

بسم الله الرحمن الرحيم

والصلاة والسلام على أشرف الخلق والمرسلين ، نبينا محمد عليه أفضل
الصلاة والتسليم ، أما بعد ،

بين يديك أخي القارئ الكريم ، كتيب بسيط يتناول وبشكل سريع التشفير بالطرق
الكلاسيكية ، والذي كان في الأصل عبارة عن مجموعه من الدروس قمت بوضعها في
منتديات العاصفة www.3asfh.com ، وتم إعادة تنسيق محتويات الدروس ، مع
إضافه العديد من النقاط الجديدة ، فشكر خاص لأعضاء ذلك المنتدى ، والقائمين
عليه .

الطرق الكلاسيكية Classical Method هي عبارة عن طرق تشفير استخدمت منذ زمن
بعيد وخاصة في أيام الحرب العالمية الأولى والثانية ، حيث كانت خطط الحرب
وطرق الهجوم على العدو ترسل عن طريق رسائل عادية مكتوبة بخط اليد (في
الأغلب) ولكنها تشفر بأحد الطرق ، خوفاً من أن تقع في أيدي العدو وبالتالي تفشل
تلك الخطط .

بالرغم من أن تلك الطرق غير مجديه أبداً في الوقت الحالي ، فإنها موضوع هذا الكتيب.
ربما تتساءل وما الجدوى من ذلك ، الجواب بكل بساطه ، لأنها تعتبر الأساس للكثير
من الشفرات الحديثة ، إضافة إلى أن دراستها ينمي العقل على التفكير والبحث ، حيث
أنها تعتمد على فقط على التلاعب بالأحرف (إما تبديل أماكن الأحرف
Transposition ، أو تبديلها بأحرف أخرى بعد عمله حسابيه ما **Substitution**) ،
غير ذلك فعملية كسر هذه الشفرات أمر في غاية المتعة .

ينقسم الكتيب إلى أربعة أقسام رئيسيه :

القسم الأول الأساسيات يتناول هذا القسم بعض من الخوارزميات والقواعد الرياضية
الضرورية في عالم التشفير لبعض الطرق الكلاسيكية ، مثل نظريه القسمة ، الأعداد
الأولية ، خوارزمية أقليدس ، خوارزمية اقليدس الممتدة .

القسم الثاني Introduction to Classical Cipher يتناول الشفرات الكلاسيكية
وكيف يمكن التشفير وفك التشفير بتلك الطرق ، و يتناول وبشكل مبسط كيف يمكن
كسر الشفرات Cryptanalysis لبعض من هذه الطرق .