الشفرة الغير قابلة للكسر

ظل نظام الشفرة إحادى الأبجدية هو النظام السائد لقرون طويلة فى التشفير ، إلا أن الجهد البحثى الذى بدءه العرب والمتمثل فى تحليل ترددات الحروف ومعدلات تكرارها فى اللغة الطبيعية من ناحية وفى النص المشفر من ناحية أخرى وإجراء المقارنة بينهما لتحديد أى الحروف الشفرية يقابل حروف طبيعية أدى إلى تدمير الحواجز الأمنية لهذا النظام .

وأصبح واضحاً أن كاسرى الشفرة فازوا فى هذه الجولة التى هى أحد جولات معركة أبدية ليس لها نهاية بين فريق واضعى الشفرة وفريق كاسرى الشفرة ولكل فريق انتصارات وهزائم .

وقد حقق فريق واضعى الشفرة طفرة إنجازية كبيرة عندما تخلى عن نظام الأبجدية الأحادية Monoalphabetic إلى نظام الأبجدية المتعددة Polyalphabetic وكان ذلك فى أوربا فى القرن الخامس عشر وعلى يد عدد من علماء الرياضيات الإيطاليين والفرنسيين اعتمد فكرهم على أن يتم تبديل حروف النص الواضح بحروف مستقاة من أكثر من ترتيب أبجدى وليس من ترتيب أبجدى واحد .

فعلى سبيل المثال إذا افترضنا التالى :

أبجدية النص الواضح (الأبجدية الطبيعية)	.....	A B C D
أول ترتيب أبجدى	.....	E Z B V
ثانى ترتيب أبجدى	.....	G O X B
⋮		
وهكذا		

فإذا أردنا تشفير كلمة CAB مثلا يتم استبدال حرف C من الأبجدية الأولى ليصبح B ويتم استبدال حرف a من الأبجدية الثانية ليصبح G ويتم استبدال حرف B من الأبجدية الأولى ليصبح Z ومن ثم تصبح الكلمة المشفرة هى BGZ . وتستخدم الترتيبات الأبجدية تبادلياً فيما بينها .

ويعنى استخدام الترتيبات الأبجدية المتعددة فى تشفير النص الواضح إزالة أى علاقة فى تكرار الحروف بين النص الواضح وأى من الترتيبات الأبجدية المستخدمة . وقد قام العالم الفرنسى «بليس دى فيجنيز» Blaise de Vigenère بتطوير هذه الفكرة لتعتمد على ٢٦ ترتيباً أبجديا بدلاً من ترتيبين اثنين فقط وصمم جدول مشهور سمى باسم مربع فيجنير Vigenère square .

الابجدية 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
1	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 A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
8	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
9	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
10	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
11	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
12	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
13	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
14	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
15	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
16	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
17	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
18	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
19	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
20	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
21	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
22	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
23	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
24	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
25	Z 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
26	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

جدول فيجنير

والصف الأعلى فى هذا المربع يمثل حروف النص الواضح ويتم تشفيرها باختيار أى من الترتيبات الأبجدية الـ ٢٦ الأخرى الواردة. فإذا استخدم مثلاً الترتيب الأبجدى الثانى فإن حرف a يتم تشفيره بحرف c ولكن إذا استخدم الترتيب الأبجدى رقم ١٢ فإن تشفير حرف a يصبح M .

ويستطيع الراسل أن يستخدم ترتيباً أبجدياً واحداً فى تشفير رسالته ولكن فى هذه الحالة سيكون تشفيراً ضعيفاً لأنه اعتمد على أبجدية واحدة ويصبح معرض للكسر بسهولة كما سبق وأوضحنا . لذا وفر مربع فيجنير إمكانية استخدام أكثر من ترتيب أبجدى . فقد يرى الراسل استخدام أربعة ترتيبات أبجدية فى تشفير الرسالة بأن يختار أبجديات السطر ٥ ، ١٤ ، ١٨ ، ٢١ ، ٢٥ مثلاً ويجب على مستقبل الرسالة أن يكون على علم بأن هذه الترتيبات الأبجدية هى التى استخدمت حتى يستطيع فك شفرة الرسالة . وبالطبع كلما زاد عدد الترتيبات الأبجدية المستخدمة زادت صعوبة

كسر شفرة الرسالة . ولكن كيف يمكن للمستقبل أن يعلم الترتيبات الأبجدية المستخدمة ؟

هناك طرق عددية ومن أشهرها ما استخدم فعلاً بكثرة وهو الاتفاق على كلمة سر معينة تحدد حروفها ترتيب الأسطر فى جدول فيجنير للترتيبات الأبجدية المستخدمة. فمثلاً إذا اتفق الراسل والمستقبل أن كلمة السر هى WHITE فإن الأسطر المستخدمة فى فك الشفرة هى تلك التى تبدأ بحروف هذه الكلمة فحرف W هو أول حرف فى السطر ٢٢ فيستخدم الترتيب الأبجدى لهذا السطر فى فك شفرة الحرف الأول من الرسالة ، وحرف H هو أول حرف من السطر السابع فيستخدم مع الحرف الثانى من الرسالة ... وهكذا . وبالرغم من الإسهام الواضح لجدول فيجنير فى زيادة صعوبة التشفير إلا أن ذلك لم يعجز فريق كاسرى الشفرة .

ولم يهدأوا وبدأوا يبحثون عن خصائص لغوية تساعدهم على كسر الأبجدية المتعددة لجدول فيجنير .

❁ ❁ ❁

بدء اهتمام الحكومات بشئون الشفرة مع بداية الثورة الصناعية فى القرن الثامن عشر الميلادى ومع تزايد الاتصالات عبر الحدود وارتفاع قيمة محتويات هذه الاتصالات من معانى وموضوعات ونوايا وبالتالى تزايد الاتجاه نحو تشفيرها لحماية ما بها إذا وقعت فى يد الغير .

وبدءت الحكومات فى تحضير وتدريب فرق من محللى الشفرة يعملون فى أماكن معدة خصيصاً لفك شفرة الغير (أعداء أو أصدقاء) . وكانت كل حكومة أوربية تقريباً لديها هذا الفريق فى أماكن كانت تسمى الغرف السوداء Black Chambers وهى عبارة عن أماكن يمكن تشبيهها بالمراكز العصبية للدولة تعمل على فك الشفرات التى تم تجميعها بواسطة أجهزة المخابرات وكانت أشهر تلك الغرف تلك التى أعدتها الحكومة النمساوية وسميت Geheine Kabinets Kanzlei وكانت تعمل وفقاً لجدول زمنى صارم حتى لا ينكشف التأخير الذى يحدث فى توقيتات تسليم البريد نتيجة تعامل هذه الغرفة معه . حيث كان البريد المفترض تسليمه للسفارات الأجنبية فى فيينا يوجه أولاً إلى هذه الغرفة ليصل فى السابعة صباحاً وتتولى مجموعة من السكرتيرات إذابة الأختام ويتولى فريق آخر نسخ محتوى الرسائل ويتواجد خبراء لغويين فى الموقع للجوء إليهم عند الحاجة . وخلال ثلاث ساعات تكون الرسائل قد أعيدت إلى أظرافها وأختامها عليها ويتم إرجاعها إلى هيئة البريد لتوزيعها .

أما الرسائل البريدية الخارجة من السفارات الأجنبية فى فيينا فكانت تصل إلى الغرفة فى الرابعة مساءاً ويعاد إرجاعها إلى هيئة البريد فى السابعة مساءاً . ويتولى فريق محللى الشفرة التعامل مع البريد الذى تم نسخه ، وكانوا يتوزعون فى كبائن معدة وكانت حصيلة عملهم تشكل قيمة مخابراتية عالية لإمبراطور النمسا كما أن بعض المعلومات التى كانوا يكتشفونها كانت تباع لحكومات أوربية أخرى .

وفى هذه الظروف استطاع محللى الشفرة الوصول إلى كسر الأبجدية المتعددة لجدول فيجنير .

❁ ❁ ❁

كسر جدول فيجنير بواسطة باباج :

يعتبر شارلز باباج Charles Babbge من أكثر محللى الشفرة سيطا فى القرن التاسع عشر ، وهو يشتهر أيضاً بأنه أول من وضع أسس الحاسب الآلى الحديث .

ولد فى ١٧٩١ وكان والده من أثرياء رجال البنوك فى لندن ، وفى ١٨٢١ كان يفحص أحد الآلات الحاسبة المستخدمة فى الملاحة البحرية فاكتشف العديد من الأخطاء بها بسبب اعتمادها على العنصر البشرى فى حساب جداولها وبالتالى كان هامش الخطأ عالى . وقد أدى ذلك إلى لفت نظره لاستنباط آلة تحسب قيم جداولها دون تدخل بشرى وقطع شوطاً كبيراً فى هذا المجال كما أن الحكومة البريطانية عاونته فى تحويل أفكاره إلا أنه لم يصل إلى ما كان يصبو إليه وإن كانت محاولاته تلك أسهمت بدرجة كبيرة فى وضع أسس الحاسب الآلى . وفى مجال كسر الشفرة كان لباباج إسهامات مساوية فى الأهمية وكان أبرزها استطاعته كسر شفرة جدول فيجنير وبذلك أصبح من أعظم كاسرى الشفرة منذ أن قام العرب بكسرة شفرة الترتيب الأبجدى الأحادى فى القرن التاسع عشر .

ولم يحتاج باباج فى كسرة شفرة فيجنير لأى آلات أو حسابات معقدة إنما اعتمد فقط على ذكاءه . وقد بدء باباج بكسر كلمة السر التى يعتمد عليها تشفير فيجنير واتبع الأسلوب التالى فى ذلك :

١ – البحث فى النص المشفر عن أى تركيبات حرفية متشابهة وحصرها مع تحديد المسافة بين وحدات كل تركيب منها فمثلاً إذا لاحظ تكرار للأحرف EFIQ وآخر للأحرف WCXYM ثم مجموعة أخرى وهى PSDLP ورابعة ETRL . فإنه يقوم برصد هذه المجموعات ويحسب المسافات فيما بينها (بالأحرف) وعدد مرات تكرار ظهورها . وبالطبع هذه المجموعات ليس لها معنى واضح لأنها مشفرة كل ما فى الأمر أنه اكتشف تكرارها بشكلها المتشابهة .

والمغزى وراء الخطوات السابقة هو أن تكرار ظهور مجموعات من الأحرف فى

النص الشفرى إنما يعنى أن هذه المجموعات هى مفتاح الشفرة الذى يستخدم فى تشفير النص الواضح حرف حرف فإذا كان المفتاح الشفرى طوله ٥ أحرف مثلاً فإن أول خمسة أحرف فى النص الواضح تشفر بواسطته ثم الخمسة التالية وهكذا .

والجدول التالى يوضح المساحة الفاصلة بين تكرار المجموعات المتشابهة والتى يمكن منها استنباط طول المفتاح الشفرى وهو فى هذه الحالة خمسة أحرف .

المجموعات المتكررة	المسافات بين المجموعات المتكررة	الطول المتوقع بالأحرف للمفتاح																	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

لأن هذا الطول هو الأكثر احتمالية بين مختلف المسافات الفاصلة فى الجدول وهى ٩٥ ، ٥ ، ٢٠ ، ١٢٠ وكلها تقبل القسمة على ٥ وهو الطول المتوقع للمفتاح الشفرى .

٢ – بناء على تحديد طول المفتاح وهو خمسة فإنه يمكن تحديد الأحرف من النص الواضح التى شفرت بالحرف الأول من المفتاح وهذه الأحرف هى ١ ، ٦ ، ١١ ، ١٦ .... مما يعنى أنها شفرت وفقاً لأبجدية واحدة Monoalphaberic وبالتالى يمكن بسهولة معرفتها ... وهكذا بالنسبة للأحرف المشفرة بواسطة الحرف الثانى من المفتاح ثم الثالث ثم الرابع ثم الخامس .

بهذه الكيفية استطاع باباج كسر شفرة فيجنير وقد تحقق هذا النجاح فى ١٨٥٤ ولكن هذا الإنجاز لم ينشر إلا فى القرن العشرين مما أدى إلى قيام عالم رياضات بولندى اسمه فريدريش وليام كاسيسكى Friedrich Wilhelm Kasiski باكتشاف هذه الطريقة وبالتالى ارتباطها باسمه حيث سميت فى الأدب العلمى باسم اختبار كاسيكى Kasiski test ولم يرد ذكر باباج بشأنها .

ويرى البعض أن هناك سبب آخر وراء عدم نشر إنجازات باباج فى فك شفرة فيجنير وهو أن موعد النشر تطابق مع نشوب حرب القرم مما أدى إلى تدخل المخابرات البريطانية ومنعت نشر هذه الأعمال حتى تحقق ميزة معلوماتية على عدوهم فى الحرب وهم الروس ولا تلفت نظرهم إلى اختراق الشفرة التى كانوا سيستخدمونها وضغطت على باباج لمنع النشر .