونها:

أولًا.. يلزم أن يكون المحلل ذكيًا ونابغة في استخراج الأنماط من النصوص، فضلًا عليه، يجب أن يكون مطلعًا على ثقافة العدو وأن يتوقع موضوع الرسالة حتى لو لم يقرأ محتواها، مثلًا يجب أن

يستنبط المحلل أن الرسائل المشفرة في الحروب تكون بالعادة أوامر عسكرية وليست رسائل حب.

ثانيًا.. توافر نصوص مشفرة كافية لتحليل واستخراج الكلمات الشائعة منها، وإلا سوف تخرج النتائج خاطئة وبعيدة عن الأصل.

ثالثًا.. يجب أن يكون النص مشفرًا بشفرات الاستبدال، أي يجب أن تكون حروف النص مستبدلة بحروف أخرى في الأبجدية، وليست مشفرة بتقنيات تشفيرية أخرى، وهذه واحدة من قوانين العالم شانون واضع نظرية المعلومات "المحلل يجب أن يعرف النظام".

ورابعًا.. يجب أن يكون عند المحلل وقت كافٍ لفك الشفرة في الوقت المناسب، حيث تصبح الرسائل العسكرية أو الأوامرية بلا فائدة إذا حللت في الوقت لاحق، فحواشي الرسالة لا تفيد المحلل في أي شيء بعد ذلك، وهذا الشرط أدى إلى تشفير العدو نصوصه بعدة شفرات متتالية حتى يصعب على المحلل تحليلها في الوقت المناسب، فمثلًا يقوم المشفر بتشفير النص الأصلي ثم إعادة تشفير النص المشفر الأول ثم إعادة تشفير النص المشفر الثاني وهكذا.

وجد ابن الكندي طريقة مثالية في تحليل وفك شفرة النصوص الكلاسيكية، واستخدمت هذه التقنية بعده بشكل واسع في عدة حروب لا سيما الحربين العالميتين في أوروبا، إلا أنهم لم يستمدوها من كتب ابن الكندي بل طوروا أفكاره بعد ترجمة كتبه، وجاء بعده عدة علماء ليضعوا شفرات أخرى يصعب على تقنية التحليل الترددي فكها.

لا تستخدم اليوم شفرات استبدالية أو كلاسيكية في الميادين الإلكترونية لسرعة الحواسيب في فك شفراتها بالتحليل الترددي أو حتى بالتجربة العشوائية للحروف، فالعالم يعتمد الآن على شفرة الأعداد الأولية في التشفير الإلكتروني، وهذه التقنية يكون صعب للغاية على الحاسوب تفككيها بسرعة.

بغض النظر عن ذلك، فإن اكتشافات أبي يوسف الكندي كانت فتيلًا لتنوير علم التشفير وما لاحقه. أُحرض القارئ على استخدام تلك الشفرات وتحليلها كلعبة لاختبار ذكاء وفطنة الأصدقاء والعوائل، أو حتى استعمالها في تشفير كلمات السر عند كتابتها على الورق، فهي فعالة جدًا ضد غير المطلعين بها.

رابط المقال : https://www.noonpost.com/36662/