التشفير و فك التشفير – نظرة سريعة –

عصام حنفي!!!Boris!!!

البيـــانات تستطيع حفظها أو نقلها من خلال شبكة Network بكل سهولة مع ذلك فأنك تستطيع استخدام متطلبات للتصريح لكي تقوم بالسيطرة على عملية الدخول لبرامجك بطريقة شرعية بإعطاء التصريحات والتصريح عن متطلباتها لكي تحمى بياناتك.

مبدئيا ، عند دخول المهاجم إلى القرص الصلب H.D أو البنية التحتية لل Network يستطيع بطرق ملتوية التعديل والعبث ببياناتك والموجودة على الشبكة.

تستطيع استخدام التشفير cryptography لحماية بياناتك الخاصة والتي يحفظها برنامجك أو يقوم بنقلها عبر أو إلى أي تدفق Stream.

الـ Net Framework. يزودك بفئات لبعض الأنواع المختلفة من التشفير cryptography متضمنـا التشفير التناظري symmetric و غير التناظري - asymmetric و المزج hashing والـتوقيعات الرقمية digital signatures .

التشفير التناظري Symmetric encryption

يستعمل هذا النوع من التشفير مفتاح سري وحيد Symmetric key أي المفتاح المتناسق و يعرف بأنه مفتاح تشفير سرى يستخدم لعمليتين التشفير وفك التشفير الـ encrypt والـ decrypt للبيانات .

الخوارزمي الذي يعمل بهذا المبدأ يعرف باسم الـ cipher يقوم بمعالجة النصوص البسيطـة بمفتاح التشفير السري لكي يقوم بإنشاء البيانات المشفرة والتي تسمى cipher text و هو آمن إلى حد كبير حيث لا يمكن معرف النص الكامل Plain Text بدون معرفة المفتاح السري Secret Key

خوارزم الـ Symmetric يعمل بسرعة عالية جدا وهو ملائم ومرن جدا عند تشفير بيانات كبيرة الحجم وهو أمن ومحكم ومحل ثقة عن التعامل به أثناء عمليات التشفير.

بشكل أخر مهاجم النظام يستطيع مطابقة النص المشفر بإعطاء ال Cipher Text والوقت المناسب لفكهـا لكي يتعرف على النص الكامل، المهاجم الذي يريد اقتحام نظامك يحتاج إلى استخدام Brute Force Attack على سبيل المثال لكي يقوم بتوليد الجميع المفاتيح الممكنة Symmetric Keys وذلك بتجربة جميع المحاولات لاستنتاج أو لتوليد الـ Symmetric Keys .

الصورة التالية تبين لنـا كيفية نقل البيانات المشفرة و المفاتيح باستخدام أساليب مختلفة للاتصالات والنقل لكي تمكن المستلم من إعادة فك التشفير لهذه الرسائل.

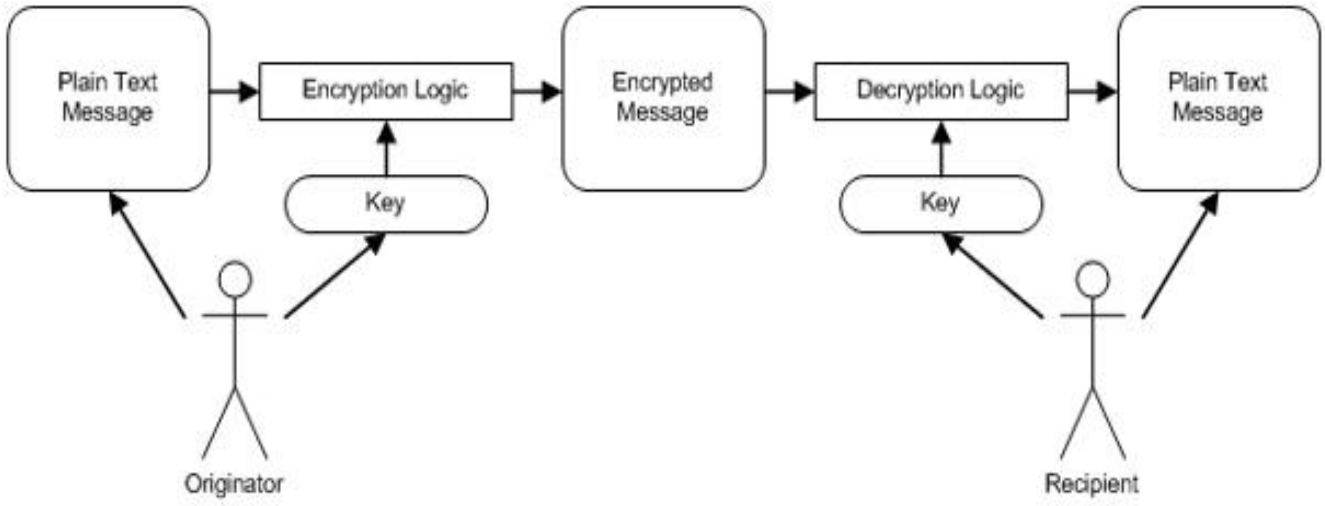

Diagram 1. Symmetric Encryption