جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل _ كلية التربية للعلوم الصرفة

قسم الرياضيات

انظمة التشفير التقليدية والحديثة

Classical and Modern Cipher Systems

مشروع بحث مقدم الى مجلس كلية التربية للعلوم الصرفة _ قسم الرياضيات

كجزء من متطلبات نيل درجة البكالوريوس في الرياضيات

من قبل الطالب

ناجي جاسم عبد الحمزه ناصر

بأشراف

د. طفول حسين

١٤٤٥هـ **٢٠٢٤م**

بسم الله الرحمن الرحيم

قال تعالى :

﴿ هُوَ الَّذِي بَعَثَ فِي الْأُمِّيِّينَ رَسُولًا مِّنْهُمْ يَتْلُو عَلَيْهِمْ آيَاتِهِ وَيُزَكِّيهِمْ وَيُعَلِّمُهُمُ الْكِتَابَ وَالْحِكْمَةَ وَإِن كَانُوا مِن قَبْلُ لَفِي ضَلَالٍ مُّبِينٍ ﴾

صدق الله العلي العظيم

﴿ سورة الجمعة ، الآية : ٢ ﴾

اقرار المشرف

أشهد إن إعداد البحث الموسوم بعنوان (**نظام التشفير انظمه التشفير التقليديه والحديثه** Cipher system's), من قبل الطالب **(ناجي جاسم عبد الحمزه ناصر)** قد جرت تحت اشرافي في قسم الرياضيات – كلية التربية للعلوم الصرفة – جامعة بابل كجزء من متطلبات نيل شهادة البكالوريوس في الرياضيات .

التوقيع :

المشرف :- **أ. م. د. طفول حسين**

المرتبة العلمية: **استاذ مساعد**

التاريخ : / / ٢٠٢٤

توصية رئيس قسم الرياضيات

بناءاً على التوصيات المتوفرة ارشح هذا البحث للمناقشة

التوقيع :

اسم رئيس القسم الرياضيات : **أ. د.**

المرتبة العلمية : **أستاذ**

التاريخ : / / ٢٠٢٤

الاهداء

بسم الله والحمد لله والصلاة والسلام على حبيب الله محمد وال بيته الطيبين الطاهرين الحمد لله الذي وفقنا لهذه الخطوة في مسيرتنا الدراسية نهدي هذا الجهد المتواضع الى سيدنا ومولانا صاحب الزمان ارواحنا لتراب مقدمه الفداء .

والى المضحين الذين اهدوا للعراق ارواحهم ليستمر ويمضي قدما والى الوالدين الكريمين حفظهما الله وادام ظلهم الوارف علينا والى من رافقني اثناء المسيرة الدراسية اخوتي واصدقائي

والى مربي الاجيال وبناة المجتمع اساتذتي الكرام الافاضل

ناجي

الشكر والعرفان

الحمد لله حمداً يليق بجلاله والشكر له على توفيقه وامتنانه، فالحمد الله الذي هدانا للإسلام وأرشدنا للعلم ووفقنا للخير والشكر لله سبحانه أن من علي بإتمام هذه الدراسة، والصلاة والسلام على نبينا محمد وعلى آله الطيبين الطاهرين...

فالشكر بعد شكر الله تعالى الى عائلتي وكل من ساعدني ولمن كانت له اليد في إنجاز هذا البحث واختص بالذكر **(الدكتورة : طفول حسين)** المشرفة على هذا البحث

كما لا يسعني إلا أن أتقدم بجزيل الشكر ووافر التقدير للأساتذة في قسم الرياضيات على ما قدموه لي من توجيه وإرشاد في جميع مراحل الدراسة.

ناجي

جدول المحتويات

ت	العنوان	الصفحة
	الخلاصة	
الفصل الاول : الخوارزميات التاريخية		
١-١	المقدمة	١
١-٢	شفرة القيصر	٢
١-٣	شفرات الاستبدال البسيط	٦
١-٤	أحصائيات اللغة الانكليزية	٨
١-٥	شفرة بلايفير	١٠
١-٦	الترميز المتناغم	١٢
١-٧	التشفير متعدد الاحرف	١٣
١-٨	التشفير التبادلي	١٦
١-٩	التشفير المعقد	١٧
الفصل الثاني : الخوارزميات الحديثة		
٢-١	المقدمة	٢٠
٢-٢	سلاسل الرقم الثنائي (البث)	٢٠
٢-٣	شفرات التدفق	٢٢
٢-٤	نظام الشفرات الكتل (نمط كتاب الشفرات الالكتروني)	٢٤
٢-٥	دوال الاختزال	٢٧
٢-٦	الاستنتاجات	٣٢
	المصادر	٣٣

الخلاصة

التشفير هو عبارة عن ممارسة حماية المعلومات باستخدام الخوارزميات المشفرة وعلامات التجزئة والتوقيعات. يمكن أن تكون المعلومات غير نشطة (مثل ملف على القرص الصلب)، أو متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)، أو قيد الاستخدام (أثناء الحوسبة على البيانات). التشفير له أربعة أهداف أساسية:

١ السرية - إتاحة المعلومات للمستخدمين المصرح لهم فقط.
٢ النزاهة - ضمان عدم التلاعب بالمعلومات.
٣ المصادقة - تأكيد صحة المعلومات أو هوية المستخدم.
٤ عدم الإنكار - منع المستخدم من إنكار الالتزامات أو الإجراءات السابقة.

يستخدم التشفير عددًا من خوارزميات التشفير لتحقيق واحد أو أكثر من أهداف أمان المعلومات هذه. تتضمن هذه الأدوات خوارزميات التشفير وخوارزميات التوقيع الرقمي وخوارزميات التجزئة ووظائف أخرى.

سنتناول في هذا البحث عددًا من خوارزميات التشفير الأكثر استخدامًا. في الفصل الاول تم استعراض الطرق التقليدية القديمة ابتداءً بشفرة قيصر، والتي تعد من اقدم الشفرات المستخدمة، وانتهاءً بالتشفير المعقد. وفي الفصل الثاني تم التطرق الى بعض الخوارزميات الحديثة مثل شفرات التدفق وانظمة المفتاح المعلن.

الفصل الاول

الخوارزميات التاريخية

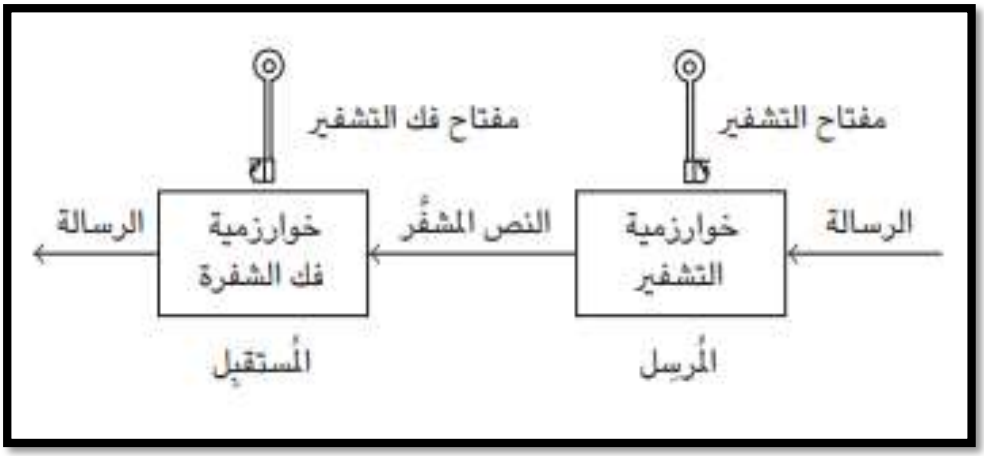
الفصل الاول

الخوارزميات التاريخية

١-١ مقدمة

تتمثل فكرة أي نظام تشفير في إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أي شخص غير مصرح له بالاطلاع عليها . يتمثل الاستخدامان الأكثر شيوعًا للتشفير في تخزين البيانات بأمان في ملف كمبيوتر أو نقلها عبر قناة غير آمنة مثل الإنترنت في كلتا الحالتين حقيقة كون المستند مشفرا لا تمنع الأشخاص غير المصرح لهم بالوصول إليه ، ولكنها تضمن عدم تمكنهم من فهم ما يرونه . غالبا ما يطلق على المعلومات المراد إخفاؤها اسم النص الأصلي ، فيما يطلق على عملية إخفائها اسم « التشفير .. ويطلق على النص الأصلي المشقر اسم « النص المشفر ، أو بيان التشفير كما يطلق على مجموعة القواعد المستخدمة في تشفير معلومات النص الأصلي خوارزمية التشفير » . عادةً ، تعتمد هذه الخوارزمية على « مفتاح التشفير » ؛ وهو يمثل مدخلا لها بالإضافة إلى الرسالة وحتى يتمكن المتلقي من استرجاع الرسالة من خلال النص المشفر . يجب أن تتوافر خوارزمية فك التشفير التي عند استخدامها مع مفتاح فك التشفير المناسب ، تسترجع النص الأصلي من النص المشفر [١].

يبين الشكل (١-١) التالي وصفا تخطيطيا لأستخدام أحد أنظمة التشفير لحماية رسالة منقولة :



الشكل (١-١) يبين وصفا تخطيطيا لأستخدام أحد أنظمة التشفير لحماية رسالة منقولة

يطلق على كلِّ مَن يعترض رسالة خلال انتقالها اسم معترض . هذا ، ويستخدم مؤلفون آخرون أسماء أخرى مثل متنصت ، و « خصم » ، و « غريم » ، و « شخص سيئ » .

في هذا الفصل نقدِّم بعض الأمثلة البدائية لتوضيح الأفكار الأساسية الخاصة بموضوع الفصل . نضرب هذه الأمثلة أيضًا لإلقاء بعض الضوء على نوع الهجمات التي قد تشنها الأطراف المعترضة ، ولبيان بعض الصعوبات التي يواجهها مصممو الخوارزميات . تنتمي جميع أمثلة الخوارزميات المذكورة هنا إلى النوع المتناظر ، وهي أمثلة لخوارزميات أمثلة جرى تصميمها واستخدامها قبل وقت طويل من اقتراح نظم التشفير ذات المفتاح المعلن كما تم طرح المبادئ الرياضية الأساسية فيها ، خاصة علم المقياس الحسابي . وأيضا سوف نطرح أمثلة رياضية توضيحية مبسطة .

تعتبر أمثلة الخوارزميات هذه قديمة ولا تعبر في واقع الأمر عن أي من أساليب التشفير الحديثة . ومع ذلك من الأهمية بمكان دراسة عدد من الأنظمة البدائية كان يجري التشفير فيها من خلال استبدال الأحرف بعضها ببعض ، فيما يُطلق عليه استبدال الأحرف ، أو تغيير ترتيب الأحرف . يوجد عدد من الأسباب وراء ذكر مثل هذه الأمثلة ؛ أولها : تمكننا هذه الأنظمة من ضرب أمثلة بسيطة وسهلة الاستيعاب تبين المفاهيم الأساسية ، كما تمكننا من بيان عدد من نقاط الضعف في الشفرات . كما يوجد سبب آخر يتمثل في كونها أمثلة تقدم متعة بالغة في حلها .

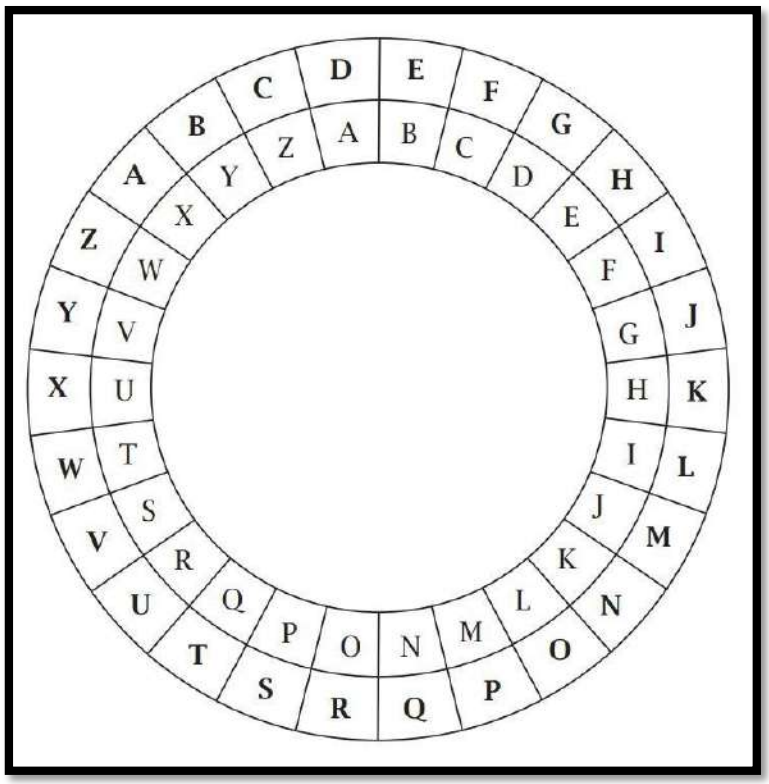
٢-١ شفرة القيصر [٢ ,١]

كانت « شفرة قيصر » ، التي ذكرها يوليوس قيصر في كتابه « الحروب الغالية » ، من أوائل الأمثلة على استخدام الشفرات وفق هذه الشفرة ، يجري تشفير الأحرف من A إلى W من خلال تمثيل كلٌّ منها بالحرف الثالث بعده في ترتيب الأبجدية .

بينما يجري تمثيل الأحرف X ، و Y ، وبالأحرف A و B و C على الترتيب . وعلى الرغم من استخدام قيصر « عملية إزاحة تتألف من ثلاثة أحرف كان يمكن تصميم شفرة مشابهة من خلال استخدام أي . عدد من ١ إلى ٢٥ في واقع الأمر ، يُنظر إلى أي عملية إزاحة في نظام التشفير بوصفها مثالا لشفرة قيصر . مرة أخرى نستخدم رسما توضيحيا لبيان إحدى شفرات قيصر ؛ يمثل الشكل الموضح حلقتين تتمحوران حول مركز واحد ؛ حيث تمتلك الحلقة الخارجية منهما حرية الدوران . إذا بدأنا بالحرف A في الحلقة

الخارجية حول حرف A في الحلقة الداخلية ، فإن الإزاحة بمقدار ٢ ستؤدي إلى وجود حرف C قبالة الحرف A وهكذا . هناك ، إذن ، ٢٦ وضع ضبط بما في ذلك إزاحة مقدارها صفر التي هي بطبيعة الحال نفس الإزاحة التي مقدارها (٢٦) ويحدد عدد حركات الإزاحة مفتاح التشفير ومفتاح فك التشفير في شفرة قيصر .

بمجرد الموافقة على عدد حركات الإزاحة تتحقق عملية التشفير في شفرة قيصر من خلال النظر إلى كل حرف من حروف النص الأصلي على أنه بمنزلة حلقة داخلية والاستعاضة عنه بالحرف الذي يقع قبالته في الشكل الموضح . وفي عملية فك التشفير نجري العملية العكسية من هنا وفق الشكل (١-٢) ، يتمثل النص المشفر لرسالة النص الأصلي DOG في GRJ عند الإزاحة بمقدار ٣ حركات ، بينما يكون CAT هو النص الأصلي المكافئ للنص المشفر FDW من أجل منح القارئ مزيدًا من الثقة في فهم نظام شفرة قيصر نطرح أربع عبارات للتأكد . إذا كان عدد حركات الإزاحة ٧ ، فسيكون نص التشفير المناظر للنص الأصلي VERY هو ، CLYF ، بينما يكون النص الأصلي SUN ، عند الإزاحة ١٧ حركة ، هو النص المناظر للنص المشفر JLE .



الشكل (١-٢) يوضح ماكينة تنفذ شفرة قيصر .

في عرضنا لشفرة قيصر ، يكون كلٌّ من مفتاح التشفير ومفتاح فك التشفير مساويًا لعدد حركات الإزاحة بينما تختلف قواعد التشفير وفك التشفير . ومع ذلك كان بإمكاننا تغيير الصياغة قليلا بحيث تتطابق القاعدتان بينما تختلفان في مفاتيح التشفير وفك التشفير . نرى ذلك مثلا عند الإزاحة بمقدار صفر أو ٢٦ حيث يتحقق الأثر نفسه ، وعند الإزاحة بعدد حركات يتراوح بين صفر و ٢٥ يكون التشفير مع هذا العدد من حركات الإزاحة مكافئًا لفك التشفير مع عدد حركات الإزاحة الجديد الذي يجري الحصول عليه - من خلال طرح عدد حركات الإزاحة الأصلي من ٢٦ . لذا - على سبيل المثال . يكون التشفير عند الإزاحة بمقدار ٨ حركات مكافئًا لفك التشفير عند الإزاحة بعدد حركات ١٨ = ٨ - ٢٦ يمكننا ذلك من استخدام القاعدة نفسها في عمليتي التشفير وفك التشفير من خلال إجراء عملية فك تشفير بالإزاحة ١٨ حركة تكافئ التشفير بالإزاحة ٨ حركات . ذكرنا سابقا عمليات البحث الشاملة المرهقة عن المفاتيح ، ومن البديهي أنه أن هناك ٢٦ حرفًا فقط لا غير يعتبر نظام شفرة قيصر عرضة لمثل هذا النمط من بما الهجمات قبل أن نضرب مثلا على كيفية تحقيق ذلك ، يجب الإشارة إلى أحد مواطن الضعف الأخرى لهذا النظام يمكن تحديد المفتاح من خلال معرفة زوج واحد من حروف النص الأصلي والنص المشفر المقابل له ، وهو ما يُعد قدرًا ضئيلا للغاية من المعلومات .

أسهل طريقة لتوضيح عملية البحث الشاملة عن المفتاح هي عرض مثال كامل وسهل – بما أنه : ٢٦ مفتاحًا فقط . النظام شفرة قيصر .

لنفترض أننا نعرف أن - يوجد - نظام شفرة قيصر يجري استخدامه ، وأننا نتوقع رسالة باللغة الإنجليزية ، وأننا نجحنا في اعتراض النص المشفّر .XMZVH . إذا كان المرسل أجرى ٢٥ حركة إزاحة لتنفيذ عملية التشفير فستُجرى عملية فك التشفير إذن من خلال إجراء حركة إزاحة واحدة ؛ بحيث يكون YNAWI هو نص للرسالة . وبما أن تلك الرسالة لا معنى لها في اللغة الإنجليزية يمكننا أن نستبعد باطمئنان العدد ٢٥ كقيمة لعدد حركات الإزاحة . يبين جدول ٣-١ نتيجة محاولات الانتقال بصورة منهجية بعدد حركات إزاحة من ٢٥ إلى ١ بترتيب تنازلي . لا توجد كلمة إنجليزية واحدة في جدول (١-٢) ذات معنى سوى كلمة CREAM ؛ ومن ثَم ، يمكن أن نستنبط من ذلك أن مفتاح التشفير هو ، ٢١ ، وهو ما يمكننا من فك شفرة جميع الرسائل المستقبلية إلى حين تغيير المفتاح وعلى الرغم من النجاح الكامل لعملية البحث الشاملة هذه عن المفتاح من الأهمية بمكان إدراك أنه في حالة الشفرات الأكثر تعقيدًا قد لا يمكن تحديد المفتاح على وجه الدقة من خلال عملية بحث شاملة واحدة فقط ؛ كل ما هنالك أنه على الأرجح ، سيحد من عدد الاحتمالات من خلال استبعاد الاحتمالات غير الواردة تمامًا .

مثال على ذلك ، وبالعودة إلى شفرة قيصر ، نلاحظ أن إجراء عملية بحث شاملة عن مفتاح التشفير للنص المشفر HSPPW يؤدي إلى احتمالين تتولد عنهما كلمتان إنجليزيتان ذواتا معنى للرسالة المفترضة . يتمثل الاحتمالان في احتمال حركات إزاحة عددها ٤ تكشف عن كلمة DOLLS ، واحتمال حركات إزاحة عددها ١١ تكشف عن كلمة (WHEEL) عندما يحدث ذلك نحتاج إلى توفر المزيد من المعلومات ، ربما سياق الرسالة المفترضة أو المزيد من نص التشفير قبل أن نتمكن من تحديد المفتاح على وجه الدقة . وعلى الرغم من ذلك ، تشير نتيجة البحث الشاملة عن المفتاح أننا قللنا من عدد احتمالات المفاتيح كثيرًا ، وأننا إذا اعترضنا المزيد من النص المشفر ، فلن نحتاج إلى إجراء عملية بحث شاملة أخرى . في حقيقة الأمر ، في حالة هذا المثال البسيط ، لن نحتاج إلا لتجريب قيمتين فقط لعدد حركات الإزاحة ؛ وهما ٤ و ١١ .

جدول (١-١) مثال على عملية بحث شامل عن المفتاح : نص مشفرة XMZVH .

مفتاح التشفير	«الرسالة» المفترضة	مفتاح التشفير	«الرسالة» المفترضة	مفتاح التشفير	«الرسالة» المفترضة
0	XMZVH	9	FUHDP	18	ODQMY
25	YNAWI	10	ETGCO	19	NCPLX
24	ZOBXJ	11	DSFBN	20	MBOKW
23	APCYK	12	CREAM	21	LANJV
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	14	JYLHT	5	SHUQC
20	DSFBN	15	IXKGS	6	RGTPB
19	ETGCO	16	HWJFR	7	QFSOA
18	FUHDP	17	GVIEQ	8	PERNZ

ثمة ملاحظة أخرى مثيرة للاهتمام في هذا المثال . فخلال حله ، سيكتشف القارئ كلمتين إنجليزيتين تتألفان من خمسة أحرف ؛ بحيث يجري الحصول على واحدة من خلال الأخرى باستخدام شفرة قيصر عن طريق إجراء عدد ٧ حركات إزاحة . ربما ترغب في أن تمضي في إجراء ذلك وأن تحاول العثور على أزواج من كلمات أطول ، بل وربما عبارات ذات معنى تكون كلٌّ منها ناتجة عن حركات إزاحة للأخرى . يتبين من هذا المثال البسيط سهولة كسر شفرات قيصر . ومع ذلك نجح يوليوس قيصر في استخدامها ؛ ربما لأن أعداءه لم يجُلْ بخاطرهم استخدامه أي شفرات في ذلك الوقت .

٣-١ شفرات الاستبدال البسيط

على الرغم من أن توافر عدد كبير من المفاتيح يعتبر شرطًا ضروريا لتحقيق الأمن في عملية التشفير ، فمن الأهمية بمكان الإشارة إلى أن توفر عدد كبير من المفاتيح لا يضمن بالضرورة قوة نظام التشفير من الأمثلة على ذلك شفرة الاستبدال البسيط (أو الشفرة أحادية الأحرف التي نعرضها تفصيلا هنا .

ان عرض هذه الشفرة يبين مخاطر الاعتماد على عدد كبير من المفاتيح كمؤشر على قوة الشفرة ، بل يبين أيضًا كيف يمكن استغلال الإحصاءات اللغوية في هذه الحالة الإنجليزية من قبل الطرف المعترض . في حالة شفرات الاستبدال البسيط نكتب الأحرف الأبجدية عشوائيا تحت أحرف الهجاء تماما كما مرتبة أبجديا ، مثلما هو موضح هنا هي تتساوى مفاتيح التشفير وفك التشفير ؛ إذ تتمثل في ترتيب الأحرف المكتوبة بخط عريض . تتمثل قاعدة التشفير في تبديل كل حرف بالحرف الذي يقع تحته فيما تتمثل - قاعدة فك التشفير في تنفيذ الإجراء نفسه على نحو معاكس . من هنا - على سبيل المثال - يتم تمثيل كلمة GET بالأحرف ZTP في النص المشفر ، فيما يتم تمثيل كلمة BIG في النص المشفر بالأحرف IYZ . لاحظ على ذكر هذا المثال [١]:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

أن شفرة قيصر تعتبر حالة خاصة من شفرات الاستبدال البسيط ؛ إذ لا يعدو الترتيب الذي جرت معه كتابة الأحرف بالخط العريض مجرد عملية إزاحة للحروف الأبجدية . يساوي عدد مفاتيح شفرات الاستبدال البسيط عدد طرق ترتيب الأحرف الستة والعشرين الهجائية ، وهو ما يطلق عليه مضروب العدد ٢٦ (وهو حاصل ضرب جميع الأعداد الصحيحة الموجبة التي تقل عن ٢٦ أو تساويه) ، أي :

١ × ٢ × ٣ × ... × ٢٤ × ٢٥ × ٢٦ ؛ أي ما يساوي :

٤٠٣,٢٩١,٤٦١,١٢٦,٦٠٥,٦٣٥,٥٨٤,٠٠٠,٠٠٠

هذا لا شك رقم كبير وليس من المحتمل أن يحاول أحد التوصل إلى المفتاح من خلال إجراء عملية بحث شاملة . لكن وجود مثل هذا العدد الضخم من المفاتيح له مشكلاته ، وهناك فضلا عن ذلك عدد من الملاحظات تتصل بمشكلات إدارة المفاتيح التي تصاحب استخدام شفرات الاستبدال البسيط تتمثل الملاحظة البديهية الأولى في طول وصعوبة تذكر المفتاح ، على خلاف شفرة قيصر ؛ من ثَمَّ ، عندما كان هذا النوع من الأنظمة يُستخدم يدويا ، في عصر ما قبل الكمبيوتر ، كانت تجري عادةً كتابة المفتاح في ورقة . وفي حال الاطلاع على هذه الورقة أو سرقتها ، يجري اختراق النظام .

وفي حال فقدان الورقة جميع الرسائل المشفرة ؛ بمعنى أنه كان يتعين على المتلقي المقصود للرسائل أن « تفقد » يتولى كسر الخوارزمية لبيان محتوى الرسائل للتغلب على هذا النوع من المخاطر ، حاول المستخدمون اكتشاف أساليب لتصميم مفاتيح يسهل تذكرها كان أحد هذه الأساليب يتمثل في التفكير في « جملة المفتاح » ، والتخلص من جميع الحروف المتكررة ، وجعل هذه الصيغة هي « بداية » تصميم المفتاح ثم التوسع في تصميم المفتاح من خلال إضافة الأحرف المتبقية مرتبة هجائيا . لذا - على سبيل المثال :- إذا كانت جملة المفتاح We hope you enjoy this book (نأمل أن تستمتع بقراءة هذا الكتاب) تصبح بداية المفتاح بالتخلص من الحروف المتكررة wehopyunjtisbk ؛ ومن ثُمَّ يصير المفتاح كاملا WEHOPYUNJTISBKACDFGLM Q R VX Z

مثال (١-١) : HKC ماذا يمكن أن نقول ؟ ليس كثيرًا . بما أنه ليس هناك معلومات أخرى ، قد تشير الرسالة إلى أي متتالية ذات معنى من ثلاثة أحرف متمايزة . بالطبع يمكننا أن نستبعد بعض المفاتيح ، لنقل تلك المفاتيح التي تشفّر ٢ إلى H ، و إلى K ، و K إلى C آنيا . في المقابل ، لا يزال عدد الاحتمالات المتبقية كبيرًا للغاية ؛ ما يجعلنا نستدرج إلى القول بأن مجرد اعتراض النص المشفر هذا لا يفيدنا في شيء من الصحيح تماما أننا إذا أردنا إرسال رسالة واحدة تتألف ثلاثة أحرف فقط ، فستبدو شفرات الاستبدال البسيط مناسبة ، وأن إجراء عملية بحث شاملة للنص المشفر سيسفر عن جميع الكلمات المؤلفة من ثلاثة من أحرف (بأحرف متمايزة) كرسائل محتملة .

مثال (١-٢) : HATTPT في هذا المثال ، نستطيع بالتأكيد حصر عدد الاحتمالات لعدد حروف النص الأصلي التي قد تحول إلى الحرف T ربما نستطيع أيضًا الاستنباط في يقين أن أحد أحرف T أو P في

الاحتمالات . المثال تمثل حرفًا متحركًا . بالإضافة إلى ذلك ، إذا كان لدينا ما يجعلنا نعتقد أن الرسالة المعترضة . هي عبارة عن كلمة واحدة كاملة ، فربما سنتمكن من كتابة جميع بعض الأمثلة على ذلك كالآتي :

CHEESE ، و MISSES ، و CANNON .

١-٤ إحصاءات اللغة الإنجليزية

كانت الأمثلة في القسم السابق جميعها قصيرة وجرى انتقاؤها بعناية لبيان نقاط محددة . لكنه ، حتى في حال استخدام شفرات الاستبدال البسيط لتشفير مقاطع طويلة من نص إنجليزي ، يوجد عدد من أساليب الاعتراض المباشر التي تسمح بالكشف عن محتوى الرسالة والمفتاح ، أو على الأقل الجزء الأكبر من المفتاح تستعين أساليب الاعتراض هذه بخصائص معروفة في اللغة الإنجليزية . يبين جدول (٢-١) معدلات التكرار في صورة نسب ، لأحرف الهجاء في عينة تتألف من أكثر من ٣٠٠ ألف حرف مأخوذة من مقاطع في عدد من الصحف والروايات . يعتمد هذا الجدول على جدول آخر نُشر في كتاب « أنظمة التشفير حماية الاتصالات » لمؤلَّفَيْه إتش جيه بيكر وإف سي بايبر .

يتماشى تمثيل الأحرف في هذا الجدول مع العديد من الجداول الأخرى التي وضعها مؤلفون آخرون ؛ إذ يمكن تفسير هذه الأحرف على أنها تمثل معدلات التكرار المتوقعة للأحرف في أي نص إنجليزي . تُظهر هذه الإحصائية بجلاء احتمالية هيمنة عدد محدود للغاية من الأحرف على أي نص إنجليزي.

جدول (١-٢) معدلات التكرار النسبية المتوقعة للأحرف في نص أنكليزي

٪	حرف	٪	حرف
6.7	N	8.2	A
7.5	O	1.5	B
1.9	P	2.8	C
0.1	Q	4.2	D
6.0	R	12.7	E
6.3	S	2.2	F
9.0	T	2.0	G
2.8	U	6.1	H
1.0	V	7.0	I
2.4	W	0.1	J
2.0	X	0.8	K
0.1	Y	4.0	L
0.1	Z	2.4	M

عند استخدام شفرات الاستبدال البسيط ، يحلُّ محلَّ كل حرف من حروف الأبجدية الحرفُ نفسه الذي جرى استبداله ، أيا كان موضعه في النص . من ثم ، إذا استخدمنا تشفيرا - على سبيل المثال – يحل فيه حرفُ R محل حرف E ، فسيظل معدل تكرار حرف R في النص المشفر مساويًا لمعدل تكرار حرف E في الرسالة ؛ وهو ما يعني أنه إذا عَكَس جدول (١-٢) معدل تكرار الحروف في رسالة ما ، فستُظهر معدلات تكرار الأحرف في النص المشفر عدم التوازن نفسه ، وإن كانت معدلات تكرار الأحرف موزعة على نحو مختلف بينها . لبيان ذلك أكثر ، نعرض الرسم البياني لمعدلات تكرار الأحرف في نص مشفر طويل جرى الحصول عليه عن طريق شفرات الاستبدال البسيط . THE بمقارنة جدول(١-٢) بهذا الشكل ، ربما يستطيع أحد محللي الشفرات تخمين أن H تمثل E وأن W تمثل . وبما أن أكثر الثلاثيات شيوعًا في اللغة الإنجليزية هي فسيكتسب الطرف المعترض ثقة في هذا الافتراض من خلال التأكد مما إذا كان أكثر الثلاثيات شيوعًا في النص المشفّر هو *W ؛ حيث تمثل * حرفًا ثابتا – وهو ما لا يدعم محاولات التخمين الأولى فقط بل يشير إلى أن النص الأصلي المكافئ للحرف * هو H.

الفقرة التالية التي جرى تشفيرها باستخدام شفرات الاستبدال البسيط :

DIX DR TZX KXCQDIQ RDK XIHPSZXKPIB TZPQ TXGT PQ TD QZDM TZX KXCJXK ZDM XCQPVN TZPQ TNSX DR HPSZXK HCI LX LKDUXI.

TZX MDKJ QTKFHTFKX DR TZX SVCPITXGT ZCQ LXXI SKXQXKWXJ TD OCUX TZX XGXKHPQX XCQPXK .

PR MX ZCJ MKPTTXI TZX HKNSTDBKCOPI BKDFSQ DR RPWX VXTTXKQ TZXI PT MDFVJ ZCWX LXXI ZCKJXK .

TD HDIWPIHX NDFKQXVWXQ DR TZPQ SCPKQ SCPKQ DR KXCJXKQ HCI SKDWPJX XCHZ DTZXK MPTZ HKNSTDBKCOQ MPTZ TZPQ VXTTXK BKDFSIB.

ان وجود مسافات بين الكلمات يسهل من عملية فك الشفرة للنص اعلاه. وكان فك الشفرة سيصبح أكثر صعوبة بكثير حال جرى حذف المسافات بين الأحرف الإنجليزية . النص نختم هذه المناقشة القصيرة بالإقرار بأننا لم نحدد على وجه الدقة حجم المشفّر الذي نعتبره « طويلًا » . لا توجد بطبيعة الحال إجابة دقيقة . وفي حين يعتبر توفر ٢٠٠ حرف كافيًا بكل تأكيد للاعتماد على نتائج الإحصاءات ، وجدنا أن الطلاب يستطيعون فك شفرة رسالة يتضمن نص مشفّرها ١٠٠ حرف أو أكثر .

كملاحظة جانبية ، نؤكد على عدم وجود ضمانة في أن تتطابق الإحصاءات لأي رسالة مع الإحصاءات في جدول ١-٢ . على سبيل المثال ، إذا جرى تشفير خطاب شخصي فمن الأرجح أن تظهر كلمة you (أنت) بكثرة مثل كلمة the أداة التعريف « أل » .

١-٥ شفرة بلايفير

ابتكر « شفرة بلايفير » السير تشارلز وتستون والبارون ليون بلايفير في عام ١٨٥٤ وجرى استخدامها من قبل إدارة الحرب البريطانية حتى بداية القرن العشرين ، وقد استُخدِمَتْ . في حرب البوير . وتُعد هذه الشفرة مثالاً على نظام شفرة « الكلمات ثنائية الأحرف » ؛ وهو ما يعني تشفير الأحرف أزواجًا في مقابل تشفيرها مفردةً . يتمثل المفتاح في مربع يتألف من خمسة أحرف طولا وعرضًا يحتوي المربع على ٢٥

حرفًا تتكون من خلال حذف حرف J من الأبجدية ؛ ومن ثَمَّ يكون لدينا المضروب ٢٥ أو عدد مفاتيح يساوي : ١٥ , ٥١١ , ٢١٠ , ٠٤٣ , ٣٣٠ , ٩٨٥ , ٩٨٤,٠٠٠,٠٠٠

قبل إجراء عملية التشفير باستخدام شفرة بلايفير يجب إعادة ترتيب الرسالة قليلًا . لتنفيذ ذلك :

- يجب استبدال كل حرف I بحرف J .
- كتابة الرسالة في أزواج من الأحرف .
- عدم السماح بوجود أزواج أحرف متطابقة ، وإن وجدت يُدرج حرف ٢ بينها .
- إضافة حرف Z في النهاية إذا كان عدد الأحرف فرديا .
- لبيان طريقة عمل نظام شفرة بلايفير سنختار مفتاحًا محددًا لا يوجد ما يميز اختيارنا له .

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

الشكل (١-٣) يوضح عملية التشفير الرسالة باستخدام شفرة بلايفير

بمجرد إعادة ترتيب الرسالة على نحو مناسب ، نعرض قاعدة التشفير في نظام شفرة بلايفير . لبيان طريقة التشفير سنتوسع في تصميم المفتاح بإضافة عمود سادس وصف سادس للمفتاح الأصلي . ويتطابق الصف السادس مع الصف الأول ، في حين يتطابق العمود السادس مع العمود الأول ؛ من ثُمَّ - على سبيل المثال . يمكن التوسع في تصميم مفتاح كما هو موضح في الشكل(١-٤) :-

S	T	A	N	D	S
E	R	C	H	B	E
K	F	G	I	L	K
M	O	P	Q	U	M
V	W	X	Y	Z	V
S	T	A	N	D	

الشكل (١-٤) يوضح عملية التشفير الرسالة باستخدام شفرة بلايفير

تتلخص قاعدة التشفير في نظام شفرة بلايفير في الآتي :

١. إذا وقع الحرفان في الصف نفسه من مربع المفتاح يحل محل كل حرف الحرفُ الذي إلى يمينه في مربع المفتاح الممتد .
٢. إذا وقع الحرفان في العمود نفسه من مربع المفتاح ، يحل محل كل حرف الحرفُ الذي يقع إلى الأسفل منه في مربع المفتاح الممتد .
٣. إذا لم يقع الحرفان في الصف أو العمود نفسه ، يحل محل الحرف الأول الحرفُ الذي يقع في صف الحرف الأول وعمود الحرف الثاني . ويحل محل الحرف الثاني الحرفُ الذي في الركن الرابع من المستطيل الذي تشكل من الحروف الثلاثة المستخدمة حتى الآن .

١-٦ الترميز المتناغم

يتمثل خيار آخر لتطوير نظام شفرات الاستبدال البسيط في التوسع في الأحرف الهجائية من خلال إضافة بعض الرموز الزائدة ؛ بحيث يُمثَّل - على سبيل المثال – حرف النص الأصلي E بأكثر من رمز في نص التشفير . يُطلق على هذه الرموز الزائدة العناصر العشوائية ، كما تُسمى عملية التوسع في الأحرف الهجائية بعملية الترميز المتناغم لبيان ذلك ، نطرح شفرة تكون فيها عناصر الأعداد ٠٠ ، ٠١ ، ٠٢ ، ... ، ٣١. يمثل كل عدد في النص المشفر حرفًا واحدًا فقط في النص الأصلي ، لكن كل حرف من الأحرف A و E و N و O و R و T يجري النص المشفر هي تمثيله برمزين مختلفين . لبيان ذلك أكثر ، نخصص أعدادًا للأحرف مثلما هو موضح في الشكل التالي :

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
01	07	14	21	04	13	27	20	29	31	06	28	12	30	17	00
N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
18	26	19	09	10	25	23	02	08	24	22	05	16	15	11	03

الشكل (١-٥) نخصص أعدادًا للأحرف في الترميز المتناغم

إذا فعلنا ذلك ، فقد يصبح من الممكن كتابة كلمة TEETH ، التي تحتوي على زوجين من الأحرف المتكررة ، كالآتي : ٢٤٢٧١٣٠٨٣١ لمن لا يعرف المفتاح ، تعتبر الأعداد الخمسة المكونة للنص المشفر مختلفة لكن لن يكون هناك احتمال لتعرُّض المتلقي الحقيقي للرسالة للارتباك . الأرجح أن تكون الأحرف الستة المنتقاة . هي الأحرف الستة الأكثر انتشارًا في النص الأصلي . على سبيل المثال ، إذا كان قرار تحديد أي من العددين المنتَقَيْنِ يمثل الحرف E قرارًا عشوائيا ، فسنتوقع أن يشغل كلٌّ من العددين حوالي ٦ % من النص المشفر . وعلى وجه العموم ، تتمثل نتيجة استخدام الترميز المتناغم في ضمان أن يكون المدرج التكراري المتوقع للنص المشفر أكثر انبساطا من المدرج التكراري للنص الأصلي ، وهو ما يجعل عملية الاعتراض من خلال استخدام الإحصاءات اللغوية أكثر صعوبة .

ملاحظة ١: في هذه الشفرة ، نكتب ٠٠ ٠١ ٠٢ لنمثل الأعداد ٠ ، ١ ، ٢ ... إلخ . ففي أي وقت لا تُستخدم فيه المسافات ، يُستخدم هذا النوع من التمثيل الرقمي للتمييز بين « اثني عشر » و « واحد يليه اثنان على سبيل المثال .

ملاحظة ٢: يعتبر كسر شفرات الاستبدال البسيط سهلا نسبيا , أما هذا النوع من التشفير الذي نناقشه فيتطلب الكثير من الصبر والحظ .

١-٧ التشفير متعدد الأحرف

عند استخدام الترميز المتناغم ، يصبح المدرج التكراري للنص المشفر أكثر انبساطا من خلال زيادة عدد الأحرف الهجائية ، وهو ما يضمن تمثيل أكثر من رمز في النص المشفر لنفس الحرف في النص الأصلي . ومع ذلك يظل صحيحًا أن كل رمز في نص التشفير يمثل حرفًا وحيدًا في النص الأصلي ، وهو ما يمثل

دائمًا خطرًا في أن يؤلف الطرف المعترض قاموسًا يحتوي على أزواج معروفة من النص المشفر والنص الأصلي لمفتاح معين .

هناك أسلوب آخر لتحقيق هدف جعل المدرج التكراري للنص المشفر منبسطا من خلال استخدام شفرة متعددة الأحرف . فعند استخدام التشفير متعدد الأحرف ، قد يختلف الرمز في نص التشفير الذي يحل محل حرف محدد في النص الأصلي عبر النص المشفر ، بل وقد يعتمد على سبيل المثال :- في تمثيله على موضعه في رسالة النص - الأصلي أو محتوى النص الأصلي الذي يسبقه , مثال على التشفير متعدد الاحرف هي شفرة فيجينر.

شفره Simple Shift Vigenere Cipher طريقة التشفير في هذا النوع من أبسط ما يكون ، حيث نقوم بتشفير الحرف الأول بالمفتاح الأول ، والحرف الثاني بالمفتاح الثاني ، وهكذا .. وفي حال انتهت المفاتيح أقوم بتكرار كتابتها مرة أخرى . مثال بسيط لتوضيح التشفير هذه الطريقه :

لدي هذه العبارة النص الأصلي : .DEFCON FOUR

أريد أن أشفرها بهذه الطريقه ، أول خطوه هي أن يكون المفتاح متغير ، أي مختلف من موقع الأخر , مثلا قد يكون المفتاح على الشكل :

الحرف الأول في النص يشفر بالمفتاح : ٥

الحرف الثاني يشفر بالمفتاح : ١٣

الحرف الثالث يشفر بالمفتاح : ٢

الحرف الرابع يشعر بالمفتاح : ٧

اذا المفاتيح (تسمى بـ Key Length) في هذه الحالة هي : ٥١٣٢٧

قبل أن نبدأ عمليه التشفير ، نضع هذا الجدول لتسهيل معرفه مواقع الحروف :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

النص المشفر الآن نضع النص المراد تشفيره ، ومقابله نضع المفتاح ، ومن ثم نبدأ بعمليه الازاحه ليخرج لدينا

نبدأ بالحرف الأول من النص الأصلي وهو D ، والمفتاح الأول هو ٥ ، الحرف المشغر الأول ٥ + D = ويساوي ١ أو (ممكن نأخذ قيمه ال D وهي ٣ وتجمع إليها ٥ مع أخذ % ٢٦ % ليخرج لدينا الناتج وهو ٩ ، الذي يمثل الحرف ١) .

نأخذ الحرف الثاني ، وهو ، والمفتاح الثاني وهو ١٣ ، وبعد عمليه الإزاحة ينتج لدينا الحرف المشفر R وهكذا لباقي الحروف في النص .....

هذه الصوره توضح عمليه التشفير ، السطر الأول هو النص الأصلي ، السطر الثاني المفاتيح ، وفي حال انتهت تعيد كتابتها مره أخرى ، السطر الأخير هو الناتج من جمع السطر الأول مع الثاني وهو النص المشفر .

Plaintext	D	E	F	C	O	N	F	O	U	R
Shift value	5	13	2	7	5	13	2	7	5	13
Ciphertext	I	R	H	J	T	A	H	V	Z	E

الآن نأخذ الناتج ونضعه في شكل Block كل منها يتكون من ٥ حروف اذا النص المشفر هو : IRHJT AHVZE

إلى هذا الأمر بسيط للغاية ، ولكن تبقى مشكله فعليه وهي صعوبة تذكر المفتاح وخاصة اذا كان طويل ، فكيف أحفظ هذه المفاتيح ؟ الحل هو استخدام نص أو جمله بدل هذه الأرقام ، وعند التشفير أعوض بكل حرف من هذه الجملة بالرقم على حسب موقعها ، مثلا الحرف A المفتاح هنا هو ٠ ، الحرف B المفتاح هو ١ وهكذا .....

اذا لو لدينا المفتاح (المفاتيح) : ١٤ ٥٥ ١٩ ١٨ ١٢ ٠ ١ , سوف يكون بالشكل التالي ، بعد تعوضه بالحروف BLAST OFF وهكذا ، سوف نقضي على مشكله حفظ المفاتيح الطويلة ، عن طريق جمله التشفير

٨-١ التشفير التبادلي

الأمثلة في جميع التي ذكرناها حتى الآن جرى الاستعاضة عن أحرف ، أو مجموعات من الأحرف في رسالة ، بأحرف أو مجموعات من أحرف أخرى من هنا تقع جميع أنظمة هذه الأمثلة تحت عنوان عام لشفرات الاستبدال . لكن توجد عائلات أخرى من التشفير التي تقوم على فكرة تبديل ترتيب كتابة الأحرف ، وهو ما يُعرف باسم « التشفير التبادلي » . نضرب مثلا بسيطا على ذلك هنا . في المثال الذي نضربه المفتاح هو رقم صغير . نستخدم رقم ٥ كمفتاح التشفير رسالة ما باستخدام هذا المفتاح نكتب الرسالة في صفوف يتألف كلٌّ منها من خمسة أحرف ، ثم نجري عملية التشفير من خلال كتابة أحرف العمود الأول أولا ، ثم العمود الثاني ، وهكذا . إذا لم يساوِ طول الرسالة أحد أضعاف رقم ٥ ، نُضيف عددًا مناسبًا من حرف Z في النهاية قبل إجراء عملية التشفير . يمكن فهم عملية التشفير بسهولة بالغة من خلال مثال صغير نشفّر الرسالة WHAT WAS THE WEATHER LIKE ON FRIDAY كيف كانت حالة الجو يوم الجمعة . بما أن المفتاح هو ٥ تتضمن الخطوة الأولى إذن كتابة الرسالة في صفوف يتألف كل صف منها من خمسة أحرف ، كالآتي :

بما أن طول الرسالة لا يساوي أحد أضعاف رقم ٥ ، يجب إضافة حرف ٧ واحد لنحصل على النتيجة التالية :-

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	Z

نقرأ الآن كل عمود على التوالي لنحصل على النص المشفر التالي :

WAWEEIHSERODATALNATHTIFYWEHKRZ

للحصول على مفتاح فك التشفير ، نَقسم طول الرسالة على المفتاح . في هذه الحالة ، نقسم ٣٠ على ٥ لنحصل على ٦. تصبح خوارزمية فك التشفير الآن مماثلة لخوارزمية التشفير لذا – على سبيل المثال - نكتب النص المشفّر في صفوف تتألف من ٦ أحرف لنحصل على النتيجة التالية :

W	A	W	E	E	I
H	S	E	R	O	D
A	T	A	L	N	A
T	H	T	I	F	Y
W	E	H	K	R	Z

يسهل الآن التحقق من أن قراءة كل عمود على التوالي سيفصح عن نص الرسالة الأصلية . يسهل كسر نوع الشفرات التبادلية المذكورة هنا . وبما أن المفتاح هو رقم يقسم طول النص المشفر ، سوف يضطر الطرف المعترض إلى حساب طول النص المشفر وتجريب كل رقم يقبل القسمة عليه على التوالي .

٩-١ التشفير المعقد

إلى الآن في هذا الفصل ، قدمنا عددًا من نماذج التشفير البسيطة يسهل كسر شفرة معظمها . نعرض الآن لمفهوم يمكن استخدامه للمزج بين نوع أو اثنين من أنظمة التشفير الضعيفة نسبيًا للحصول على نظام تشفير أقوى كثيرًا من أيهما ، وهو ما يعرف باسم « التشفير المعقد » . يعتمد التشفير المعقد على فكرة بسيطة للغاية . هب أننا نريد أن نجري عملية تشفير معقدة باستخدام نظام الاستبدال البسيط ونظام التشفير التبادلي ؛ سنشفّر أولا الرسالة باستخدام شفرة الاستبدال البسيط ، ثم نشفّر النص المشفر الناتج باستخدام التشفير التبادلي . سنطرح من خلال مثال بسيط طريقة إجراء هذه العملية .

نشفّر الرسالة ROYAL HOLLOWAY من خلال تشفيرها تشفيرًا معقدًا عن طريق تشفيرها أولاً باستخدام شفرة قيصر بمفتاح قيمته ٢ ثم استخدام التشفير التبادلي باستخدام مفتاح قيمته ٤. بالنسبة إلى شفرة قيصر باستخدام مفتاح قيمته ٢ ، نحصل على الآتي : بالنسبة إلى نظام التشفير التبادلي باستخدام

مفتاح قيمته ٤ نحصل على الآتي : يعتبر التشفير المعقد أسلوبًا في غاية الأهمية ؛ إذ يمكن النظر إلى كثير من خوارزميات التشفير القوية الحديثة كنتاج لنظام التشفير المعقد باستخدام عدد من الخوارزميات الضعيفة نسبيًا .

بالنسبة إلى نظام التشفير التبادلي باستخدام مفتاح قيمته ٤ نحصل على الآتي :

الرسالة: T Q A C N J Q N N Q Y C A

النص المشفَّر: **T N N A Q J Q Z A Q Y Z C N C Z**

يعتبر التشفير المعقد أسلوبًا في غاية الأهمية ؛ إذ يمكن النظر إلى كثير من خوارزميات التشفير القوية الحديثة كنتاج لنظام التشفير المعقد باستخدام عدد من الخوارزميات الضعيفة نسبيا .

الفصل الثاني

الخوارزميات الحديثة

الفصل الثاني

الخوارزميات الحديثة

٢-١ المقدمة

خلال الفصل الاول ، أكدنا على أن الأمثلة التي عرضناها لا تشير إلى الممارسات الحالية ، وأن نظام خوارزميات التشفير الحديثة تستخدم في الأغلب البتات (الأرقام الثنائية) بدلا من استبدال الأحرف في الأمثلة التي عرضناها في هذا الفصل ، نناقش الخوارزميات الحديثة . وبما أنها أكثر تعقيدًا من أمثلة الخوارزميات التي سقناها في الفصل الاول ، فإننا لا نذكر أي أمثلة محددة بالتفصيل ، لكننا نركّز على الأساليب العامة المستخدمة في تصميمها .

٢-٢ سلاسل الرقم الثنائي (البت) [٢ ,١]

مثلما أشرنا سابقًا ، لا تتضمن الشفرات الحديثة عملية استبدال للأحرف . بدلا من ذلك ، عادة ما يستخدم التشفير الحديث أنظمة ترميز لتحويل الرسائل إلى سلسلة متتالية من الأرقام الثنائية (بتات) ؛ أي من أصفار وآحاد ويعد نظام (ASCII) , نظام الترميز القياسي الأمريكي لتبادل المعلومات ، أكثر أنظمة التشفير الحديثة شيوعًا . بعد ذلك ، يجري تشفير سلسلة الأرقام الثنائية هذه التي تمثل النص الأصلي للحصول على النص المشفر في صورة سلسلة الأرقام الثنائية. يمكن تطبيق خوارزمية التشفير على سلسلة الأرقام الثنائية بطرق عدة. ثمة فارق « طبيعي » بين نظام شفرات التدفق ؛ حيث يتم تشفير السلسلة بتّا بتا (أي رقمًا ثنائيًّا رقما ثنائيًا) ، ونظام « شفرات الكتل » ؛ حيث يتم تقسيم السلسلة إلى كتل (مجموعات) لها طول محدد سلفًا. يتطلب نظام الترميز القياسي الأمريكي لتبادل المعلومات ثمانية بتات لتمثيل رمز واحد ؛ لذا يُجرى تطبيق خوارزمية التشفير على ثمانية رموز مرة واحدة في حالة شفرة الكتل التي تكون فيها الكتلة تتألف من ٦٤ رقما ثنائيا . من الأهمية بمكان أن ندرك أن سلسلة الأرقام الثنائية نفسها يمكن كتابتها بطرق مختلفة ، كما يتعين علينا أن ندرك أن طريقة كتابتها تعتمد على طول الكتل التي جرى تقسيمها إليها .

خذ - على سبيل المثال - السلسلة التالية المؤلفة من ١٢ رقما ثنائيا : ١١ ١٠٠١ ٠١١٠ ٠١. إذا قسمنا هذه السلسلة إلى كتل تتألف من ثلاثة أرقام ثنائية نحصل على : ١٠٠١١١٠١٠١١٠. في المقابل ، أيُّ سلسلة أرقام ثنائية بطول ٣ تمثل عددًا صحيحًا يقع بين قيمتي ٠ و ٧ ؛ ومن ثُمَّ تتخذ السلسلة التي لدينا الصورة الآتية : ٤ ٧٢٦.

باستخدام التمثيل الثنائي للاعداد الصحيحة اعلاه، تكون السلسلة على النحو التالي :

$$000 = 0,\ 001 = 1,\ 010 = 2,\ 011 = 3,\ 100 = 4,\ 101 = 5,\ \bar{110} = 6,\ 111 = 7.$$

إذا أخذنا السلسلة نفسها ثم قسمناها إلى كتل بطول أربعة نحصل على : ١٠٠١١١٠١ ٠١١٠. في هذه المرة ، بما أن سلسلة الأرقام الثنائية التي لها طول أربعة أرقام ثنائية تمثل الأعداد الصحيحة الواقعة بين قيمتي ٠ و ١٥ ، نحصل على السلسلة ٩١٣٦. بوجه عام ، يمكن النظر إلى سلسلة الأرقام التي طولها N على أنها تمثل عددًا صحيحًا يقع بين قيمتي ٠ و١ – ٢^N ؛ ومن ثَمَّ بمجرد الاتفاق على طول كتلة بقيمة S ، يمكن كتابة أي سلسلة أرقام ثنائية طويلة كسلسلة تتألف من أعداد صحيحة تقع في نطاق القيمتين ٠ و١ – ٢^N بينما لا تعتبر التفاصيل الرياضية الدقيقة مهمة من الأهمية بمكان ملاحظة أن سلسلة الأرقام الثنائية نفسها يمكن تمثيلها في صورة سلسلة من الأعداد بعدة طرق ، اعتمادًا على طول الكتلة التي جرى انتقاؤها من الأهمية بمكان أيضًا إدراك أنه في حال تحديد طول الكتلة ، وكانت الأعداد صغيرة ، ربما يكون ضرورياً إضافة بعض الأصفار الإضافية في البداية . على سبيل المثال ، يعتبر التمثيل الثنائي للعدد الصحيح ٥ هو ١٠١ في المقابل ، في حال استخدام كتلة طولها ٦ أعداد تمثل ٥ كالآتي : ٠٠٠١٠١ ، وبالنسبة إلى كتلة طولها ٨ فإننا نمثل ٥ كالآتي : ٠٠٠٠٠١٠١

هناك طريقة أخرى شائعة لكتابة سلسلة الأرقام الثنائية ؛ وتتمثل في استخدام « التمثيل السادس العشر » . بالنسبة إلى التمثيل السادس عشر ، تُقسم السلسلة إلى مجموعات من أربعة أعداد تمثل كالآتي :

0000 = 0	0001 = 1	0010 = 2	0011 = 3
0100 = 4	0101 = 5	0110 = 6	0111 = 7
1000 = 8	1001 = 9	1010 = A	1011 = B
1100 = C	1101 = D	1110 = E	1111 = F

من هنا ، يصير التمثيل السادس عشر للسلسلة السابقة : ٩٦ . بما أن خوارزميات التشفير يجري تطبيقها على سلسلة من الأرقام الثنائية فسنحتاج إلى التعرف على أسلوب شائع الاستخدام لدمج رقمين ثنائيين يطلق عليه أسلوب OR الحصري وعادةً ما يجري كتابته كالآتي : « XOR » أو . إنه يطابق الجمع بالنسبة إلى المقياس الحسابي ٢ ويعرف كالآتي : ٠ = ٠٠٠ ، ١ = ١ ٠ ٠ ، ١ = ١ ٠ ٠ ، و ٠ = ١٠١ ، وهو ما يمكن تمثيله في جدول .

	0	1
0	0	1
1	1	0

الشكل (٢-١) يوضح عملية OR

توفر هذه العملية البسيطة طريقة للدمج بين سلسلتين من الأرقام الثنائية لهما نفس الطول نجري هذه العملية على أزواج من الأرقام الثنائية في مواضع متناظرة . على سبيل المثال ، هب أننا نريد حساب ١١٠٠١١٠٠١١. الرقم الثنائي هو ١ والرقم الثنائي إلى يسار ١١٠٠١ هو ١ أيضًا ؛ من هنا ، بما أن الرقم الثنائي إلى يسار ١٠٠١١ XOR ١١٠٠١ يجري الحصول عليه من خلال تطبيق أسلوب XOR على الأرقام الثنائية في يسار كل سلسلة منفردة .

1	0	0	1	1
1	1	0	0	1
1 ⊕ 1	0 ⊕ 1	0 ⊕ 0	1 ⊕ 0	1 ⊕ 1
0	1	0	1	0

٢-٣ شفرات التدفق

يستخدم الكثير من المؤلفين هذا المصطلح بطريقة مختلفة نوعا ما . يتحدث الكثيرون عن شفرات تدفق تعتمد على الكلمات أو الرموز . في هذه الحالة يجري تشفير الرسالة كلمة كلمة (أو رمزا رمزًا) ،

ويجري تحديد قاعدة التشفير لكل كلمة (رمز) من خلال موضعها في الرسالة . تتوافق شفرة فيجنر ، التي جرى مناقشتها في الفصل الاول ، ودفتر المرة الواحدة هذا التعريف .

ربما كان أكثر النماذج التاريخية شهرةً هو شفرة إنيجما . مع في المقابل ، يتمثَّل أكثر الاستخدامات الحديثة شيوعًا لمصطلح « شفرة تدفق » - وهو الاستخدام الذي نتبناه هنا - في أنها شفرة يجري تشفير النص الأصلي فيها رقما رقمًا . بداهة ، كل ما يمكن أن يحدث لأي رقم ثنائي هو تغير قيمته إلى القيمة البديلة أو عدم تغيرها .

وبما أن أي رقم ثنائي يمكن أن يكون له قيمة واحدة من قيمتين اثنتين فقط ، فإن تغيير أي رقم ثنائي يعني تبديله بقيمة أخرى . بالإضافة إلى ذلك ، إذا جرى تغيير رقم ثنائي مرتين فإنه يعود إلى قيمته الأصلية . إذا كان الطرف المعترض يعلم أن شفرة تدفق جرى استخدامها ، فسينحصر جهده إذن في تحديد مواضع الأرقام الثنائية التي جرى تغييرها ، ثم تغييرها إلى قيمها الأصلية . إذا كان ثمة نمط سهل التتبع يمكن من خلاله تحديد الأرقام التي جرى تغييرها ، فربما ستصبح مهمة الطرف المعترض سهلة . من هنا ، بينما يجب ألا تكون مواضع الأرقام الثنائية التي جرى تغييرها قابلة للتنبؤ من قبل الطرف المعترض ، بل يجب أن يتمكن الطرف المستقبل دومًا من تحديدها بسهولة . بالنسبة إلى شفرات التدفق ، يجري النظر إلى عملية التشفير باعتبارها سلسلة تتألف من العمليتين الآتيتين : التغيير وعدم التغيير .

يحدد مفتاح التشفير هذه السلسلة التي عادة ما يطلق عليها سلسلة مفتاح التدفق. للتبسيط والاختصار ، لنتفق على أن قيمة ٠ تشير إلى « عدم التغيير» وقيمة ١ تشير إلى « التغيير » . بلغنا الآن مرحلة صار فيها النص الأصلي ، والنص المشفر ، ومفتاح التدفق كلها سلاسل تتألف من أرقام ثنائية . للمزيد من التوضيح هب أن لدينا النص الأصلي ١١٠٠١٠١ ومفتاح التدفق ١٠٠٠١١٠ ؛ إذن بما أن قيمة ١ في مفتاح التدفق تشير إلى تغيير الرقم الثنائي في النص الأصلي في ذلك الموضع فسنجد أن قيمة ١ التي تقع في أقصى يسار النص الأصلي يجب تغييرها ، لكننا سنلاحظ أن الرقم الثنائي التالي يظل كما هو . بتكرار هذه العملية نحصل على النص المشفر ٠١٠٠٠١١ أشرنا توا إلى أن تغيير رقم ثنائي مرتين يترتب عليه إعادة الرقم إلى قيمته الأصلية ؛ وهو ما يعني أن عملية فك التشفير تماثل عملية التشفير ؛ ومن يحدد مفتاح التدفق أيضًا طريقة فك التشفير . يتمثل كل ما قمنا به في العرض السابق في دمج سلسلتين من الأرقام الثنائية لتوليد سلسلة ثالثة من خلال قاعدة يمكن النص عليها كالآتي في حالتنا الخاصة هذه : « إذا كان هناك رقم ١ في أحد مواضع السلسلة الثانية غير إذن الرقم في الموضع نفسه من السلسلة الأولى » تعتبر هذه العملية هي بالضبط عملية XOR ,تمثل الرقم الثنائي للنص الأصلي ، ومفتاح التدفق والنص المشفر

على التوالي في الموضع i ، يجري الحصول على الرقم الثنائي للنص المشفر Ci من خلال لاحظ أن عملية التشفير Ci . تتمثل المشكلة في دفتر المرة الواحدة في أنه بما أن مفتاح التدفق يكون عشوائيا ، فمن المستحيل توليد نفس مفتاح التدفق آنيًّا على طرفي الإرسال والاستقبال ، وهو ما يجعلها تتطلب قناة ثانية آمنة لتوزيع المفاتيح ، وهذه القناة تحمل من المحتوى ما يساوي محتوى قناة الاتصالات الرئيسية . وتجري نفس الاشتراطات في حالة شفرات التدفق مثلما هو الحال مع أي قناة آمنة للمفتاح ، ولكن في ظل وجود محتوى معلومات أقل بكثير . تحتاج شفرة التدفق إلى مفتاح قصير لتوليد مفتاح تدفق طويل ، وهو ما يتحقق من خلال استخدام مولد سلسلة أرقام ثنائية . تذكَّر أننا خلال مناقشتنا لشفرة فيجنر في الفصل الاول ، طرحنا مفهوم استخدام مولّد لتوليد مفتاح تدفق طويل ذي أحرف هجائية من خلال مفتاح قصير ذي أحرف هجائية . لكن في تلك الحالة ، كانت عملية التوليد بدائية للغاية ؛ إذ جرى انتقاء كلمة المفتاح وتكرارها يجب أن تكون مولدات مفتاح التدفق في شفرات التدفق العملية أكثر تعقيدًا من ذلك . للتدليل على سبب ذلك ، نلاحظ مما سبق أن الرقم الثنائي لمفتاح التدفق يمكن تحديده على أنه نتاج عملية XOR للنص الأصلي والنص المشفر في الموضع i . يسلط ذلك الضوء على ضعف شفرات التدفق ؛ حيث إن أي طرف معترض يتمكن من إجراء عملية اعتراض استنادًا إلى معرفته بالنص الأصلي سيستطيع استنباط أجزاء من سلسلة مفتاح التدفق من خلال زوجي الأرقام الثنائية للنص الأصلي والنص المشفر المقابلين . من هنا ، يجب على مستخدمي شفرات التدفق حماية شفراتهم ضد عمليات الاعتراض التي يستطيع الطرف المعترض عبرها استنباط جزء من مفتاح التدفق . بعبارة أخرى ، يجب أن تكون سلسلة مفتاح التدفق غير متوقعة ؛ بمعنى أن القدرة على معرفة جزء منها يجب ألا يمكن الطرف المعترض من استنباط الباقي .

٢ـ ٤ نظام شفرات الكتل (نمط كتاب الشفرات الإلكتروني)

في حالة « شفرة الكتل » ، يتم تقسيم سلسلة الأرقام الثنائية إلى كتل أو مجموعات بطول محدد . تطبق خوارزمية التشفير على هذه الكتل لتوليد كتل نص مشفّر لها نفس الطول وذلك في حال معظم الشفرات المتناظرة .

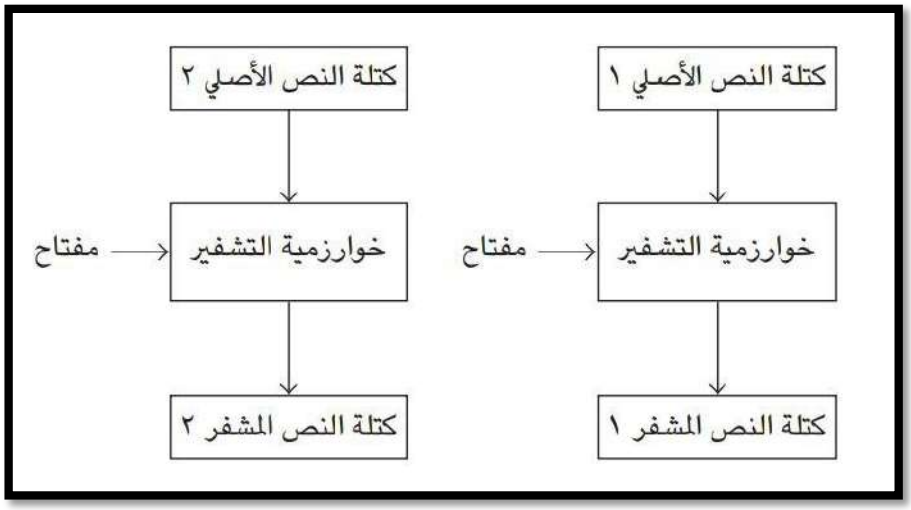
هناك العديد من التطبيقات لشفرات الكتل . ويمكن الاستعانة بها لتوفير السرية أو سلامة البيانات أو التحقق من هوية المستخدمين، بل يمكن استخدامها في توفير مولد مفتاح التدفق في شفرات التدفق ومثلما هو

الحال مع شفرات التدفق من الصعوبة بمكان إجراء عملية تقييم محددة لدرجة الأمن التي يحققها هذا النظام . بداهة ، مثلما رأينا ، يمثل طول المفتاح حدًّا علويًّا لقوة خوارزمية التشفير .

ثمة عدد من الخواص البديهية يجب أن تتوفر في شفرة الكتل القوية وهي خواص يسهل بيانها . إذا حصل طرف معترض على زوج من نص أصلي معروف ونص مشفر لمفتاح غير معروف ، فلن يمكنه ذلك بالضرورة من استنباط النص المشفر المقابل لأي نص أصلي آخر أحد هذه الخواص هي خاصية الانتشار في نظام شفرات الكتل ، وهي الخاصية التي تتمثل في أن إجراء أي تغيير بسيط في النص الأصلي ، ربما - على سبيل المثال – من خلال تغيير موضع أو موضعين ، سيؤدي إلى حدوث تغيير غير متوقع في النص المشفر . وذلك لتفادي مخاطر عمليات البحث الشاملة للمفتاح خلال إجراء مثل هذا النوع من عمليات البحث ، قد يجرب الطرف المعترض مفتاحًا لا يختلف عن القيمة الصحيحة للمفتاح الحقيقي إلا في عدد محدود من المواضع .

الخاصية الاخرى التي يجب توفرها في شفرات الكتل خاصية التشويش التي تتمثل في أنه في حال محاولة طرف معترض إجراء عملية بحث شاملة عن المفتاح ، يجب ألا تتوفر أي إشارة إلى الاقتراب من المفتاح الصحيح .

تتمثل أسهل الطرق ، وربما أكثرها منطقية ، لتشفير رسالة طويلة بشفرة الكتل في تقسيم سلسلة الأرقام الثنائية إلى كتل مناسبة الطول ، ثم تشفير كل كتلة على حدة وعلى نحو مستقل عندما يجري تنفيذ ذلك ، نطلق على هذه العملية استخدام نمط « كتاب الشفرات الإلكتروني » . عند انتقاء مفتاح واستخدام نمط كتاب الشفرات الإلكتروني ، ينتج عن الكتل المتناظرة في الرسالة كتل متناظرة في النص المشفر ؛ وهو ما يعني أنه في حال حصول طرف معترض على الزوج المقابل من كتلة النص الأصلي ونص التشفير سيستطيع تحديد موضع الكتلة في النص الأصلي في كل مكان في الرسالة من خلال إيجاد الأرقام الثنائية المقابلة في النص المشفر . لذلك يكون من المفيد انتقاء كتل كبيرة الطول نسبيًّا ، مثل الكتل التي تشمل ٦٤ رقما ثنائيًّا ، تحتوي كل مجموعة منها على ثمانية رموز ومع ذلك يوجد عيب محتمل في استخدام نمط كتاب الشفرات الإلكتروني ، وهو ما سنبينه من خلال مثال .



الشكل (٢-٢) يوضح شفرات الكتل وفق نمط كتاب الشفرات الالكتروني

هَبْ أن شفرة كتل غير معروفة ومفتاحا غير معروف جرى استخدامهما لتشفير الرسالة التالية : The price is four thousand pounds السعر أربعة آلاف جنيه) ؛ لا توجد معلومات متوفرة سوى أن كتلة من كتل الرسالة تتألف من حرفين ، وأنه حدث تجاهل لعلامات الترقيم ، والمسافات ، إلخ ، وأن النص المشفر على النحو التالي :

. C1 , C2 , C3 , C4 , C5 , C6 , C7 , C8 , C9 , C10 , C11 , C12 , C13 , C14

هَبْ أن الطرف المعترض يعرف محتوى الرسالة سيستطيع إذن استنباط أن C1 تمثل TH ، وأن C2 تمثل ep ، إلى آخره . ثم يتلاعب الطرف المعترض بالنص المشفر بحيث لا يجري تلقي سوى الكتل التالية :

C1 , C2 , C3 , C4 , C5 , C6 , C7 , C12 , C13 , C14

ويستخدم الطرف المستقبل خوارزمية فك التشفير من خلال المفتاح الصحيح في فك شفرة النص المشفر الذي يتلقاه ليحصل على الآتي : The price is four pounds (السعر أربعة جنيهات) . بما أن عملية فك التشفير نجحت وصار للرسالة معنى ، فلن يشك الطرف المتلقي في أن النص المشفر جرى التلاعب به ؛ ومن ثُمَّ سيفترض صحة السعر .

يمكن التخلص من هذه المخاطر المحتملة في استخدام شفرة الكتل وفق نمط كتاب الشفرات الإلكتروني من خلال جعل عملية التشفير لكل كتلة مفردة على حدة تعتمد على جميع الكتل التي تسبقها في الرسالة في

حال تنفيذ ذلك ، فإن الكتل المتشابهة في الرسالة ستعطي على نحو شبه مؤكد كتلا متشابهة في النص المشفر ، وسيؤدي التلاعب في النص المشفّر إلى رسائل لا معنى لها بعد إجراء عملية فك التشفير . ثمة طريقتان قياسيتان لتحقيق ذلك ؛ ألا وهما نمط استجابة الشفرات ونمط تسلسل شفرات الكتل .

٢-٥ دوال الاختزال

يوجد حالات عديدة يجري فيها استخدام التشفير لكن دون الحاجة إلى توفر القدرة على استنباط محتوى « الرسالة » الأصلية من صيغتها المشفرة .

بالنسبة إلى نظام المفاتيح المعلنة ، يعتبر كلٌّ من الخوارزمية ومفتاح التشفير معروفين (معلنين). وهكذا، يواجه الطرف المعترض مهمة محاولة استنتاج الرسالة من النص المشفر الذي جرى الحصول عليه من خلال أسلوب يعرفه معرفة تامة . بديهيا ، يجب انتقاء عملية التشفير بعناية بالغة لضمان صعوبة مهمة الطرف المعترض في المقابل ، يجب عدم نسيان أن المتلقي الأصلي للرسالة يجب أن يمتلك القدرة على فك شفرة الرسالة بسهولة ؛ لذا يجب انتقاء عملية التشفير بحيث تيسر معرفة مفتاح فك التشفير عملية تحديد الرسالة من النص المشفر . هذا مفهوم يصعب استيعابه . ثمة سؤال يُطرح كثيرًا وهو : « إذا كان الجميع يعرفون ما قمت به لتحديد النص المشفر ، فلماذا إذن لا يفكون شفرة الرسالة ؟ » يساعد المثال غير الرياضي التالي عادةً في تقديم الإجابة . هب أنك في غرفة مغلقة لا يوجد بها هاتف وقُدمت إليك نسخة ورقية من دليل الهاتف في لندن ؛ إذا أعطاك أحد اسمًا وعنوانًا وسألك عن رقم هاتف صاحبهما ، فستكون هذه مهمة سهلة في المقابل ، هب أن أحدهم أعطاك رقم هاتف عشوائيا وسألك عن اسم وعنوان صاحبه ؛ تأكيدًا ، هذه مهمة شاقة للغاية . لا يرجع السبب إلى عدم معرفتك بما يجب القيام به . [١]

فمن الناحية النظرية ، قد تبدأ من الصفحة الأولى ثم تقرأ جميع الأرقام حتى تجد الرقم الصحيح تكمن الصعوبة هنا في حجم المجهود المبذول ؛ لذا ، إذا نظرنا إلى الاسم والعنوان باعتبارهما الرسالة ، وإلى رقم الهاتف » باعتباره النص المشفر ، وإلى إيجاد رقم كذا باعتباره عملية التشفير فسنكون قد حققنا الهدف في حالة دليل الهاتف في لندن .

من الأهمية بمكان الإشارة إلى أنه في حال تطبيق العملية نفسها على أدلة هاتف أصغر حجمًا ، سيتمكن الطرف المعترض من إجراء عملية عكسية بالإضافة إلى ذلك ، لا يمكن التحديد على وجه الدقة عدد

الأشخاص المطلوب قبل أن نشعر بأن لدينا أسبابًا قوية للادعاء بتحقيق الهدف يتضمن دليل الهاتف في لندن أكثر من ٧٥٠ ألف اسم ، ونستطيع أن نقول ونحن مطمئِنّين إن ٧٥٠ ألفًا يعتبر رقمًا ضخما في هذا السياق . بالنسبة إلى إحدى منشآت العمل التي لا تزيد فيها الأرقام الداخلية عن ١٠٠ رقم ، يعتبر إجراء عملية عكسية لاستنباط عدد صحيح من بين قائمة الأرقام عملية سهلة على الأرجح . لكن ماذا عن دليل يشتمل على ٥٠٠٠ رقم ؟ يوجد ، بطبيعة الحال ، مؤسسات معينة مثل خدمات الطوارئ التي تستطيع تحديد هوية مالكي أي أرقام هاتفية ؛ إذ تمتلك هذه المؤسسات دليلًا مرتبا ترتيبا رقميًّا .

ابتكر أكثر هذه الأنظمة شهرةً رون ريفست ، وآدي شامير ، ولين أدلمان في عام ١٩٧٨ وهو النظام المعرف اختصارًا باسم RSA . في هذا المسألة الرياضية المصاحبة للنظام هي عملية تحليل الأعداد إلى عواملها الأولية ؛ حيث يوجد مفتاح معلن معروف ، وهو ناتج ضرب عددين أوليين قيمتاهما سريتان هذان العددان في غاية الأهمية ؛ حيث إن أي شخص يعرف قيمتيهما يستطيع حساب المفتاح السري من خلال المفتاح المعلن . لذا ، يجب أن يكون العدد N الذي يحدد طول كتلة الرسالة ، كبيرًا بما يكفي بحيث لا يستطيع أي طرف معترض استنباط العددين الأوليين ؛ بمعنى أنه لا يستطيع تحليل العدد N إلى عوامله الأولية . بداهة ، إذا كان العدد N صغيرًا ، فسيستطيع أي شخص تحديد العددين الأوليين . كمثال بسيط على ذلك ، افترض أن N = ١٥ ؛ ومن ثَمَّ فالعددان الأوليَّان هما ٣ و ٥ .

لكن يُعتقد أن اكتشاف العددين الأوليين مسألة غير ممكنة في حال كان العدد N كبيرًا بما يكفي .

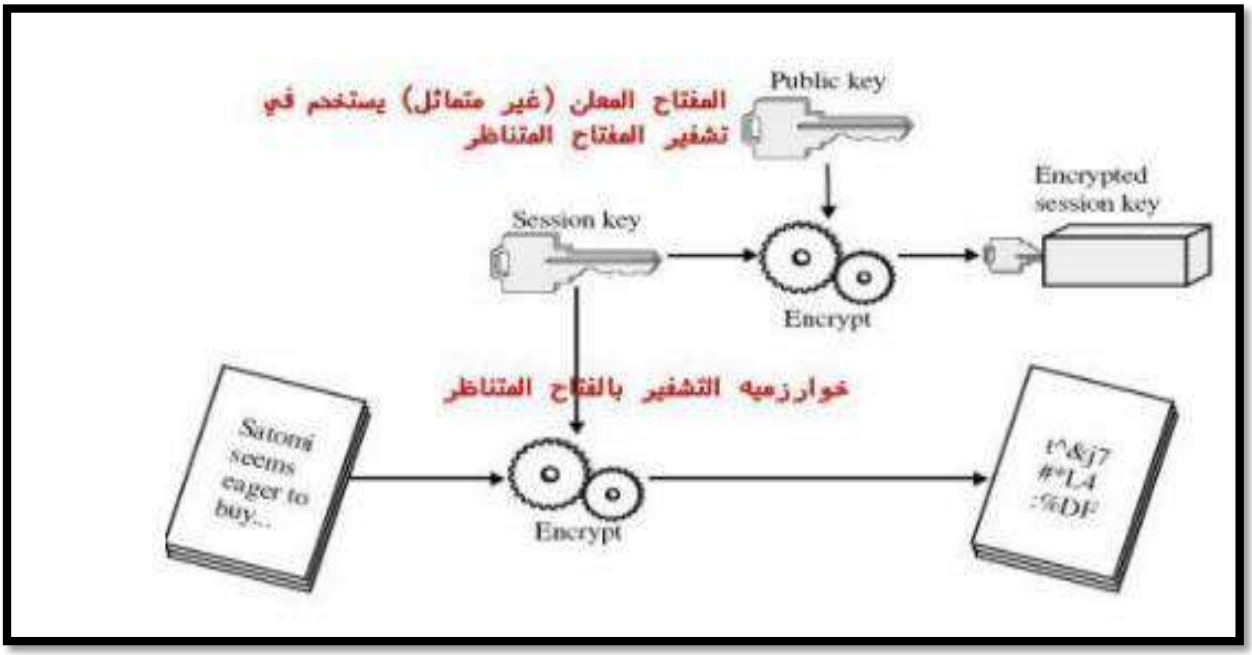
ففي حالة الشفرات المتناظرة تعتبر الأطوال النموذجية للكتل هي ٦٤ أو ١٢٨ رقمًا ثنائيًا ، فيما تبلغ في حالة نظام RSA٦٤٠ رقما ثنائيا على الأقل .

في السبعينيات تم اختراع تلك الطريقه ، وهي تستخدم مفتاحين ، مفتاح عام public Key للتشفير ، ومفتاح خاص private Key لفك التشفير ، مثلا اذا أراد محمد إرسال رسالة مشفره لعلي باستخدام التشفير بالمفتاح الغير متناظر (أو المعان أو العام) ، يقوم محمد بأخذ المفتاح العام من علي ، وبعدها يقوم بتشفير الرسالة بهذا المفتاح ، بعدها يقوم بإرسال الرسالة إلى علي الذي يقوم بفك التشفير بالمفتاح الخاص به ...

- المفتاح العام public Key : يكون معروف للجميع وأي شخص يستطيع الحصول عليه (هو يستخدم فقط للتشفير) .
- المفتاح الخاص private Key : يكون غير معروف معروف لشخص واحد , وهو يستخدم للتفشير.

ولكي نكون أكثر صوابا ، فإن المفتاح العام يستخدم لتشفير مفتاح الجلسة.

محمد يريد إرسال رسالة لعلي ، ويريد طريقه أمنه لإرسال المفتاح ، لذلك تم اختيار طريقه التشفير بالمفتاح الغير متناظر ، بعدها يقوم محمد بتشفير الرسالة بخوارزمية التشفير بالمفتاح المتناظر ، سأذكر السبب بعد قليل ، وبعدها يقوم بأخذ المفتاح العام لعلي (الذي هر معروف للجميع) ويقوم بتشغير المفتاح (الجلسة) بعدها يرسل هذا المفتاح المشفر والرسالة إلى علي ، الذي يقوم بدوره بفك تشفير المفتاح بالمفتاح الخاص ، بعدها يقوم بفك تشفير الرسالة [٢]



الشكل (٢-٣) يوضح مفتاح عام public Key للتشفير ، ومفتاح خاص private Key لفك التشفير .

طريقه عمل الخوارزمية RSA [٣]:

- يحتاج كل شخص إلى الحصول على زوج من المفاتيح المختلفة مفتاح خاص (Private Key) مفتاح عام (Public Key) ، حيث ترتبط هذه المفاتيح ببعضها رياضيا ، فعند استخدام أحد المفاتيح للتشغير يمكن للآخر فك تشفير النص المشفر مرة أخرى إلى النص الأصلي .
- **كيفيه توليد المفتاح العام public key و المفتاح الخاص (private key) :**

١. اختر عددين أوليين بشكل عشوائي كبيرين مختلفين Q و P .

٢. حساب n= p*qn يُستخدم كالمعامل لكلا المفاتيح الخاصة والعامة .

٣. حساب $\text{Compute } \varphi(n) = (p-1)\,(q-1)$

١. اختر عدد صحيح e بشرط ان يكون ((e, φ(n)) ليس لهم اي عامل مشترك غير ال ١

Select the public exponent $e \in \{١,٢, \ldots, \varphi(n) - ١\}$ s.t. $\gcd(e, \varphi(n)) = ١$,

Compute the private key d, s.t.

٢. نحسب D من خلال المعادله:

$d.e \equiv ١ \bmod \square(n)$.

The public key is $K_{pub} = (n, e)$, and

RSA Encryption

Given the public key $(n, e) = k_{pub}$ and the plaintext x, the encryption function is:

$$y = e_{k_{pub}}(x) \equiv x^e \bmod n \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where $x, y \in Z_n$.

RSA Decryption

Given the private key $d = k_{pr}$ and the ciphertext y, the decryption function is:

$$x = d_{k_{pr}}(y) \equiv y^d \bmod n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

where $x, y \in Z_n$.

مثال ٢-١:

Alice $x = ٤$

Bob

$p = ٣, q = ١١$

$n = ٣٣$

$\varphi(n) = ٢٠١٠ = ٢٠$

Choose $e = ٣$

$\gcd(٢٠,٣) = ١$

Compute $d \equiv e^{-١} \equiv ٧ \bmod ٢٠$

$,k_{\text{pub}} = (٣٣,٣)$

$$y = ٤^{٣} \bmod 33$$
$$= ٦٤ \bmod ٣٣ = ٣١$$

٦-٢ الاستنتاجات

وفي ختام البحث يمكن ان نستنتج ما يلي:

١. يعني التشفير في الأمن الإلكتروني تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر. لا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فك تشفيرها. ويعد التشفير وحدة البناء الأساسية لأمن البيانات. وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض ضارة.

٢. إن التشفير وسيلة لحماية المعلومات الخاصة من السرقة أو الاختراق في مجال الأمن الإلكتروني. وهناك جانب آخر مهم للأمان عبر الإنترنت، وهو استخدام حل مكافحة فيروسات عالي الجودة، مثلKaspersky Premium ، الذي يحظر التهديدات الشائعة والمعقدة مثل الفيروسات والبرمجيات الضارة وبرامج طلب الفدية وتطبيقات التجسس وأحدث حيل التسلل والقرصنة.

٣. يتضمن التشفير استخدام مفتاح تشفير، وهو مجموعة من القيم الرياضية يتفق عليها كل من المرسل والمتلقي. يستخدم المستلم المفتاح لفك تشفير البيانات وإعادتها إلى هيئة نص عادي يمكن قراءته

٤. .وكلما كان مفتاح التشفير أكثر تعقيدًا، كان التشفير أكثر أمانًا، حيث تقل احتمالية قدرة الجهات الخارجية على فك تشفيره من خلال (هجمات القوة الغاشمة) أي محاولة الأرقام العشوائية إلى أن يتم تخمين المجموعة الصحيحة.

٥. **مفاتيح التشفير المتماثلة :**يُعرف هذا أيضًا باسم تشفير المفتاح الخاص. يكون المفتاح المستخدم للتشفير هو نفسه المستخدم لفك التشفير، مما يجعل هذا الأسلوب الأفضل للمستخدمين الفرديين والأنظمة المغلقة. وبخلاف ذلك، يجب إرسال المفتاح إلى المتلقي. على أن هذا يزيد من خطر التعرض للاختراق إذا اعترضته جهة خارجية، مثل المتسللين. لكن هذه الطريقة أسرع من الطريقة غير المتماثلة.

٦. **التشفير غير المتماثل :**يستخدم هذا الأسلوب مفتاحين مختلفين، أحدهما عام والآخر خاص، مرتبطَين معًا حسابيًا. والمفتاحان هما في الأساس أرقام كبيرة، وتم ربطهما معًا لكنهما ليسا متماثلين، ومن هنا جاءت التسمية "غير متماثل". يحتفظ المالك بالمفتاح الخاص سرًا، ويتم إما مشاركة المفتاح العام بين المستلمين المصرح لهم أو إتاحته للجمهور بشكل عام. ولا يمكن فك تشفير البيانات المشفرة باستخدام المفتاح العام للمستلم إلا باستخدام المفتاح الخاص المقابل.

المصادر Sources

١. فريد بايبر وشون ميرفي، علم التشفير مقدمة قصيرة جدا، ترجمة محمد سعد طنطاوي، مؤسسة هنداوي للتعليم والثقافة، الطبعة الاولى، ٢٠١٦.

٢. وجدي عصام عبد الرحيم، مقدمة في التشفير بالطرق الكلاسيكية، متوفر في الموقع:

https://uotechnology.edu.iq/ce/lecture14/forth%20class/Computer%20Security/Classical_Cryptography.pdf

٣. https://ar.quora.com/%D9%85%D8%A7-%D9%87%D9%8A-%D8%AE%D9%88%D8%A7%D8%B1%D8%B2%D9%85%D9%8A%D8%A9-RSA