و هنا يتم استخدام الهادريسك كذاكره ، ومبدأ عملها في حاله امتلأت الذاكرة يتم إفراغ بعض من محتوياتها التي لم تستخدم من وقت طويل إلى الهادريسك في مكان معين ، بعدها في حال طلبت تلك المواقع (التي أصبحت موجودة في الهارديسك) سوف يقوم نظام الذاكرة بعمل تبديل Swap بين المحتويات ، على العموم في عام 1999 قام احدهم بكتابه برنامج لمسح هذا المكان التي تحفظ فيه الذاكرة وتمكن من إيجاد الباسورد الخاص به في احد البرامج.

كل طرق الهجوم السابقة ، دليل على أنك وحتى "بنظام تشغيلك الخارق" قد تكون بيانات وملفاتك في خطر ، لذلك لا بد من اضافه الحماية بواسطة التشفير و عدم الاعتماد على تلك الحماية المقدمة من نظام التشغيل والافتراض بأن المخترق يعرف أساليب التراوغ والاختراق ، والتشفير هو ببساطه تحويل النصوص المفهومة غلى كلام غير مفهوم gibberish ،

مثل: my name is wajdy , im a Beginer in java programming
تصبح: kjdkp isjeu epdmp owdkl kld dkl kqklq ds

وحتى لو استطاع المخترق بالوصول إلى نظامك وكسره ، سوف يشاهد ملفك بالصورة السابقة ، ولن يحصل على شيء مفيد أبدا .

**يعني بالتشفير سوف تحصل على (أهداف التشفير ):**
*الخصوصية أو السرية Privacy
لن يستطيع احد قرائه ملفاتك السرية (وملفاتك الطبية) ، إلا من تريده أنت فقط !

*تكامل البيانات Data Integrity
ويعني التأكد من أن رسالتك لم تتغير (قام احدهم بتغيير شيء ما ) أثناء إرسالك للرسالة ، أو قام بتغيير ملف محفوظ مسبقا .

*التحقق Authentication
التحقق من الشخص الفلاني هو الشخص الذي تريده لقرائه الرسالة ،

*عدم الإنكار nonrepudiation :
مصطلح غريب قليلا ، ولكن الفائدة هنا جعل الشخص المرسل للرسالة الالتزام وعدم إنكار انه هو الشخص المرسل للرسالة .

## التشفير بالمفتاح المتناظر ***Symmetric key Cryptography*** :

نذكر مره أخرى أن التشفير هو عبارة عن تحويل المعلومات المفهومة إلى معلومات غير مفهومه Gibberish ، والعملية العكسية فك التشفير ، هي عمليه تحويل المعلومات الغير مفهومه إلى معلومات مفهومه .

النوع الأول من أنواع التشفير هو: التشفير بالمفتاح المتناظر ، وهنا سوف نستخدم مفتاح مع خوارزمية (هناك الكثير) لتشفير المعلومات ، وسوف نستخدم نفس المفتاح ونفس الخوارزمية لفك التشفير . (لاحظ يجب أن تكون نفس المفتاح ونفس الخوارزمية ، ومن هنا جاء الاسم "متناظر" ) .