ركزنا على خوارزميات التشفري التي يمكن استخدامها لتوفري السرية. يصبح من املمكن إعادة بناء رسالة النص الأصلي عبر النص املشفَّر. ومع ذلك يوجد حالات عديدة يجري فيها استخدام التشفري، 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 املرور من القيمة املخزنة.ً هناك أيضا العديد من الأمثلة في التشفري يجري فيها ضغط الرسائل الكبرية إلى سيكون من الحتمي أن تُفضي أكثر من رسالة واحدة إلى نفس سلسلة الأرقام ً تتمثل الفكرة الأساسية لدوال الاختزال في أن قيمة التشفري املحور الناتجة تمثل وللقيمة الناتجة عن اختصار الرسالة الأصلية أسماءً تتضمن عملية التشفري املحو ً ر عددا من التطبيقات؛ تقبل دوال الاختزال م َدخلات بأي طول وتُ نطلق 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 ٪١٢٫٥ُ في أن يكون لرسالتني اعتباطيتني نفس القيمة. بالإضافة إلى ذلك، اشتمال أي مجموعة تتألف من تسع رسائل أو أكثر على حالة صدام واحدة على الأقل.