ميكنة الشفرة

منذ أن قام باباج وكاسيسكى بكسر سرية شفرة فيجنير أصبحت الاتصالات الشفرية فى نهاية القرن التاسع عشر فى وضع غير سار ، وكان هناك سعى دؤوب من فريق واضعى الشفرة للبحث عن بديل لشفرة فيجنير يحقق للاتصالات المدنية والعسكرية الاستفادة من ثورة الاتصالات التى صاحبت اكتشاف أسلوب الاتصالات التلغرافية ويليه اكتشاف التليفون بواسطة العالم الإيطالى ماركونى .

وأدى اندلاع الحرب العالمية الأولى إلى تسابق الأطراف المتحاربة فى البحث عن النظام الشفرى المثالى الذى يضمن أمن الاتصالات على جبهات القتال . وقد استطاع الجانب الألمانى فى مارس ١٩١٨ وضع نظام شفرى سمى ADFGVX وهو عبارة عن خليط من الأحرف والأرقام أى أنه لا يعتمد على ترتيب أبجدى معروف مما يحد من إمكانية كسره من خلال تتبع تكرارات الأحرف ، إلا أن هذه الفكرة لم تكن كافية لتحقيق الصعوبة المطلوبة فى هذه الشفرة والتى استطاع العالم الفرنسى جورج بينفين Georges Painvin التعرف على نقاط ضعف هذا النظام ومن ثم كسر شفرته .

وقد ساهم ذلك بصورة أساسية فى فقدان الجيش الألمانى عنصر المفاجأة فى تنفيذ هجومه الأخير على باريس بعد أن وصل على بعد مائة كيلو متر منها واستطاع الحلفاء وقف الهجوم ، وبدأت بعد ذلك سلسلة الهزائم لألمانيا والتى انتهت بهزيمتها فى الحرب .

وفى كتاب «فن الحرب The Art of war» يقول المؤلف سن تزو Sun Tzu «أنه لا يوجد شىء أفضل من المعلومات بالنسبة للأطراف المتحاربة ، ولا يوجد شىء مدعاة للثقة مثلها . وكان الاهتمام بجمع المعلومات أثناء الحرب وتحليلها يحظى بأكبر قدر من الإمكانات ومع التوسع فى أساليب الاتصال اللاسلكية ابتدع الفرنسيين أسلوباً ذكياً لتحديد مراكز ونقاط الإرسال ، فكانوا يقومون بإنشاء مراكز للاستماع يبلغ عددها فى بعض الأحيان إلى ستة مراكز ولا تقل أبداً عن ثلاثة مراكز ويتم توزيع مواقع هذه المراكز فى أماكن متباعدة وعند التقاط هذه المراكز الإرسال الصادر من نقطة محددة يمكن بسهولة تحديد موقعها من خلال تقاطع الخطوط المستقية الواصلة بين كل مركز استماع وهذه النقطة فيما سمى بعد ذلك بعمليات تحديد الاتجاه Direction Finding . ويلى تحديد موقع نقطة الإرسال رصد ما ترسله وإجراء التحليلات عليه والتى سميت بتحليلات المرو Traffic Analysis ثم تاتى المرحلة الأخيرة وهى تحليل الشفرة المستخدمة فى هذا الإرسال للتعرف على ما بها من خطط ونوايا .

وقد قام البريطانيين والأمريكان بإسهامات قوية فى مجال فك الشفرة أثناء الحرب العالمية الأولى كان أبرزها التعاون بينهم فى فك شفرة البرقية الألمانية التى أرسلت فى ١٩١٧/١/١٧ والتى أطلق عليها اسم برقية زيمرمان . وتبين قصة هذه البرقية مدى فن تحليل وكسر الشفرة على تغيير مجرى الأحداث وحسم الحروف فبفضل كشف سر هذه البرقية قررت الولايات المتحدة التخلى عن عزلتها وحيادها وقررت الاشتراك فى الحرب جنباً إلى جنب مع الحلفاء الأوربيين ضد ألمانيا .

وكان وزير خارجية ألمانيا فى ذلك الوقت أرثر زيمرمان Arthur Zimmer-mann قد أرسل البرقية إلى سفير ألمانيا فى واشنطن لكى يتولى إرسالها إلى سفير ألمانيا فى المكسيك والذى سيقوم بدوره بتسليمها إلى رئيس جمهورية المكسيك وجاء فى البرقية ما يلى :

«نحن ننوى بدء مجهود حربى غير محدود باستخدام الغواصات فى بداية فبراير القادم وسنحاول بالرغم من ذلك الإبقاء على حياد الولايات المتحدة وعدم تدخلها فى الحرب وفى حالة عدم استطاعتنا تحقيق ذلك فإننا نعرض على المكسيك عرضا للتحالف معنا على الأسس التالية :

١ – نخوض الحرب معا .

٢ – نحقق السلام معا .

٣ – نقدم دعم مالى سخى من جانبنا .

٤ – نتفهم من ناحيتنا بأن المكسيك ستغزو أراضيها المحتلة فى تكساس ونيومكسيكو وأريزونا لتحريرها من الولايات المتحدة .

وأننا ندعوكم إلى التنسيق فيما بيننا وبين اليابان أيضاً كما نتوقع أن هذا المجهود الحربى سيؤدى خلال أشهر قليلة إلى طلب انجلترا عقد سلام معنا وإلى عدم قدرتها على مواصلة الحرب » .

أرثر زيمرمان

وقد أرسلت هذه البرقية عبر الاتصالات اللاسلكية وتم التقاطها وسلمت إلى «الغرفة ٤٠» وهو الاسم الكودى لمكتب الشفرة التابع لادميرالية البحرية البريطانية والذى يحوى مجموعة نادرة من علماء الرياضيات واللغويات ومدمنى حل الكلمات المتقاطعة . وقد تمكن هؤلاء العلماء من كسر شفرة برقية زيمرمان وتم عرض محتواها على الرئيس الأمريكى وودرو ويلسون فى ١٩١٧/٢/٣ والذى كان قد ظل

ملتزم بالحياد الأمريكى بالرغم من بدء حرب الغواصات الألمانية الواسعة النطاق لمنع قوافل الإمداد البحرية من الولايات المتحدة إلى أوربا ولكن بعد استلامه البرقية وتأكده من نوايا ألمانيا اتخذ قرار طلب الكونجرس الموافقة على إعلان الحرب على ألمانيا .

❁ ❁ ❁

شكل جدول فيجنير أحد ساحات المعارك بين فريق واضعى الشفرة وفريق كاسرى الشفرة . وكما سبق وذكرنا فقد كسرت شفرة فيجنير بالاعتماد على أن كلمة السر أو المفتاح الشفرى يبلغ طوله فى حدود من خمسة إلى ستة أحرف وبالتالى يمكن التعرف عليها بسهولة .

وقد ظل واضعى الشفرة فى حيرة من أمرهم حتى وصلوا إلى فكرة إطالة كلمة السر مما يزيد من صعوبة كشفها .

تخيل نصاً طوله ١٠٠٠ حرف تم تشفيره بواسطة جدول فيجنير وكان طول المفتاح الشفرى خمسة أحرف فقط . ففى هذه الحالة سنحتاج إلى تحليل ترددات الأبجدية لخمس مجموعات من النص الأصلى طول كل مجموعة ٢٠٠ حرف وهذا أمر سهل . ولكن إذا بلغ طول المفتاح ٢٠ حرف فإن عدد المجموعات سيصل إلى ٢٠ مجموعة طول كل منها ٥٠ حرف . فما بالك لو وصل طول المفتاح ١٠٠٠ حرف ... إن عدد المجموعات سيكون ١٠٠٠ مجموعة وطول كل منها حرف واحد وهو أمر شديد الصعوبة على القائمين على كسر الشفرة .

وقد تم تطوير هذه الفكرة لكى يصبح المفتاح الشفرى مساوياً فى طوله للنص المطلوب تشفيره بحيث يقابل كل حرف فى المفتاح حرفا واحدا فى النص ... .أكثر من ذلك أن المفتاح أصبح يستخدم مرة واحدة فقط ثم يعدم بعد ذلك ويتم ذلك من خلال آلات خاصة تعد المفاتيح بشكل عشوائى ويتم وضعها فى أسطوانات خاصة بحيث لا يخرج من فتحة الأسطوانة إلى شريحة من المفتاح تعادل سطر واحد ويتم جذب هذه الشريحة لاستخراج مفتاح مساوى فى طوله مع النص المطلوب تشفيره وبعد التشفير يعدم المفتاح . ويوجد لدى جهة الاستقبال أسطوانة مشابهة يتم استخراج المفتاح منها لفك الشفرة ثم يعدم بعد ذلك ويسمى هذا الأسلوب بمفتاح المرة الواحدة One - time pad cipher .

وهكذا تستمر المعركة وكل فريق يحقق إنجازاً ما يقابله الفريق الآخر بإنجاز مضاد يهدم ما عمله الفريق الأول .

❁ ❁ ❁

تطوير الآلة الشفرية :

يقدم المؤلف نبذة تاريخية عن تطور الآلات الشفرة بدءاً من القرص الشفرى الذى صححه الإيطالى ليون البرتى فى القرن الخامس عشر وهو عبارة عن قرصين من المعدن متداخلين القرص الخارجى عليه الأبجدية المستخدمة والقرص الداخلى عليه أبجدية أخرى ورموز تستخدم فى التشفير ويتم تحريك القرص الداخلى للتعرف على الحروف الداخلية المقابلة للحروف الخارجية وتستخدم فى تشفير الرسالة وقد تعددت أنواع هذه الآلة ومنها نوع استخدم أثناء الحرب الأهلية الأمريكية .

قرص التشفير
الذى استخدم فى الحرب الأهلية الأمريكية

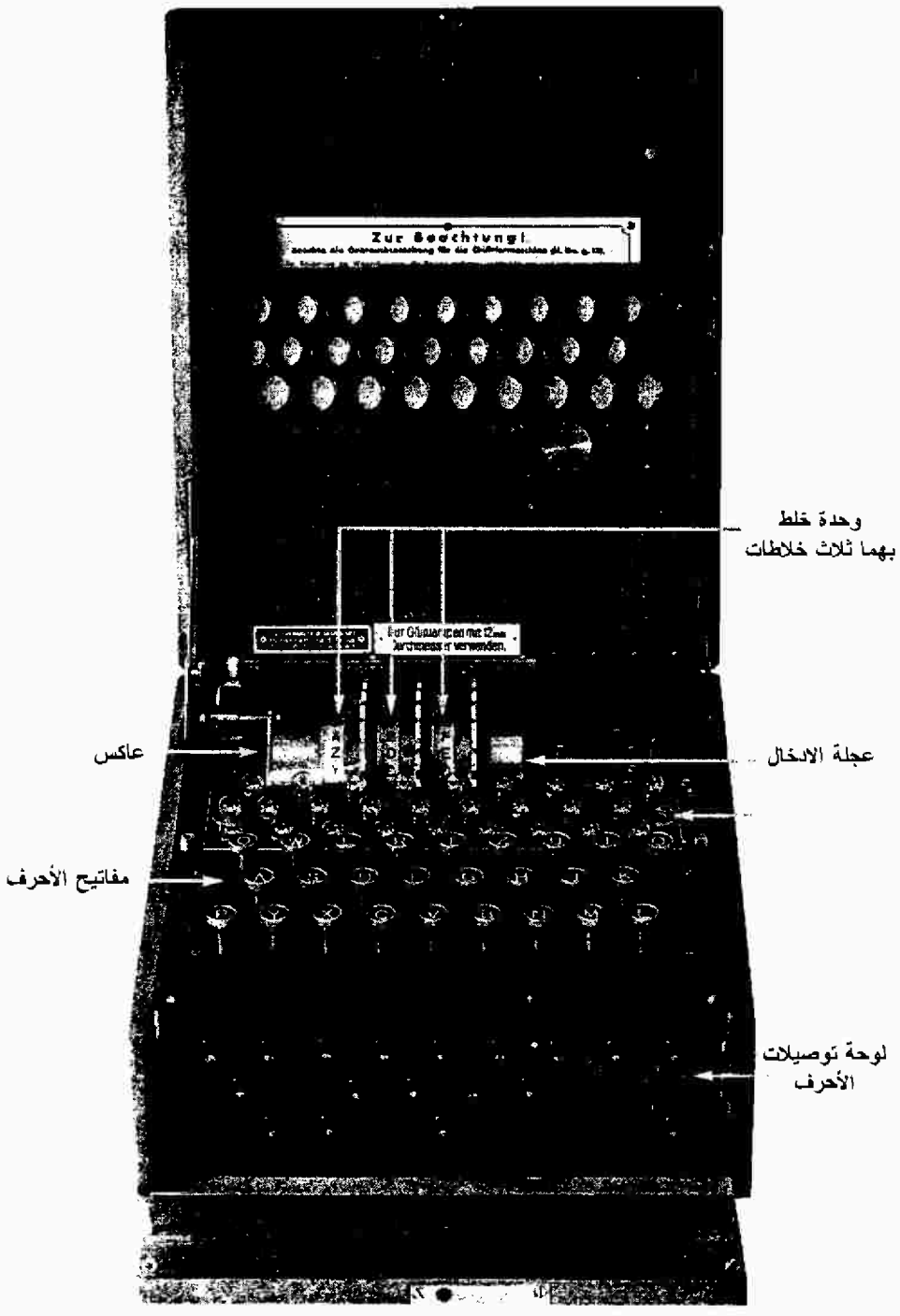
إلا أن أشهر آلات الشفرة وأكثرها سيطا كانت الآلة الألمانية أنيجا Engma التى ابتدعها المهندس الألمانى أرثر شيربيوس Arthur Scherbius فى ١٩١٨ واستخدمت لمدة طويلة فى تأمين الاتصالات الألمانية وكانت شفرتها من أكثر الشفرات إرباكاً للدول الغربية .

وتتكون هذه الآلة من ثلاثة أجزاء :

١ – لوحة مفاتيح لإدخال النص الواضح .

٢ – وحدة خلط حروف Scrambler لتحويل حروف النص الواضح إلى حروف شفرية .

٣ – وحدة عرض تظهر الحرف الشفرى المستخدم بدلاً من الحرف الأصلى .



آلة انجما

وقد استطاع شريبوس مصمم الانجما أن يجعل منها آلة فذة فى التشفير بحيث أن شفرتها كانت مستحيلة الكسر واعتمدت عليها العسكرية الألمانية فى الحرب العالمية الأولى وفى فترة ما بين الحربين العالميتين .

وتكمن صعوبتها فى أن بها ثلاثة خلاطات للحروف وليس خلاطا واحداً بالإضافة إلى أفكار هندسية أخرى تزيد من صعوبة كسرها وتصل بعدد الاحتمالات التى يجب دراستها للوصول إلى كسر هذه الشفرة إلى عشرة ملايين بليون احتمال أو بعبارة أخرى واحد وأمامه ١٥ صفر .

واستمر استخدام الانجما حتى الحرب العالمية الثانية أى أنها ظلت طيلة ثلاثين عاماً معجزة التشفير الآلى ، وبلغ عدد الوحدات التى انتجت منها لصالح الجيش الألمانى ٣٠٠٠٠ وحدة .

وقد استطاع محللى الشفرة البريطانيين فى «الغرفة ٤٠» وبعد جهود مضنية اعتمدت على الاستيلاء على أحد آلات الانجما من بارجة ألمانية غرقت فى ١٩١٤ تحليل مكونات الآلة وكسر شفرتها .