شفره أتباش *Atbash Cipher*

هذه الشفرة أيضا من أبسط أنواع الشفرات ، وهي كانت في الأصل للغة العبرية ، ولكن يمكن استخدام المفهوم في باقي اللغات .
وطريقتها كالتالي ، وهي أن نجعل الحرف الأول في اللغة هو الحرف الأخير ، والحرف الثاني هو قبل الأخير ، وهكذا...

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA
مثلا ، لتشفير الكلمة money ، يصبح لدينا الناتج nlmvb .

في بعض الأحيان من الممكن أن الكلمات بعد التشفير يكون لديها معني وهي مشفره مثل:
النص الأصلي = "hob" بعد التشفير تصبح "sly" ، وهكذا للكلمات الأخرى
النص الأصلي = "hold" بعد التشفير تصبح "slow"
النص الأصلي = "holy" بعد التشفير تصبح"slob"
"horn" = "slim"
"irk" = "rip"
"low" = "old"
"glow" = "told"
"grog" = "tilt".

ومع ذلك تبقى تلك الشفرات من أسهل الأنواع على الإطلاق!

شفره *ROT13*

تعتبر هذه الشفرة (كما هو الحال مع جميع شفرات نوع Monoalphabetic) ضعيفة للغاية ، حيث أن التشفير وفك التشفير يتم بنفس الطريقة ، و مفتاح التشفير 13 ، وللتشفير نقوم بجمع 13 على الحرف الأول من النص الأصلي ، ولفك التشفير تقوم أيضا بجمع 13 على الحرف الأول من النص المشفر .

P = ROT13 (ROT13 (P))

الحرف p يعني الحرف الأول من النص الأصلي Plaintext ، نقوم بعدها بتشفيره بجمع 13 حرف إليه، لنفرض أن الحرف الأول من النص الأصلي هو D ، الحرف D قيمته 3 ، نجمع (3+13)%26 والناتج هو 16 ، أو ممكن نتحرك 13 خطوه من الحرف D والناتج في النهاية سواء بالجمع أو بالتحرك هو الحرف Q .

قبل أن نبدأ عمليه التشفير دائما ، نضع هذا الجدول الذي سنستخدمه كثيرا لتسهيل معرفه مواقع الحروف: