ملخص الرسالة

عندما أرسل يوليوس قيصر رسائله إلى عماله على الأقاليم المختلفة لم يكن يثق في رسله، وعلى ذلك قام باختراع نظريه شفرية عرفت بنظرية الإزاحة، حيث قام باستبدال كل حرف Aبحرف الـ D وكذلك حرف الـ B بحرف الـ E ... الخ. و بالتالي كل من يعرف نظرية الإزاحة الثلاثية فقط يستطيع أن يحل ويقرأ رسائله. وكان هذا حجر الأساس لنظريات النظم الشفرية.

على مدار التاريخ شعر الإنسان دائما بحاجته إلى سرية المعلومات وحفظها بعيدا عن الآخرين، وعلى ذلك كان علم الشفرة هو الأساس في تكوين الأنظمة الشفرية والتي استخدمت لآلاف السنين لإخفاء المعلومات سواء كانت موضوعة أو منقولة عن من هو ليس معنى بهذه المعلومات والذي بالطبع يحاول جاهداً تحليلها وكشفها. كما كان و مازال هناك صراع دائم بين صانعي الشفرة وبين محلليها، على انه في حالة كسرها يكون هناك حاجة لأخرى جديدة.

وقد كانت استخدامات الشفرة في الثلاثين عاماً الماضية قاصراً على الأغراض العسكرية والحكومية وبعد ذلك امتدت إلى الحياة العامة، ودليلاً على ذلك استخدام الشفرة في ماكينات الصرف وكوابل التليفزيون والإنترنت والتجارة الإلكترونية.....الخ، الأمر الذي ولد الحاجة إلى البحث والتعمق في علوم الشفرة وتحليلها.

وتكمن الفكرة الرئيسية في عملية الشفرة في عمليتين أساسيتين هما عملية التشفير وعملية الحل، حيث تقوم الأولى بتحويل النص الواضح إلى نص غير مقروء يسمى بالنص الشفري وتقوم العملية الأخرى بعكس هذا التحويل واستعادة النص الواضح، وكلتا العمليتين ترتبطان ارتباطاً وثيقاً بما يسمى بالمفتاح.

ويمكن تقسيم الأنظمة الشفرية إلى مجموعات تعتمد على كيفية تكوينها، حيث انه في بعض الأنظمة يستخدم نفس المفتاح في كل من عمليتي التشفير والحل وهذه تسمى بالأنظمة المتماثلة أو الأنظمة التقليدية أو شفرة المفتاح السري، في حين أن الأنظمة الغير متماثلة تستخدم مفاتيح مختلفة في عمليتي التشفير والحل وتسمى أيضا بشفرة المفتاح العلني. وتنقسم شفرة المفتاح الخاص نوعين أساسيين هما: شفرة المتسلسلات وشفرة القوالب، على انه في حين تقوم شفرة المتسلسلات بتشفير حرف واحد تلو الآخر تقوم شفرة القوالب بتشفير مجموعة من الحروف باستخدام دالة معقده.

والهدف الرئيسي من هذه الرسالة هو تقييم النظم الشفرية المختلفة لكل من شفرة القوالب وشفرة المتسلسلات، وذلك لتكوين معيار للقوة الشفرية لمثل هذه النظم ووضع مقاييس واضحة لمقارنة أي منها بالآخر. غير أن معايير التقييم لكثير من الأنظمة الشفرية المختلفة ليست كاملة الوضوح؛ إلا أن هذه الرسالة تعد محاولة عملية لتقديم معايير عامة لتقييم شفرة المفتاح الواحد بشقيها (المتسلسلات والقوالب). حيث انه في حالة شفرة القوالب يكون الاختبار الإستاتيكي العشوائي هو أهم معايير التقييم وهو أيضا أحد المعايير المستخدمة لتقييم شفرة المتسلسلات.