

ركزنا على خوارزميات التشفير التي يمكن استخدامها لتوفير السرية. يصبح من الممكن إعادة بناء رسالة النص الأصلي عبر النص الملتفّر. ومع ذلك يوجد حالات عديدة يجري فيها استخدام التشفير، لكن دون الحاجة إلى توفر القدرة على استنباط محتوى «الرسالة» الأصلية من صيغتها بالحفاظ على سرية كلمات مرورهم؛ أيضا يحاول ضمان هذه السرية. هنا عادةً في القدرة على التحقق من صحة كلمة مرور جرى تسجيلها؛ توجد حاجة إلى توفر القدرة على استنباط كلمة المرور من القيمة المخزنة. هناك أيضا العديد من الأمثلة في التشفير يجري فيها ضغط الرسائل الكبيرة إلى سيكون من الحتمي أن تُفسي أكثر من رسالة واحدة إلى نفس سلسلة الأرقام تتمثل الفكرة الأساسية لدوال الاختزال في أن قيمة التشفير الملحور الناتجة وللقيمة الناتجة عن اختصار الرسالة الأصلية أسماء تتضمن عملية التشفير الملحور عددا من التطبيقات؛ تقبل دوال الاختزال مداخل بأي طول وتُطلق على ذلك «صدام». يجب انتقاء دالة الاختزال جيدا لضمان استحالة اكتشاف حالات الصدام حتى يترتب على ذلك عدد من النتائج، قيم البصمات الرقمية املمكنة. هناك ثمانية قيم محتملة فقط للبصمة الرقمية، فسيكون هناك احتمال نسبته 1/8 في أن يكون لرسالتني اعتباريتني نفس القيمة. بالإضافة إلى ذلك، اشتغال أي مجموعة تتألف من تسع رسائل أو أكثر على حالة صدام واحدة على الأقل.