عنوان المقال: التشفير

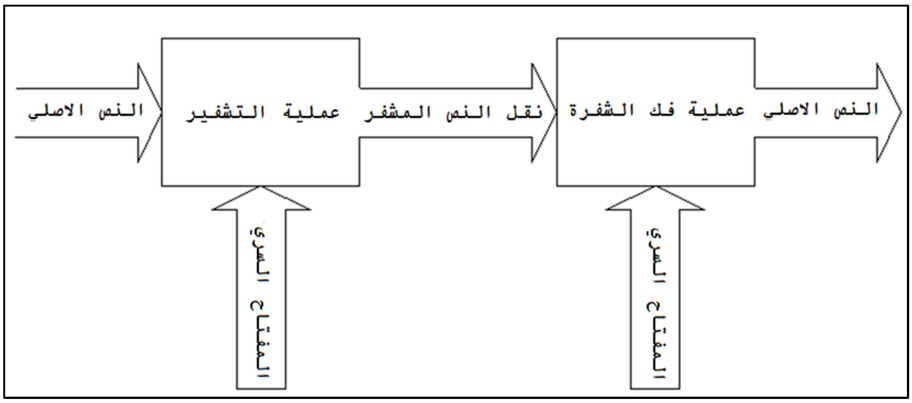
م. د. نجلاء فلاح حميد
جامعة الكوفة / كلية علوم الحاسوب والرياضيات / قسم الرياضيات
najlaa.hameed@uokufa.edu.iq

علم التشفيرهو دراسة المبادئ والتقنيات التي يمكن تحويلها الى نص مشفر بحيث يمكن استرجاعها لاحقا من قبل المستخدمين الشرعيين باستخدام مفاتيح قد تكون سرية او معلنة، ولكن بصورة اما تكون مستحيلة او غير قابلة للحل ضمن فترة زمينة معينة لاي شخص غير مصرح له استرجاع تلك المعلومات.

في الحقيقة علم التشفير كلمة اصلها يوناني مع ما يسمى تحليل الشفرة والتي اصلها يوناني ايضا يكونان ما يسمى بعلم التشفير . أما ما يسمى بالتشفير الحديث فهو دراسة الأنظمة الرياضياتية لحل النوعين الرئيسيين من المشاكل الأمنية (المصداقية والخصوصية). يوجد نوعان مختلفان من أنظمة التشفير:

① انظمة التشفير بإستخدام المفتاح السري:

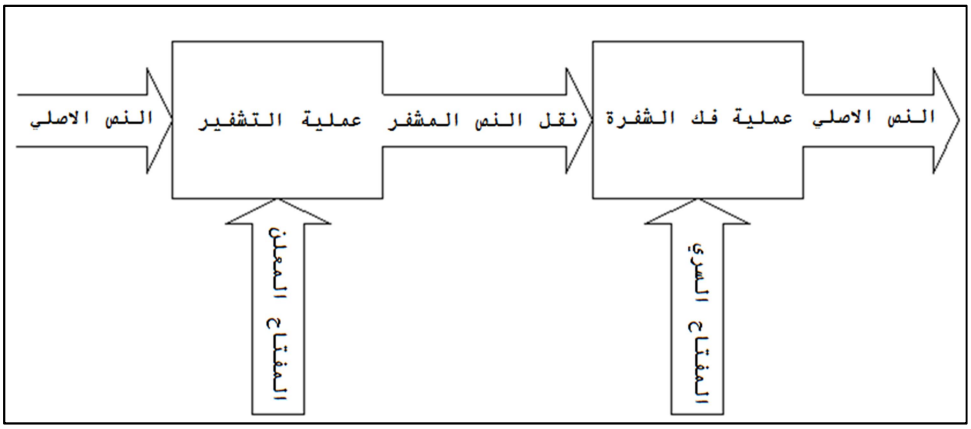
يسمى أيضاً التشفير المتماثل حيث انه يستخدم مفتاح واحدا لعملية التشفير وفك التشفير للبيانات قيد العمل. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه الاطلاع على كافة البيانت التي تم تشفيرها.



صورة (١) التشفير بإستخدام المفتاح السري

② انظمة التشفير بإستخدام المفتاح المعلن

يسمى ايضا التشفير اللامتماثل تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح المعلن والمفتاح السري، حيث أن المفتاح المعلن هو لتشفير الرسائل والمفتاح السري لفك تشفير الرسائل.



صورة (٢) التشفير بإستخدام المفتاح المعلن