5 طرق تستطيع بها كتابة رسالة مشفرة

كتبه أسماء العمر | 15 نوفمبر ,2017

كتابة رسالة مشفرة

هناك أكثر من طريقة يستطيع بها المرء اختلاق كلمات سر مختلفة، لدرجة أن كل فرد منا يخلق كلمته الخاصة به التي تُعبر كثيرًا عن شخصيته، سواء كانت كلمة سر هزلية تعبر عن جانب السخرية الذي يتحلى به، أم كانت كلمة سر بلغات مختلفة كتبها باللغات التي يُتقنها، إلا أن هناك حياة كاملة خلف كلمات السر أو خلف مفهوم التشفير بالأساس، جمّعنا إليك أشهر 5 طرق استخدمها البشر للتواصل بالشفرات.

لقد كانت حاجة البشر لإخفاء معاني الرسائل المهمة موجودة منذ آلاف السنين، ولذلك وجدوا كثيرًا من الطرق المعقدة لتشفير رسائلهم وإخفاء معانيها، لتختلف طريقة حل أو فك الشفرة على حسب درجة تعقيد الشفرة نفسها.

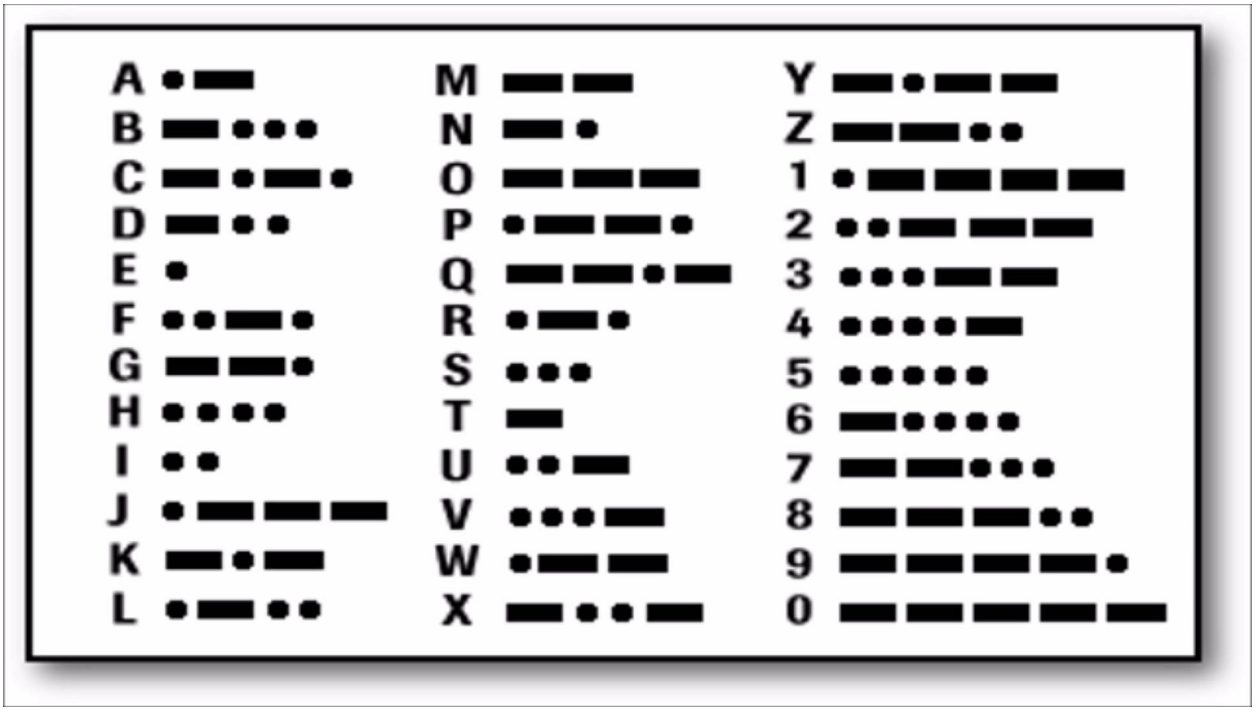
هناك فرق بين الرمز (Code) والكتابة بالرمز (Cipher)، ففي حالة الرمز، تكون كل كلمة مكتوبة فيه ترمز إلى رمز آخر (Code) أو إلى مثال آخر، بينما في الكتابة بالرمز "Cipher" يكون كل حرف في الشفرة يرمز إلى حرف آخر أو إلى رمز آخر مختلف، إلا أن تشفير الرمز وتشفير الكتابة بالرمز تكون مختلفة.

استخدم البشر طرق فك الشفرات والرموز لفهم الأساطير اليونانية والهيروغليفية (اللغة المصرية القديمة)، كان أشهرها "حجر رشيد" على سبيل المثال، وهو الحجر الذي يُعطي مفتاح الفهم الحديث للغة الهيروغليفية بعد اكتشافه في مدينة رشيد "Memphis" في الدلتا المصرية وترجمته لأول مرة من العالم الفرنسي "شامبليون"، استخدمت الشفرات أيضًا في صُنع طريقة كتابة يستطيع من خلالها المكفوفين القراءة.

عشرة من الأكواد وطرق الكتابة بالرموز

5 طرق لكتابة رسالة مشفرة

1- شفرة مورس (Morse Code)



صنعها صامويل مورس عام 1840، وهي إحدى الشفرات الحرفية التي استُخدمت لإرسال الرسائل التلغرافية، تستخدم تتابعات قياسية "شرطة طويلة أو قصيرة" من الممكن تكوينها من خلال نقاط أو علامات مائلة، كانت تُستخدم في أغلب الاتصالات عالية السرعة، حيث يمكن تكوينها من خلال الأصوات كذلك، وهي من إحدى الشفرات التي لا تقرأها الأجهزة ويجب على الإنسان فك شفرتها بنفسه.

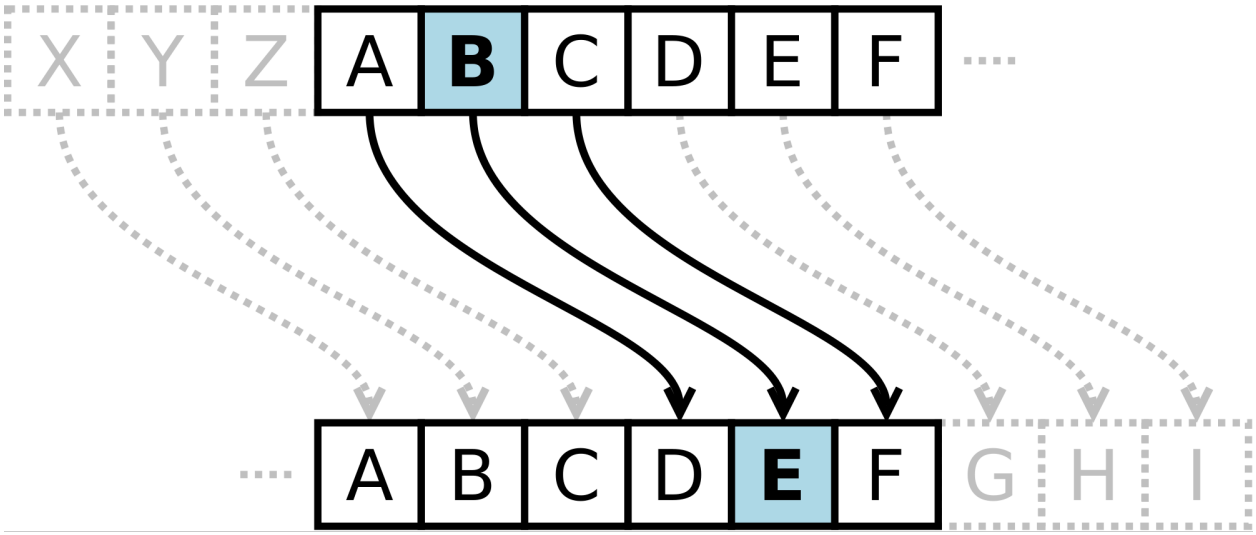
يتضمن ترميز لغة مورس العالي الحروف العربية أيضًا، والجدول السابق يبين قائمة بالرموز الموافقة لكل حرف عربي، مكتوبة من اليمين لليسار.

استخدمت شفرة مورس قديمًا في الاتصالات اللاسلكية وفي إرسال البرقيات والملاحة البحرية، حيث

كانت تعتمد هذه الشفرة على مبدأ بسيط وهو تحويل الإشارات الكهربائية المنقولة عبر خطوط البرق إلى مقاطع صوتية طويلة وقصيرة بحيث تحول المقاطع الطويلة إلى شرط والقصيرة إلى نقاط والتي بدورها يتم ترجمتها لاحقًا إلى حروف وكلمات مفهومة.

صار استخدام شفرة مورس محدودًا حاليًّا من بعض الهواة، إلا أنك يمكنك أيضًا تكوين جملة كاملة باستخدام النقاط والشرطة الطويلة أو القصيرة المقابلة للحروف اللاتينية والعربية، ويمكنك بذلك إخفاء محتوى رسالة مهمة لا يمكن لأي شخص قراءتها إلا إذا كان مُلمًا بشفرة مورس.

2- شفرة قيصر (Ceaser Cipher)



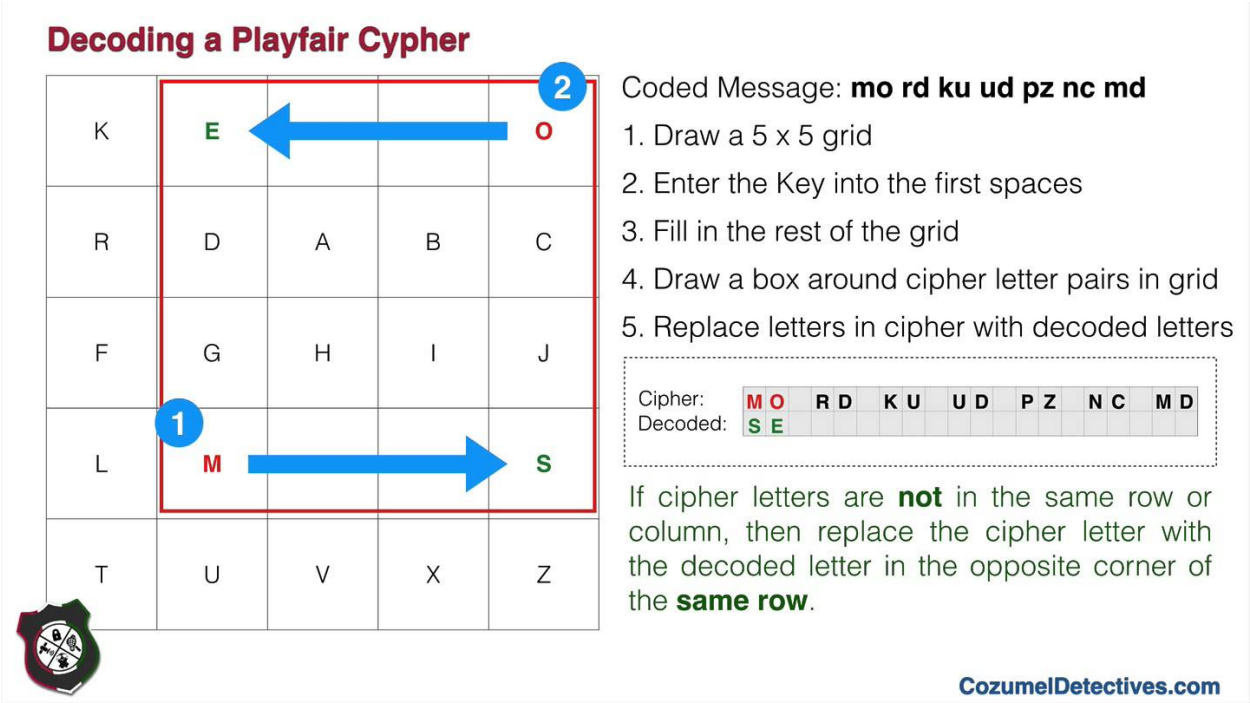
يُقال إن يوليوس قيصر أول من استخدمها، إلا أنه شاع استخدامها قديمًا، وهي وسيلة لتشفير النصوص، تعد خوارزمية التشفير الخاصة بها من أبسط الخوارزميات بالنسبة للشفرات الأخرى، حيث يقوم المرء بتبديل الحرف المراد تشفيره بالحرف الثالث الذي يليه، أي إذا أردت تشفير حرف "أ" يجب عليك تبديله بحرف الثاء، وعادة ما تُستخدم معادلة رياضية كمفتاح لفك الشفرة كالآتي.

إذا رمزنا للنص قبل التشفير بالحرف اللاتيني P، وهو مركب من مجموع الحروف الأبجدية، وإذا رمزنا للنص بعد التشفير بالحرف اللاتيني C، وعادة ما يُستخدم في التشفير مفتاح سري والذي يعرفه فقط باعث الرسالة ومتلقيها ونرمز له عادة بالحرف k، وهو عدد الحروف اللازم لتبديل الحرف المراد تشفيره، وفي حالة شفرة قيصر يكون K مساويًا لـ 3، أي الحرف الثالث بعد الحرف المراد تشفيره، وأحيانًا يكون الحرف الذي يسبقه، في حالة شفرة قيصر يكون الحرف الثالث الذي يسبقه.

> وسيلة لتشفير النصوص، تعد خوارزمية التشفير الخاصة بها من أبسط الخوارزميات بالنسبة للشفرات الأخرى، حيث يقوم المرء بتبديل الحرف المراد تشفيره بالحرف الثالث الذي يليه

إذا أردت كتابة "أنا سعيد" بشفرة قيصر، سيكون عليك إعادة توزيع الحروف الأبجدية العربية، واستخدام الحرف الثالث لكل حرف أردت تشفيره، لتنتهي جملة "أنا سعيد" بهذا الشكل في شفرة قيصر "ثيث ضقتز".

3- شفرة ديغراف (Digraph Cipher)



إحدى طرق فك شفرة "ديغراف"

هي أكثرهم صعوبة واحتياجًا للتركيز، ذلك لأنك تلعب بالحروف أكثر من أنك تفك شفرة، كلمة ديغراف في اللاتينية تعني حرفان يكونان معًا صوتًا منفردًا، وهو ما يحدث في أثناء فك شفرة ديغراف بالفعل، حيث يكتب المرء الحروف اللاتينية أو العربية على هيئة أزواج من الحروف وليست حروفًا منفردة، وبالتالي يحاول تشفير كل زوج من الحروف بزوج آخر.

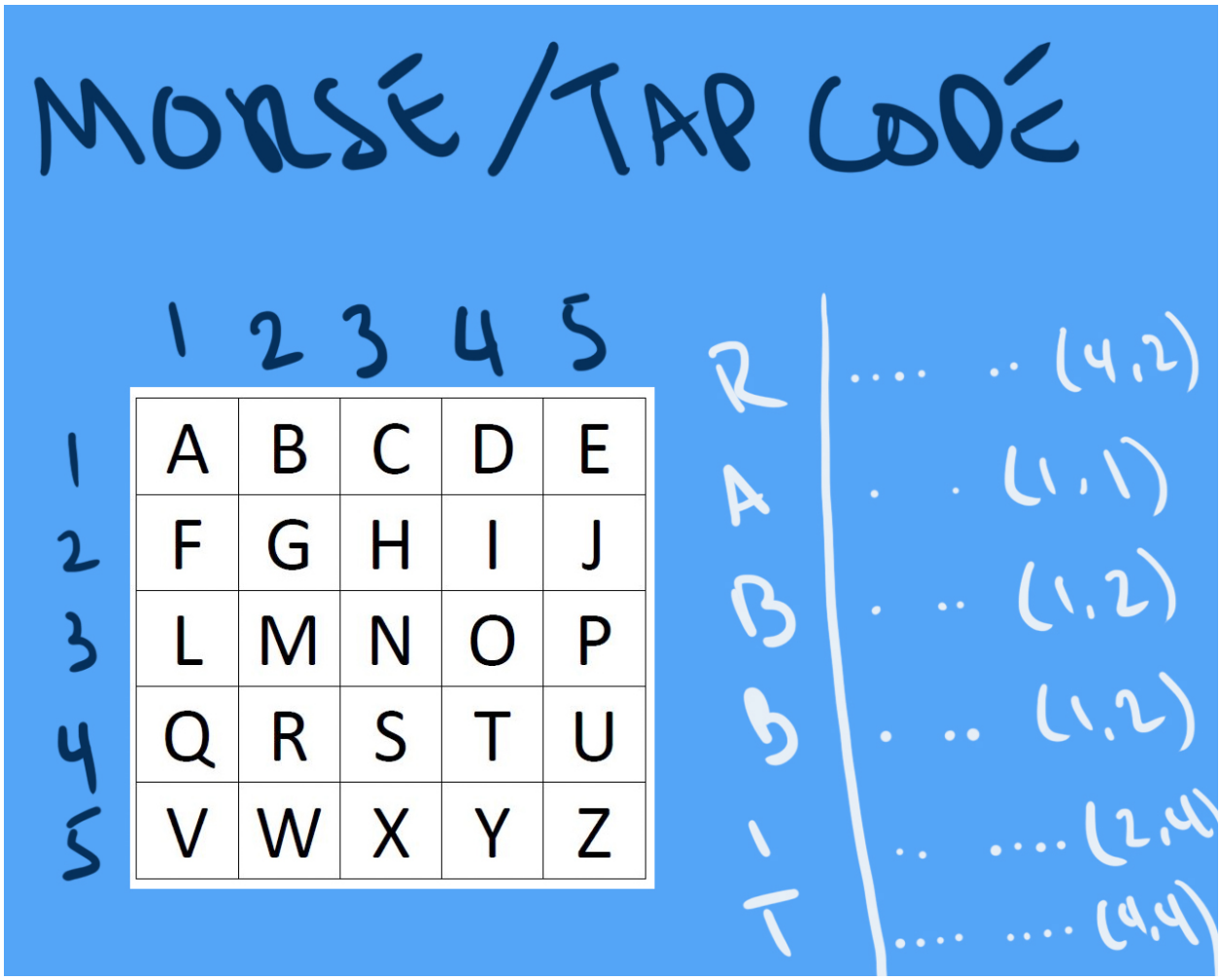
كما في الصورة، تظهر الحروف على هيئة أزواج، كل حرف منها يعادل حرفًا واحدًا من الحروف المُشفرة، وإذا أردت فك التشفير، عليك رسم جدول تقريبًا 5 صفوف و5 أعمدة إذا كنت تتعامل مع اللغة اللاتينية، وتملأ الفراغات الأولى بكلمة "مفتاح" أو "Keyword"، وهي الكلمة التي يجب عليك أنت ومن تتواصل معه فقط معرفتها، وتتبعها بالحروف اللاتينية لتملأ الجدول.

هي أكثرهم صعوبة واحتياجًا للتركيز، ذلك لأنك تلعب بالحروف أكثر من أنك تفك شفرة

بعد ذلك يمكنك البدء باللعب بالحروف طبقًا لقواعد وقوانين الشفرة، حيث تُحدد لك الشفرة ما

إن كنت تتعامل مع حرفين في نفس الصف، أو في نفس العمود أو ليسوا في نفس الصف ولا في نفس العمود كل على حسب الجدول الذي ملأته بالحروف، وعليه تختلف القواعد في كل حالة.

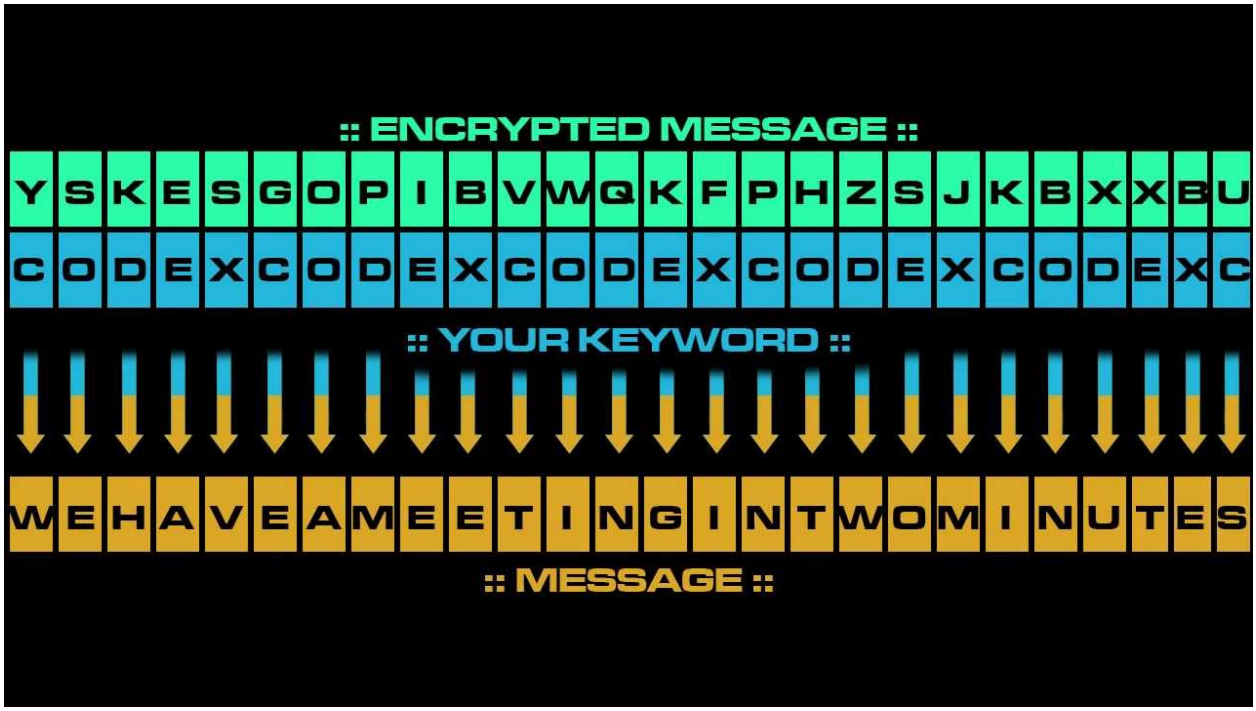
4- شفرة النقر (Tap Cipher)



قيل إنها اخترعت في السجون في حرب فيتنام، استخدم فيها الساجين مزيجًا من شفرة مورس وشفرة قيصر، ليتم دمجهما في شفرة تستعمل جدول خماسي من الأرقام من واحد إلى خمسة في صف ومن واحد إلى خمسة في عمود، وعليه يقوم الساجين بتكوين كلمات.

يستخدم فيها الساجين رقمين لتحديد الحرف المستخدم ومن ثم يقومون بكتابته على هيئة شفرة مورس على هيئة مجموعة من النقاط والشرط القصيرة والطويلة، ويستخدمون الشرطة المائلة للفصل بين الكلمات بينما تُستخدم الفاصلة (،) لتحديد الأرقام التي يستخدمونها.

5- شفرة فيجنير (Vigenère cipher)



تم إعادة اختراعها أكثر من مرة، مهمتها تشفير النص الأبجدي، ولكن يجب أن تكون الرسالة الأصلية مكتوبة من دون مسافات بين الكلمات من الأساس، كما يجب عليك استخدام كلمة مفتاحية "Keyword" في بداية التشفير، إلا أن تلك الكلمة يجب أن تكون معروفة فقط لك وللشخص الذي تود التواصل معه برسالة مشفرة.

> تتكون الشفرة باختصار من مجموعات متتالية من شفرة قيصر ولكن بترتيب رأسي وأفقي مختلف

فمثلًا إذا اخترت عبارة غدًا لدينا اجتماع وكتبتها باللغة اللاتينية ستكون كالآتي "Tomorrowwehaveameeting" ومن ثم يجب عليك كتابة الكلمة المفتاحية ولتكن كلمة "أكواد" أو "Codes" تحت العبارة التي تود تشفيرها، وعليك تكرار الكلمة المفتاحية حتى تنتهي العبارة التي تود تشفيرها، ثم عليك استخدم جدول "فينيجر" لتقاطع حروف العبارة الأصلية مع حروف الكلمة المفتاحية بشكل رأسي ومن ثم أفقي.

تتكون الشفرة باختصار من مجموعات متتالية من شفرة قيصر ولكن بترتيب رأسي وأفقي مختلف، تم تحويل الشفرة حاليًا لنموذج جبري ليتم حلها عن طريق المعادلات الرياضية الجبرية لأجل فك شفرات بعض الرسائل الحديثة.

تعد هذه الشفرات من أشهر وأسهل الشفرات الكتابية المستخدمة التي يستطيع الإنسان تشفيرها وفك شفرتها بنفسه دون الحاجة لاستخدام آلة أو حاسوب، ولا استخدام أنواع معينة من البرمجيات لتفكيكها، ولهذا يستخدمها الكثير من الهواة لإخفاء محتوى كلمات السر الخاصة بهم، أو في إرسال رسائل يستطيع فهم محتواها القليل من الناس.