UNIVERSIDAD DE
MURCIA

FACULTY OF
MATHEMATICS

Theory of Error Correcting Codes and Cryptography

Course code:	1601
Number of ECTS credits:	6
Semester:	1st (September-January)
Prerequisites:	60% of basic courses and 60% of obligatory courses.
Recommended components:	Linear Algebra (1569), Sets and Numbers (1570), Groups and Rings (1585) and Galois Theory
Language of instruction:	Spanish (students are allowed to ask questions and write homeworks and exams in English)

Course description

The purpose of this course is to introduce the basic theory, and fundamental results and tools of the Theory of Error Correcting Codes and Cryptography with two underlying objectives:

1. Facilitate the employment of mathematicians in the field of information and telecommunications.

2. Get the threshold of research in a field of great activity.

Learning outcomes and competences

After completion of this course you will:

1. know the problems relative to data transmission.

2. learn models for those problems and fundamental mathematic tools for their study.

3. know algebraic, number theoretic and computational methods to solve problems related with this topic.

4. know some fundamental families of codes and their algebraic frame.

5. know the basic cryptographic methods.

6. know some cryptoanalysis techniques and some complexity problems associated.

Course contents

I. Error Correcting Codes

1. Basics
2. Linear codes
3. Polynomials over finite fields.
4. Cyclic codes.

II. Cryptography

1. Cryptosystems, cryptology and cryptoanalysis. Pubic and private keys.
2. Factorization and primality methods.
3. Introduction to cryptography based on elliptic curves.

References

1. C. Munuera y J. Tena, Codificación de la información, U. de Valladolid, 1997.

2. Jorn Justensen and Tom Hoholdt, A course in Error-Correcting codes.

3. W. C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, Cambridge UP 2003.

4. O. Pretzel, Codes and Finite Fields, Clarendon, 1992.

5. S. Roman, Introduction to Coding and Information Theory, Springer, 1996.

6. Samuel S. Wagstaff Jr, Cryptanalysis of Number Theoretic Ciphers, Chapman and Hall, 2002.

7. Neal Koblitz, A course in Number Theory and Cryptography, Springer Graduate Texts in Mathematics, 1994 A Course in Number Theory and Cryptography (Graduate Texts in Mathematics).