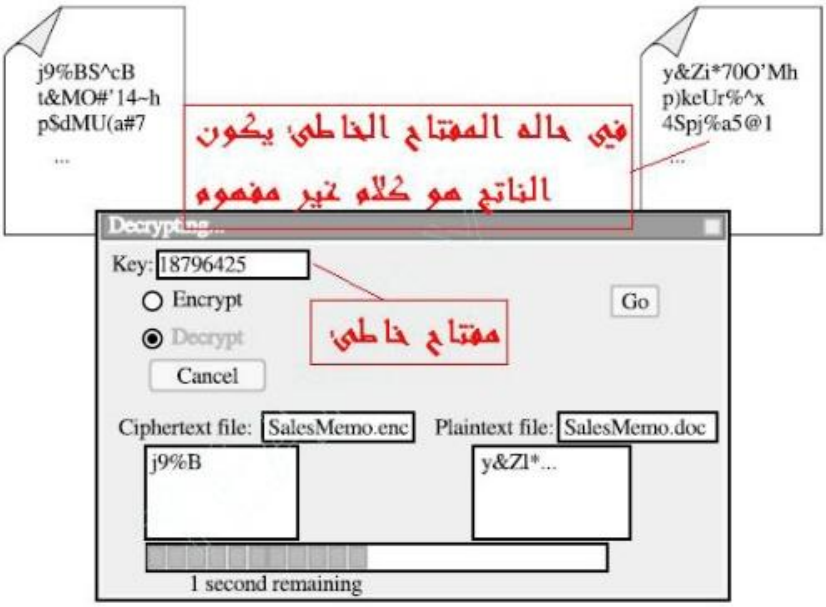

وهكذا ، أي احد لن يستطيع الحصول على الرسالة الاصليه إلا بعد كتابه المفتاح السري ، وإذا ادخل المفتاح الخاطئ سوف يكون الناتج غير مفهوم ،وحتى لو كان هذا المفتاح الخاطئ اقل من المفتاح السري برقم واحد .

طريقه التشفير السابقة التي استخدمناها تسمى (**التشفير بالمفتاح المتناظر أو المتماثل Symmetric key Cryptography**) والبعض يسميها **Secret key Cryptography** ، أيضا اسم (**التشفير التقليدي Conventional Encryption**) ، لكن نحن نأخذ المصطلح الأول .

بالنسبة إلى علم التشفير هناك الكثير من المصطلحات لها نفس المعنى ، على العموم سأحاول وضع الأغلب والأشهر هنا .
في حال أردت أن تحول المعلومات المفهومة إلى غير مفهومه تسمى العملية **تشفير Encryption**
في حال أردت أن تحول المعلومات الغير مفهومه إلى مفهومه تسمى العملية **فك التشفير Decryption**

للتشفير أو فك التشفير ، يجب أن تتبع **خوارزمية Algorithm** معينه ، الخوارزمية هي مجموعه خطوات مرتبه بطريقه معينة تؤدي هدف معين ، بالطبع مفهوم الخوارزمية مفهوم لدى اغلب المبرمجين ، وتستطيع تطبيق الخوارزمية بأي لغة برمجه ، المهم في التشفير الخوارزمية ممكن أن تكون علميه رياضيه معقده للغاية وممكن أن تكون عمليه جمع بتات أو عمليه XOR (في اغلب الخوارزميات التعامل بيكون على حسب البت bit ، لذلك سوف تستخدم عمليات الـ Bitwise operation) .