مقـــدمة العرض

أننا نعيش عصر المعلومات أو الثورة المعلوماتية ومن يملك المعلومات هو الأكثر قوة والأكثر حذراً والأكثر استفادة من الفرص والمواقف والأكثر استعداداً لتخطيط المستقبل بكفاءة . ولقد أصبح تبادل المعلومات وانتقالها عبر خطوط الاتصال والشبكات الرقمية عنصراً متكاملاً فى حياتنا الحضارية .

ويقدر بأن عشرات الملايين من الرسائل الإلكترونية تتحرك يومياً عبر الإنترنت وبلايين الدولارات يتم الاتفاق عليها عبر التجار الإلكترونية – التى لا تزال فى بدايتها – وكمية الأموال التى تنتقل عبر خطوط الاتصال البنكية فى نظام SWIFT يومياً تعادل نصف الناتج العالمى .

وقريباً سيكون من الممكن جمع الأصوات الانتخابية وإدارة الشئون الحكومية وإقرارات الضرائب وغيرها من خلال شبكات الاتصال الرقمية .

إلا أن نجاح نهضة عصر المعلوماتية يتوقف على القدرة على حماية المعلومات أثناء انتقالها وهذا بدوره يعتمد على القدرة على تشفير الرسائل . فنظم الشفرة الآن هى الحارس على نجاح الحضارة المعلوماتية . وقد ظلت هذه النظم ولمدة تقرب من ألفين عام حكراً على الحكومات والجيوش ولكنها الآن تلعب دوراً هاماً فى حماية المعلومات والمعاملات المدنية والتجارية .

يقدم هذا الكتاب سرداً تاريخياً لتطور نظم الشفرة والمواجهة المستمرة التى لم تنتهى بعد بين فريق واضعى الشفرة وفريق كاسرى الشفرة .

مقدمة المؤلف

اعتمدت رئاسات الدول منذ آلاف السنين على الاتصالات الجيدة فى إدارة شئون البلاد وقيادة الجيوش . وعلى قدر هذا الاعتماد كان هناك إدراك بالمخاطر التى يمكن أن تتعرض لها هذه الاتصالات إذا وقعت فى يد الأعداء واكتشفوا ما بها من خطط ونوايا . وقد كان هذا الخطر الجاثم هو الدافع وراء تطور وتقدم نظم الأكواد ونظم الشفرة وأساليب إخفاء وتمويه الاتصالات مما دفع دول وحكومات كثيرة إلى إنشاء إدارات مستقلة للشفرة مسئولة عن وضع نظم التشفير وأيضاً عن اكتشاف أساليب لكسر الشفرات الأجنبية التى تقع فى حوزتها . وعادة ما تتبع هذه الإدارات لأجهزة المخابرات القومية فى الدولة . ويطلق على خبراء كسر الشفرة اسم كيميائيو اللغات فهم جماعات متفانية فى عملها تعمل بدئب وعزيمة لتحويل رموز لا معنى لها إلى كلمات مفهومه .

إن تاريخ الأكواد والشفرة هو قصة المعركة الممتدة عبر القرون بين واضعى الشفرة Code makers وكاسرى الشفرة Code breakers . وهو سباق فكرى وذهنى كان له أثر ملموس على التاريخ البشرى .

إن تطور نظم الشفرة يشبه تماماً تطور الكائنات الحية منذ نشأة كوكب الأرض . فالنظام الشفرى يتعرض فور نشأته إلى هجوم مستمر من كاسرى الشفرة فإذا استطاعوا اكتشاف نقاط ضعف وكسره أصبح فى الحال لا فائدة له وهو وضع يحتم أحد احتمالين إما فناء النظام واندثارة أو تطوره وتحوره إلى شكل جديد يظل قائم طالما لم يكسر أو ينكشف ضعفه .

وهذا السيناريو يشبه تماماً ما يحدث مع تطور الكائنات الحية مثل البكتريا التى تعيش وتتكاثر طالما لم يظهر مضاد حيوى فعال لها ... فإذا ظهر فإنها تبدأ فى التطور إلى شكل جديد يقاوم هذا المضاد الحيوى ...

لقد ساهم هذا الصراع (فى مجال الشفرة) فى تطورات علمية عظيمة فى اللغويات والرياضيات ونظرية المعلومات والحاسبات الإلكترونية ونظرية الكوانتم (متناهيات الصغر) .

يهدف هذا الكتاب إلى سرد تاريخ نظم الشفرة وبيان أهميتها القصوى فى الوقت الحاضر مع تزايد الاعتماد بدرجة كبيرة على الاتصالات المفتوحة كالبريد الإلكترونى والتجارة الإلكترونية والمؤتمرات عن بعد مما يزيد بشكل موازى مخاطر تعرض محتويات هذه الاتصالات للكشف بواسطة جهات غير مرغوب فيها .

ويسعى الكتاب أيضاً إلى توضيح أن موضوعه يعتبر أكثر ارتباطاً بالحياة الحاضرة

عن الماضى فمع زيادة قيمة المعلومات كعنصر إنتاج ومع تغير شكل المجتمعات مع ثورة الاتصالات يتزايد استخدام أساليب الشفرة فى الاتصالات . فاليوم تتقاطر المكالمات التليفونية عبر الأقمار الصناعية وتعبر الرسائل الإلكترونية العديد من الحاسبات قبل أن تصل إلى مستقبلها ويتزايد دور التجارة والأعمال الإلكترونية بدرجة ملحوظة وكافة هذه الاتصالات ستكون عرضة للاختراق والكشف إذا لم تشفر . فالشفرة الآن هى الضمان الوحيد لحماية الخصوصية ولنجاح تعاملات الأسواق الإلكترونية عبر العالم .

ولكن هذا الاحتياج المتزايد للشفرة يتعارض فى بعض جوانبه مع سياسات أجهزة الأمن القومى التى تلزمها المصلحة القومية العليا ضرورة تتبع اتصالات العناصر الخطرة والمريبة والمشبوهة .

وتشفير اتصالات هذه العناصر سيكون عائق مزعج أمام عمل هذه الأجهزة لذا تسعى هذه الأجهزة إلى وضع يدها على تطوير نظم الشفرة بالمشاركة فيها من ناحية أو بوضع قيود وقواعد تحول من زيادة قوة هذه النظم بدرجة كبيرة من ناحية أخرى.

ومع إقرار أن للشفرة دور هام ومتزايد فى الحياة المدنية فإن الحقيقة المؤكدة هى أن الشفرة العسكرية تعتبر من الموضوعات الهامة للغاية فهى التى تلعب دوراً بارزاً فى حسم نتائج الحروب . وقد سمى البعض الحرب العالمية الأولى بحرب الكيميائيين (لما استخدم فيها من غازات سامة) ويسمى البعض الحرب العالمية الثانية بحرب الفزيائيين (حيث اكتشف فيها الدمار الهائل الناجم عن تفتيت الذرة) ويسمى البعض الحرب العالمية الثالثة بحرب الرياضيين Mathematicians لأنهم سيسطروا على أهم عناصر هذه الحرب وهو المعلومات والشفرة . فالرياضيون هم القادرون على استنباط نظم الشفرة كما أنهم هم القادرون على كسر الشفرة ووضع الإجراءات المضادة لها .

ويشير المؤلف فى نهاية المقدمة إلى صعوبة إعداد كتاب عن الشفرة فبما أن نظم الشفرة هى علم السرية فهى أيضاً فى حد ذاتها علم سرى ينتمى أساساً إلى أجهزة مغلقة غير مسموح بدخولها يعمل بداخلها جنود مجهولون بدأب متناهى وبفكر علمى راقى . ومن هذه الأجهزة جهاز الاتصالات الحكومية البريطانى GCHQ وكالة الأمن القومى الأمريكى NSA وكافة أجهزة المخابرات التى ارتقت إلى مستوى يسمح لها بإجراء البحوث والتطوير فى مجال الشفرة(*) .

(*) يشرفنى فى هذا الصدد أن أذكر جهاز المخابرات العامة المصرية الذى عملت فيه لأكثر من ثلاثين عام (المترجم) .