٥١ = ١+٣+٩+٣٨ ، أي الاعداد الأول والثاني والرابع والسادس من مصفوفة المفتاح والتي نمثلها بالعدد ١ في الموقع الأول والثاني والرابع والسادس ، وبالعدد صفر في الموقعين الثالث والخامس لتكون النتيجة ١٠١٠١١ أو ٤٣ وهو النص الأصلي ، وتكمن سرية هذه الطريقة في كون تجزئة عدد ما إلى مجموع أعداد صحيحة مختارة من مجموعة معينة مسألة في غاية الصعوبة ، إذا لم تكن هناك معلومات اضافية . وفي هذه الحالة فان المعلومة الاضافية تكمن في مفتاح حل الشفرة ، وهذه المعلومة هنا هي ان كل عدد من مصفوفة المفتاح الشفري يزيد عن مجموع الاعداد التي سبقته ، أي الاعداد التي تقع إلى اليسار منه .

يمثل كل من الأمثلة ٢ و ٣ النظم الحديثة في التشفير ، والواقع ان المثال الثاني يمثل أهم الطرق الشفرية ذات المفتاحين ، ويدعى نظام ريفست شمير ادلمان ، وقد قاوم هذا النظام جميع محاولات الكسر التي تعرض لها . أما المثال الثالث فيمثل أحد النظم الحديثة التي لم تصمد أمام محاولات الكسر ، وتوجد الآن طرق سريعة لكسر هذا النظام مبنية على مفاهيم رياضية متقدمة يمكن للقارئ الاطلاع عليها في السجل العلمي لمؤتمر الشفرة لعام ١٩٨٢م والذي يعقد سنوياً بولاية كاليفورنيا في الولايات المتحدة الأمريكية .

كما ان هناك نظماً للتشفير تجمع الخصائص الشفرية المتسلسلة والمقطعة لأنها تقسم النص إلى أجزاء كل واحد منها يعد سلسلة من الاعداد الثنائية ، ومن أشهر هذه النظم ما يسمى « النظام الشفري القياسي » الذي تبنته هيئة المقاييس والمواصفات الأمريكية ، وعلى الرغم من انه ليست هناك محاولات ناجحة معلنة لكسر هذا النظام إلا انه تعرض لكثير من النقد لأن بعض تفاصيل تصميمه أبقى عليها سراً بإيعاز من وكالة الأمن القومي الأمريكي مما أدى إلى عدد من الشكوك حول درجة أمنه .

المراجع :

١ ـ Cryptography and Data Security, D. Denning, Addison-Wesley 1983.

٢ ـ Data Security, D. Denning and P. Denning, ACM Computing Surveys Vol 11 No. 3 1979.

٣ ـ The Codebreakers, D. Khan, Macmillan 1967.

٤ ـ Asymmetric and Symmetric Encryption, G.J. Simmons, ACM Computing Surveys, Vol 11, No. 4 1979.

٥ ـ Cryptology in Transition, A. Lempel, ACM Computing Surveys, Vol 1 No. 4 1979.

عرض كتاب

مقدمة في الاتصالات

عرض : د. إبراهيم المعتاز

جامعة الملك سعود

طبع في مطابع جامعة الملك سعود ١٤٠٩هـ

ألف هذا الكتاب الدكتور سعد علي الحاج بكري ، والدكتور محمد عبدالرحمن الحيدر ، ويعد الكتاب مساهمة جيدة في حركة تعريب العلوم الحديثة ومحاولة ناجحة لكتابة العلوم التقنية والهندسية باللغة العربية ، والكتاب هندسي الاختصاص يخاطب المهندسين والعاملين في قطاع الاتصالات بشكل خاص إلى جانب تقديم الأسس العلمية الهندسية في مجال الاتصالات ، ويحتوي الكتاب على خمسة فصول رئيسة ، يبدأ بنظرة عامة لهندسة الاتصالات ثم المباديء الأساس لتحليل الطيف ثم أنواع وأساليب تعديل (تضمين) ارتفاع الموجات (المطال) والتردد والنبضات .

نظرة عامة إلى هندسة الاتصال

يقدم الفصل الأول من الكتاب نظرة عامة إلى هندسة الاتصال تبدأ بلمحة تاريخية تستعرض تطور أساليب الاتصال وتنتهي بتطلعات لمستقبل هندسة الاتصال وأساليبها ، ويقدم الفصل أيضاً شرحاً لعناصر وأنظمة الاتصالات والتي تتكون عادة من :

١ ـ مصدر المعلومات .
٢ ـ محول المعلومات المرسلة .
٣ ـ جهاز ارسال .
٤ ـ قناة اتصال .
٥ ـ جهاز استقبال .
٦ ـ محول المعلومات القادمة .
٧ ـ مقصد المعلومات .

وترسل المعلومات وتستقبل بشكل تمثيلي أو رقمي اما بصورة مستمرة واما متقطعة ، وتشمل ثمانية مجالات رئيسة لتردد الموجات عبر طيف الترددات الكهرومغناطيسية والتي يحتوي هذا الفصل أيضاً على وصف مفصل لها .

ويقدم الفصل أيضاً تعريفاً ميسراً لفكرة تعديل (تضمين) الموجات ولظاهرة التشويش ، ثم يعرض الفصل أخيراً للأساليب المختلفة في تحليل أنظمة الاتصالات في مجالي الزمن والتردد وتحويل التعبيرات الرياضية من مجال لآخر بمساعدة النظريات التالية :

١ ـ نظرية تحليل الترددات .
٢ ـ نظرية التعديل (التضمين) .

٣ ـ نظرية الاتصالات .

٤ ـ النظرية الاحصائية للكشف والتخمين .

٥ ـ نظرية المعلومات والرموز .

٦ ـ نظرية حركة احمال أنظمة الاتصالات .

تحليل ترددات الطيف

يستعرض الفصل الثاني تحت هذا العنوان استخدام الوسائل الرياضية لايجاد مواصفات الموجات في مجال التردد ، ومعرفة العلاقة التي تربط هذه المواصفات بتلك القائمة في مجال الزمن ، ويساعد هذا في دراسة الموجات المرسلة والمستقبلة والمعالجة في أنظمة الاتصالات ، ويشمل هذا الفصل دراسة مفصلة لمفكوك فوريور Fourier Expansion وتحويل فوريور Fourier Transform واستخدامها في حساب القدرة القياسية للموجات عند الترددات المختلفة ، والقدرة القياسية للموجات هي اصطلاح يعبر عن القدرة الناتجة عن تطبيق جهد موجة كهربائية على مقاومة كهربائية تبلغ قيمتها أوماً واحداً .

ثم يعرض الفصل الثاني أيضاً لنظرية الالتفاف وطرق معرفة استجابة الأنظمة للموجات الداخلة . ونظرية الالتفاف Convolution theory تستخدم لايجاد الموجات ذات تحويل فوريور معلوم عبارة عن حاصل ضرب تحويلين فوريوريين لموجتين معروفتين . كما يستفاد من معرفة استجابة الأنظمة تحديد الموجات الخارجة من هذه الأنظمة ومعرفة دالة التحويل ، وينتهي هذا الفصل بشرح ظاهرة ارتباط الاشارات والتي يحتاج إليها مهندس الاتصالات كثيراً لمعرفة مدى الترابط أو التشابه بين موجتين .

تعديل (تضمين) الموجات

يحتوي الكتاب على شرح مفصل لعملية تعديل الموجات ، يشمل تعديل ارتفاع الموجة كما في الفصل الثالث ، وتعديل التردد كما في الفصل الرابع ، وأخيراً تعديل النبضات في الفصل الخامس والأخير .

ويمكن التعبير عن فكرة التعديل (التضمين) كما يقول المؤلفان من خلال المثال التالي : « إذا كان لدينا رسالة مكتوبة على ورقة يطلب نقلها من نقطتين متباعدتين . فان رمي ورقة الرسالة من نقطة المصدر باتجاه المقصد سوف يؤدي إلى نقل الرسالة مسافة قصيرة تسقط بعدها الرسالة على الأرض ، ولكن لو أمكن ربط هذه الورقة بحجر ثم جرى رمي الحجر من نقطة المصدر فانه يمكن قطع مسافة أطول ، وبذلك يمكن تأمين الاتصال بين هاتين النقطتين . تمثل الورقة المكتوبة في هذا المثال المعلومات المطلوب ارسالها ويمثل الحجر الموجة الحاملة ، وتمثل العملية فكرة التضمين » .

ومن فوائد عملية التعديل (التضمين) مايلي :

١ ـ يؤدي إلى تسهيل عملية البث بتحميل موجة المعلومات على موجة عالية التردد .

٢ ـ يساعد على توزيع وتحديد الأقنية المستخدمة .

٣ ـ يساهم في تنفيذ فكرة تعدد الارسال ضمن قناة واحدة .

٤ ـ يساهم في تقليل التشويش .

ويعد تعديل ارتفاع الموجة (تضمين المطال) أول أنواع تعديل الموجات تهيئة لارسالها عبر مسافات بعيدة ، وهو أكثر الأنواع استخداماً في مجال الارسال الاذاعي وكذلك ارسال موجة الصورة في الارسال التلفزيوني .

ويحتوي الفصل الثالث على شرح لنظرية تعديل ارتفاع الموجه وعرض لنطاق الترددات وتوزيع القدرة على مدى تلك الترددات ، كما يشمل أيضاً دراسة للأنواع الخاصة من هذا التعديل كتعديل النطاق المزدوج المخمد الحامل ، وتعديل النطاق الوحيد ، وتعديل النطاق الوحيد مع الحامل ، ويقدم الفصل أيضاً دراسة لأساليب ازالة أو كشف تعديل ارتفاع الموجة واسلوب استخدام الموجة الحاملة ، وأخيراً يوضح الفصل طريقة ارسال عدد من الموجات عبر قناة مشتركة باستخدام تعدد تقسيمات نطاق التردد .

وفي الفصل الرابع ، يقدم الكتاب شرحاً وافياً لتعديل التردد والمستخدم بشكل رئيس في المحطات الاذاعية التي تعمل ضمن المجال مابين ٨٨ إلى ١٠٨ ميجاهيرتز كما يستخدم أيضاً في ارسال الصوت من محطات البث التلفزيوني ، ويحتوي هذا الفصل على عرض لنظرية تعديل التردد وتحليل لعرض نطاق التردد المعدل وكذلك دراسة توزيع القدرة في نطاق التردد ثم شرح نظرية تعديل الطور phase ووصف طرق توليد تعديل التردد والحاجة إلى مضاعفة التردد ثم بيان مبدأ كشف تعديل التردد والمكونات الأساس لأجهزة ارسال واستقبال تعديل التردد ، ويقدم الفصل أيضاً دراسة لاستخدام الصوت المجسم في تعديل التردد .

وبسبب الاعتماد المتزايد على الاتصالات الرقمية تلاقي عملية تعديل النبضات pulse modulation اهتماماً متزايداً ، ولقد أفرد المؤلفان الفصل الخامس والأخير من الكتاب لدراسة تعديل النبضات والتي تبدأ بتقديم نظرية العينات وشرح مفهوم تعدد تقسيم الزمن يلي ذلك استعراض لأنواع تعديل النبضات التمثيلي كتعديل ارتفاع النبضات وتعديل فترة النبضات وتعديل مركز النبضات ثم يقدم الفصل أيضاً دراسة لتعديل النبضات الرقمية كتعديل رمز النبضات وتعديل دلتا ، ويختتم الفصل بالتعريف بالارسال الرقمي وأنواعه المختلفة .

وأخيراً فان الكتاب متخصص في موضوعه يقدم المعلومات الأساس لهندسة الاتصالات بسهولة وتتابع ، وهو كما جاء في مقدمته يصلح للطلبة الجامعيين الذين يبدأون بدراسة مقرر الاتصالات لأول مرة ، ويتطلب الكتاب من هؤلاء الطلبة معرفة بأسس علوم مختلفة تشمل الرياضيات والفيزياء والدوائر الكهربائية والألكترونية ، وهو مفيد جداً لسائر العاملين في مجال الاتصالات ، بل المهندسين والفنيين .

ولقد اشتمل الكتاب على أمثلة عديدة في كل فصل إلى جانب الاسئلة والتمارين الملحقة بكل فصل والتي أشار المؤلفان إلى وجود حلول لها في كتيب خاص ، والكتاب بوجه عام ذو طابع أكاديمي نظري خال من التطبيقات العملية ، ملائم جداً لما وضع له ككتاب منهجي ، يقدم الأسس النظرية لهندسة الاتصالات ، ولقد أحسن المؤلفان صنعاً بارداف المصطلحات العلمية المترجمة بأصلها الانجليزي عند كل استخدام لها ، كما الحقا الكتاب بمعجم لهذه المصطلحات ، ولعل عدم اختيارهما للمصطلح المناسب يعود كما ذكرا لغياب الترجمة العربية الموحدة ولا ينقص هذا من قيمة الكتاب العلمية والمعنوية ، بل هو كما ذكرت سابقاً خطوة لتوطين العلوم الهندسية والتقنية ودين للأجيال العربية الصاعدة المتشوقة إلى التعلم والمتطلعة إلى التفوق والمتفائلة بالمستقبل .