وهذه صوره لها وهي في العالم الحقيقي :

كيف نقوم بالتشفير في هذه العجلة ، ببساطه أولا أقوم باختيار المفتاح وهو في هذه الحالة عبارة عن حرف واحد ، وليكن اخترت المفتاح S .

الآن قبل أن أبدأ بالتشفير ، أحرك الجزء الداخلي (الخاص بالشفرة) وأجعل الحرف S تحت الحرف A كما هو موضح في الصوره أعلاه (الصوره الأولى للعجلة) .

الآن اذا أردت أن أشفر الحرف G ، أنظر في الجزء الخارجي إلى G ، بعدها أشاهد ماذا يقابله وهو الحرف. Y وهكذا لباقي الحروف في النص.

فك التشفير هو العملية العكسية ، أريد أن أفك تشفير الحرف H ، أنظر في الجزء الداخلي إلى H وأنظر ما يقابله وهو الحرف p . وهكذا...

كسر شفرات فجينير *Vigenere* البسيطة

لأن المفتاح يتكرر في هذه الشفرات بحيث تعيد دوره المفاتيح من البداية من مره (تعرف هذه بالـ **Period** أي الفترة التي ما بين تكرار المفتاح ، وكلما كانت هذه الفترة أطول، كلما كانت الشفرة أكثر أمانا)، يمكن استغلال هذه الإعادة وتطبيق طريقه التحليل الإحصائي ، ولكن يجب أن يكون النص المشفر كبير بما يكفي ، أيضا يجب أن يتم معرفه عدد المفاتيح المستخدمة أو **Key Length** وهو أصعب جزء في العملية.

وفي حال تم معرفه عدد المفاتيح Key Length نقوم بتقسيم النص المشفر إلى مجموعه صغيره من النصوص ، بعدها وبطريقه ما نطبق عليها طريقه التحليل الإحصائي على كل مجموعه على حده ، ونلاحظ ما هو الحرف الذي يتكرر كثيرا في المجموعة الأولى وقد يكون هو E (نعيد نفس خطوات كسر Monoalphabetic)، طبعا على كل مجموعه من المجموعات الصغيرة.