القسم الأول : الأساسيات PRELIMINARIES

لفهم أغلب الشفرات الحديثة يلزم فهم الكثير من **نظريه الأعداد Number Theory** ، ولكن بما أن الكتيب يركز على الشفرات بالطرق الكلاسيكية فسوف نتناول ما يهمنا فقط في الوقت الحالي . وسوف تكون القواعد مكتوبة ولكن من غير إثبات رياضي لها Prove ، يمكنك تجاوز هذا القسم والعودة إليه لاحقا عندما تحتاجه في شفره Affine Cipher ، ولكني لا أفضل ذلك .

اذا كان لدينا عددين صحيحين a و b ، وكان a !=0 (لا يساوي 0) . نقول عن a يقسم b اذا كان لدينا عدد ثالث c بحيث b = a*c . اذا كان a يقسم b نشير إليه بالرمز a|b .

مثال بسيط :

3|27 صحيح ، لان 27 = 9*3 .

5|32 غير صحيحة ، لأن 32 = 4*c ولا توجد عدد صحيح يحل مكان c .

اذا كان لدينا ثلاثة أعداد صحيحة x,y,z ، وكان x|y و y|z اذا x|z .

مثال :

لدينا 3|9 ، و 9|72 ، اذا 3 تقسم 72 = 3|27

خوارزمية القسمة THE DIVISION ALGORITHM

وهي أحد الخوارزميات المهمة جدا ، حيث تقول انه يمكننا أن نمثل أي عدد صحيح ، وذلك بواسطة ضرب عدد صحيح b مع اضافه باقي r بحيث يكون الباقي عدد موجب وأقل من العدد b .

اذا كان لدينا عددين صحيح y,b ، وكان b أكبر من صفر ، اذا سيكون لدينا عددين q,r بحيث :

Y = b*q + r

q هو حاصل القسمة Quotient . r هو الباقي remainder . b هو المقسوم Divisor ، y هو القاسم dividend .

مثال لدينا المعادلة :

65 = 3*q + r

قيمه ال q هي 21 (وذلك بقسمه 65 على 3) ، والباقي r هو 2 .

3*21+2 وتساوي 65 .

PDF created with pdfFactory Pro trial version www.pdffactory.com