نظم الشفرة الأولية

انجلترا القديمة :

فى التاريخ الإنجليزى المليء بقصص التآمر تعتبر قصة الملكة مارى واحدة من أشهرها، فقد تآمرت لاغتيال الملكة الشرعية اليزابيث لكى تستولى على عرش انجلترا بدلاً منها وعندما كشفت المؤامرة قبض عليها وقدمت للمحاكمة فى اكتوبر عام ١٥٨٦م .

وكان لابد من تقديم الدليل الدامغ على اشتراكها فى هذه المؤامرة وكان قد تم القبض أيضاً على المجموعة المعاونة لها وهم من الكاثوليك الذين كانوا يسعون إلى إسقاط اليزابيث البروتستانية عن العرش وإحلال مارى الكاثوليكية مكانها .

كانت مراسلات مارى معهم قد تم الاستيلاء عليها إلا أن مضمونها كان غير معروف بسبب كونها مشفرة .

إلا أن مستشار الملكة اليزابيث والزينجهام Walsingham الداهية والذى كان يدير مجموعة من الجواسيس لتقصى المعلومات كما كان من أوائل من فكروا فى إدارة عملية الشفرة وأنشأ فى لندن مدرسة للشفرة أعدت مجموعة من الأفذاذ فى تحليل الرسائل ومن أساليب التحليل هذه تتبع عدد مرات تكرار كل حرف للتعرف على أى حرف أكثر تردداً من غيره ثم مقارنة ذلك بتردد الحروف الشفرية فى الرسالة المشفرة لمعرفة الحرف الواضح الذى يقابله حرف شفرى. وبهذه الطريقة التى تعتبر بدائية فى علم الشفرة استطاع والزينجهام كسر شفرة الملكة مارى فى مراسلاتها مع أعوانها وأثبت بالدليل القاطع اشتراكها فى مؤامرة اغتيال الملكة اليزابيث وبالتالى الحكم عليها بالإعدام .

اليونانيون :

استخدم اليونانيون أسلوب شفرة بدائى فى حروبهم مع الفرس يعتمد على الإخفاء المادى للرسالة أو ما يسمى Stegnography وهى كلمة مشتقة من كلمتين فى اللغة اليونانية هما Steganos بمعنى تغطية و graphein بمعنى كتابة وتركيبهما معا يعنى «تغطية الكتابة» وقد استخدم هذا الأسلوب لفترة طويلة من الزمن إلا أنه يحوى نقاط ضعف خطيرة فإذا استطاع من يسعى إلى كشف الرسالة إلى إزالة الغطاء الذى يخفيها فإنه سيعلم على الفور مضمونها . وكان هناك أساليب عدة لتغطية الرسائل مثل تغطيتها بالفخار فى شكل وعاء أو إناء وعند كسر الفخار تظهر الرسالة وكان الصينيين يكتبون الرسائل على نسيج حريرى رقيق ثم يطوى داخل كرة صغيرة ويتولى القائم بتوصيل الرسالة بلع هذه الكرة لإخفاء الرسالة . وابتكر العالم الإيطالى جيوفانى بورتا أسلوب الإخفاء بالكتابة على سطح البيض المسلوق باستخدام الخل . وكان من الأساليب المستخدمة فى الإخفاء أيضاً أسلوب الحبر السرى حيث استخدم القدماء عصارة بعض النباتات بطريقة تشبه الكتابة بالحبر السرى .

ولمعالجة العيب الأساسى فى أسلوب التغطية والمتمثل فى بقاء الرسالة واضحة ظهر أسلوب تغيير محتوى الرسالة بحيث يصعب معرفة معناها الحقيقى فى حالة كشفها وهو ما يسمى بعلم التشفير Cryptography وهى أيضاً كلمة مشتقة اليونانية وتعنى «إخفاء الكتابة» حيث أن كلمة Kryptos تعنى المختفى .

ومن الممكن الجمع بين أسلوب التغطية وأسلوب التشفير فى رسالة واحدة مثلما حدث فى الحرب العالمية الثانية حين استخدم الجواسيس الألمان أسلوب تصغير الرسالة على ميكروفيلم بحيث تصبح فى حجم نقطة علامة التعجب ويتم لصقها مكان النقطة فى الخطاب المرسل ، وفى نفس الوقت تكون الرسالة نفسها مشفرة وغير قابلة للقراءة الفورية . وقد اكتشفت أول رسالة من هذا النوع بواسطة مكتب التحقيقات الفيدرالى الأمريكى FBI فى ١٩٤١ .

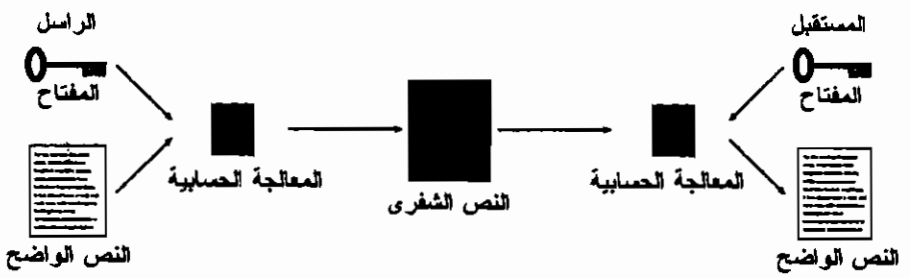
وتعتمد الشفرة على أسلوبين أساسيين فى إخفاء المعنى الأصلى وهما :

١ – أسلوب إعادة الترتيب Transposition حيث يتم إعادة ترتيب أحرف الرسالة الأصلية بطريقة متفق عليها بين الراسل والمستقبل فقط بما يخفى المعنى ويجعل الرسالة غير قابلة للقراءة الواضحة وعند وصولها إلى جهة الاستقبال يتم إرجاع ترتيب الحروف إلى أوضاعها الأصلية .

٢ – أسلوب التبادل Substitution حيث يتم استخدام أحرف بدلاً من الأحرف الأصلية وفقاً لمفتاح معروف لدى الراسل والمستقبل وعادة ما يتم إعداده بطريقة حسابية معروفة للطرفين .

الأبجدية الواضحة	a b c d e f g h i j k l m n o p q r s t u v w x y z
الأبجدية الشفرية	D E F G H I J K L M N O P Q R S T U VW X Y Z A B C

الرسالة الواضحة	v e n i, v i d i, v i c i
الرسالة الشفرية	Y H Q L, Y L G L, Y L F L



العرب :

كان اهتمام الحكم العباسى بتنمية المجتمع والحياة الثقافية فى مناخ سلمى وراء تقدم وازدهار الدولة الإسلامية فى ذلك الوقت وقد صاحب ذلك نظام إدارى قوى اعتمد على اتصالات على قدر عالى من التأمين بفضل استخدام أساليب ذكية فى التشفير . وذلك طبقاً لما ورد فى مرجع «أدب الكتاب» الذى صدر فى القرن العاشر الميلادى .

وكان الأسلوب الدارج فى التشفير هو استخدام حروف أبجدية مرتبة ترتيباً مختلفاً عن الأبجدية العادية وبأشكال مختلفة أيضاً عن شكل الأبجدية العادية وذلك بإجراء عملية تبادل بين الحروف أو باستخدام رموز غير حرفية بدلاً من الحروف .

ويسمى هذا الأسلوب «بالشفرة التبادلية أحادية الأبجدية» Mono-alphabetic substitution cipher . ولم يقتصر الإسهام العربى فى مجال الشفرة على التشفير بل كان لهم إنجازات كبيرة فى تحليل الشفرة وفكها crpto - analysis وهى المهمة الأكثر صعوبة .

ويرى المؤلف أنه من الصعب إيجاد إمكانيات عالية فى تحليل وفك الشفرة إلا إذا بلغ المجتمع بأكمله درجة عالية من الرقى العلمى وبصفة خاصة فى علوم الرياضيات والإحصاء واللغويات وكان هذا بالضبط حال الأمة العربية فى ذلك الوقت.

ومن كبار الفلاسفة العرب فى فك الشفرة العالم «أبو يوسف يعقوب ابن إسحاق الصباح» ابن عمران ابن إسماعيل الكندى» والذى اشتهر باسم «الكندى فيلسوف العرب» وعاش فى القرن التاسع الميلادى ومن أهم أعماله التى لم تكتشف إلا مؤخراً فى عام ١٩٨٧ م فى أرشيف سليمانية عثمان بمدينة استنبول كتاب «دليل فك شفرة الرسائل المشفرة» وقد أسهم بدرجة خاصة فى ابتداع أسلوب كشف الحروف الشفرية من خلال قياس درجة ترددها فى الرسائل الشفرية ومقارنتها بدرجة ترددها وتكرارها فى اللغة الطبيعية فالحرف الأكثر تردداً فى الرسالة غالباً ما يكون له نفس التردد فى اللغة الطبيعية الواضحة وبهذه الطريقة ومع قدر معقول من التخمين المنطقى استطاع الكندى فك أسرار الرسائل الشفرية .

❁ ❁ ❁

النهضة الأوربية :

اهتم رهبان العصور الوسطى بتحليل كتاب العهد القديم وكانت لديهم القناعة أنه يحوى مفاتيح شفرية يمكن إذا تم فك لغزها الوصول إلى معانى أعمق . فمثلاً تصوراً أن هناك عملية استبدال حرفى تعتمد على الكلمة العبرية اتاباش Atabash والتى تشمل الحروف أ ، ب ، ث من اللغة العبرية بالإضافة إلى الحرف ش. ومعنى

هذا المفتاح أن يتم استبدال حرف الباء بحرف الشين لأن الباء هو الحرف الثانى فى الترتيب الأبجدى العبرى والشين هو الحرف القبل الأخير من هذا الترتيب ومن ثم يتم استبدال باقى الحروف الواردة فى بداية الترتيب الأبجدى بالحروف الواردة فى نهاية الترتيب الأبجدى وفقاً لنفس التسلسل (الحرف الأول بدل الحرف الأخير، الحرف الثانى بدل الحرف قبل الأخير ...) . ولم تسفر هذه المحاولات عن إنجازات تذكر إلا أنها فتحت الطريق أمام استخدام الأساليب الشفرية التبادلية فى المعاملات التجارية والمدنية وخصوصاً بعد بداية ازدهار التجارة فى عصر النهضة الأوربية واستنبطت أساليب عدة اعتمد جزء منها على التقدم الذى أحرزه المفكرين العرب فى مجال الشفرة .

وكانت بداية استخدام الكود الشفرى فى هذا الوقت حيث تستبدل الكلمة بأكملها بشكل آخر قد يكون كلمة أخرى أو رمز . وبدأت ملامح علم الشفرة تظهر وفقاً للتقسيم التالى :