Departament d'Informatica
Unitat de Combinatòria
i de Comunicació Digital

Edifici C
08193 Bellaterra (Barcelona), Spain
Tel.: (3) 581 14 70
Fax: (3) 581 24 78
E-mail: IINF1@CC.UAB.ES

Universitat Autonoma de Barcelona

Teoria Matemàtica de la Informació
Codificació Algebraica i Seguretat Computacional*

*Curs 1992-1993

Capítol 1

Objectius

La assignatura de "*Teoria Matemàtica de la Informació*" no és una assignatura terminal que pretengui formar professionals informàtics especialitzats en alguna branca de les que hi ha demanda social. La assignatura és bàsica i fonamental per a la formació matemàtica d'un llicenciat o enginyer superior en informàtica, tot i que en ella també desenvolupem aplicacions molt especialitzades, tant en la correcció d'errors com en la seguretat computacional. Des d'aquest punt de vista els objectius terminals de l'assignatura són d'adquisició de coneixements matemàtics i desenvolupament de les eines de càlcul necessaries per a la descodificació amb correcció/detecció d'errors/esborralls i per l'implementació de mètodes i protocols criptogràfics en la transmissió de la informació.

Els objectius de fets i procediments que pretenem que l'alumne assoleixi són:

1. Calcular polinomis irreductibles i/o primitius que permetin construir cossos finits més complexes a partir del cos on pertanyen els coeficients dels mateixos.

2. Construir cossos finits i entendre, en cada cas, quins són els elements amb els que estem treballant.

3. Treballar totes les operacions d'un cos finit, tant vectorialment com exponencialment a partir d'un element primitiu. Resoldre equacions i/o sistemes.

4. Saber descodificar un codi lineal senzill a partir de la taula estandard i via síndrome.

5. Saber utilitzar la matriu generadora i de control d'un codi lineal i el polinomi generador d'un codi cíclic.

6. Saber calcular la probabilitat d'error en la correcció d'errors i en la detecció d'errors.

7. Coneixer les fites de correcció d'errors i/o esborralls d'un codi.

8. Saber codificar i descodificar els codis *Reed-Solomon*, *BCH*, etc. i, en general, qualsevol codi algebraic, tant si es tracta de detectar errors o ràfegues d'errors, com corregir-los, com corregir esborralls.

9. Coneixer i saber usar les tècniques de concatenació i d'*interleaving*.

10. Usar l'algorisme de les fraccions continues en qualsevol de les seves aplicacions: càlcul del *m.c.d.*, càlcul de l'invers en un cos finit, sintetitzar *L.F.S.R.*, descodificació de codis algebraics, descodificació numèrica, filtres lineals i funcions de transferència, problemes d'interpolació racional, etc.

11. Esquematitzar un sistema criptogràfic, reconeixent-ne la seva seguretat, autenticitat, etc., d'acord amb els teoremes de Shannon i Simmons.

12. Utilitzar els sistemes criptogràfics clàssics més coneguts.

13. Compendre el funcionament general dels sistemes de clau privada, especialment el *DES* i el *PES*.

14. Coneixer els fonaments matemàtics de les funció unidireccionals amb trampa usades a la Criptologia.

15. Utilitzar els criptosistemes *RSA*, *Knapsack*, *ElGamal* amb paràmetres petits.

16. Diferenciar *Protocols Criptogràfics* de *Sistemes Criptogràfics*.

17. Coneixer els protocols criptogràfics més usuals com el de Diffie-Hellman i alguna prova sense transferència de coneixament.

Capítol 2

Programa de l'assignatura

Teoría Matemàtica de la Informació

Codificació Algebraica i Sistemes Criptogràfics

I: Aritmètica i Cossos finits.

1. Funció de Moebius. Fórmula d'inversió de Moebius. Indicador d'Euler.
2. Anells euclidians.
3. Algorisme d'Euclides. Factorització
4. Aritmètica modular.
5. Cossos finits. Característica.
6. Teorema d'existència d'elements primitius.
7. Càlcul vectorial i exponencial.
8. Teorema d'existència de polinomis irreductibles.
9. Càlcul dels polinomis irreductibles.
10. Teorema d'existència i unicitat de cossos finits.

11. L'estructura vectorial d'un cos finit. Diferents tipus de bases: estandard, traça-ortogonals, auto-traça-ortogonals.

12. Electrònica i càlculs en un cos finit.

13. Arquitectura clàsica: Divisor i multiplicador de Berlekamp.

14. Arquitectura sistòlica: Divisor i multiplicador.

II: Codificació. Conceptes básics

15. Introducció a la codificació

16. Parámetres d'un codi bloc

17. Codis lineals. Introducció

18. Codi ortogonal d'un codi lineal

19. Nous codis a partir de codigos

20. Codis lineals sistemàtics

21. Descodificació. Conceptes básics

22. Descodificació d'un codi lineal vía síndrome

23. Codis de Hamming

24. Introducció als codis BCH

25. Descodificación per lògica majoritaria

26. Codis convolucionals

27. Descodificación d'un codi convolucional

28. Enumerador de pesos d'un codi

29. Codigos Regulares

30. Fites sobre els paràmetres d'un codi

III: Codificació algebraica i la seva implementació electrònica. Aplicacions

31. Introducció als codis cíclics
32. Codificació de codis cíclics
33. Codis alternants i equació clau
34. Codis BCH, RS, de Goppa
35. Fraccions continues. Teorema de Dirichlet
36. Correcció d'errors i/o esborralls
37. Sistemes de comunicació
38. Criteris d'avaluació de un sistema
39. Algorítmica de protecció
40. Alguns sistemes de comunicació
41. Codificació numèrica
42. Altres aplicacions
43. Registres amb retroalimentació lineal
44. Filtres lineals discrets

IV: Secret i Autenticitat

45. Sistema Criptogràfic
46. Teoria del Secret Perfecte de Shannon
47. Teoría de la Autenticitat Perfecta de Simmons

48. Diseuy de Criptosistemes

V: Criptosistemes de clau secreta

49. Criptosistemes basats en transposicions
50. Criptosistemas basats en substitucions
51. Altres criptosistemes
52. El criptosistema DES
53. El criptosistema PES

VI: Criptosistemes de clau pública

54. Complexitat computacional
55. Funcions unidireccionals
56. El problema del càlcul dels logaritmes discrets. Criptosistemes basats en logaritmes discrets.
57. Funcions unidireccionals amb trampa. Criptosistemes RSA y ElGamal
58. Criptosistemes basats en problemes NP
59. El Knapsack.
60. Criptosistemes basats en codis alternants.
61. Criptografia probabilística.
62. Criptografia quàntica.
63. El problema de la autentificació

VII: Protocols Criptogràfics. Seguretat Computacional

64. Seguretat en xarxes d'ordinadors

65. Administració de claus i secrets. Esquemes de llindar.

66. El sistema d'intercanvi de claus de Diffie-Hellman.

67. Autentificació de documents.

68. Firmas digitals.

69. Mecanismes de crèdit.

70. Smart Cards.

71. Proves sense transferència de coneixaments. Zero Knowledge Proof.

72. Seguretat en bases de dades i sistemes operatius

Bibliografia

[1] Brassard G.: "*Modern Criptology*", LNCS, n.325, Springer-Verlag. (1988).

[2] Clark, G.C. & Bibb, J.: "*Error correcting code for Digital Communications*". Plenum Press. (1986).

[3] Feller, W.: "*Introducción a la Teoria de Probabilidades y sus aplicaciones*". Limusa. Mexico. (1975).

[4] Goppa, V.D.: "*Geometry and codes*", Kluwer Academic Publishers. (1988).

[5] Hardy, G.H. & Wright, E.M.: "*An Introduction to the Theory of Numbers*". Oxford Science Publications, Clarendon Press. Oxford. (1989).

[6] Hill, R.: "*A First Course in Coding Theory*". Clarendon Press. Oxford. (1986).

[7] McEliece, R.J.: "*The Theory of Information and Coding*". Addison-Wesley Publishing Company. (1977).

[8] McEliece, R.J.: "*Finite fields for computer scientists and engineers*", Kluwer Academic Publishers. (1987).

[9] Mc.Williams-Sloane: "*The Theory of error-correcting codes*", North-Holland Publishing Company. Amsterdam-N.Y.-Oxford. (1978).

[10] Poli, A. & Huguet, L.: "*Codes correcteurs*", Masson. Paris (1988).

[11] Rifà, J. & Huguet, L.: "*Comunicación Digital*". Masson Ed. (1991).

[12] Robling Denning D.E.: "*Cryptography and Data Security*". Addison-Wesley Publishing Ccompany. (1988).

[13] Simmons, G.S.: "*Contemporary Criptology. The Science of Information Integrity*", IEEE Press. (1991).

[14] Shu Lin, and Costello,D.: "*Error Control Coding: Fundamentals and Aplications*", Prentice-Hall, Inc.Englewood Cliffs, N.J. 07632. USA. (1987).