Mario J. Perez Jimenez, Full Professor at the Department of Computer Science and Artificial Intelligence at Universidad de Sevilla, Spain, since 2009, and currently Emeritus Professor. From 2005 to 2007 he was a Guest Professor of the Huazhong University of Science and Technology, Wuhan, China. He is a numerary member of the Academia Europaea (The Academy of Europe) in the Section of Informatics. His main research interests include theory of computation, computational complexity theory, natural computing (DNA computing and membrane computing), bioinformatics and computational modelling for complex systems. He has published 19 books in computer science and mathematics, and over 300 scientific papers in international journals (collaborating with researchers worldwide) and he is a member of the Editorial Board of six ISI journals. He has been the first scientist awarded with "Important Contributions to Membrane Computing" under the auspices of the European Molecular Computing Consortium, Edinburgh, 2008. In 2014, he received the University of Sevilla's FAMA award for his outstanding research career. He has been the main researcher in various European, Asian, Spanish and Andalusian research grants. From 2003 he is an expert reviewer of the Prospective and Evaluation National Agency of Spain. From May 2006 he is an European Science Foundation peer reviewer, from July 2008 he is an expert reviewer from the Romanian National University Research Council and from October 2015 he is an international expert from the Russian Science Foundation, invited by the Russian International Affairs Council.

Talk: Membrane systems breaking cryptosystems

Abstract: Cryptography is a scientific discipline that concerns information security in presence of possible intruders, as well as authentication and identification, providing privacy and integrity. The first ever published public key cryptosystem, named RSA, was developed by R. Rivest, A. Shamir and L. Adleman in 1978. The security that resides in this system is based on the apparent computational hardness of the integer factorization problem. More precisely, the semiprime factorization problem (given a natural number product of two prime numbers, find its decomposition) is used.

In this talk, the cited problem, among others, is studied from the Membrane Computing perspective, and a new kind of membrane systems with the ability to compute partial functions among natural numbers, are presented. This provides a new approach to attack RSA cryptosystems.