" Cryptogtraphy using Chaos"

The quest for inventing innovative techniques which allow only authorized users to transfer information that is impervious to attack by others has, and continues to be, an essential requirement in the communications industry. This requirement is based on the importance of keeping certain information secure, obvious examples being military communications and financial transactions, the former example being a common theme in the history and development of cryptology. The use of chaos in cryptography was first considered in the early 1950s by the American mathematician and electrical engineer Claude Shannon who laid the theoretical foundations for modern information theory and cryptography. It was Shannon who first explicitly mentioned the basic stretch-and-fold mechanism associated with chaos for the purpose of encryption in which complex data transformations can be formed by repeated products of two simple non-commuting operations. However, the value of chaos for encrypting data was not fully appreciated until the late 1980s when the simulation of chaotic dynamical systems became common place and when the role of cryptography in IT became increasingly important. Since the start of the 1990s, an increasing number of publications have considered the use of chaos in cryptography. These have included schemes based on synchronized chaotic (analogue) circuits and secure radio communication. Over the 1990s cryptography started to attract a variety of engineers from diverse fields who began exploiting dynamical systems theory for the purpose of encryption. This included the use of discrete chaotic systems such as the cellular automata, Kolmogorov flows and discrete affine transformations in general to provide more efficient encryption schemes. Since 2000, the potential of chaos-based secure communications, especially with regard to spread spectrum modulation, has been recognized. However, the emphasis has been on information coding and it is only relatively recently that the application of chaos-based ciphers have been implemented in software and introduced to the market. One example product of this is *Crypstic* in which the principle of multi-algorithmicity using chaos-based ciphers is use to produce meta-encryption engines mounted on pairs of USB flash memory sticks. This lecture discusses the background to cryptography using chaos and explores the rationale, architecture and development of *Crypstic.*

Lecture co-financed by the European Union in scope of the European Social Fund

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

EUROPEAN UNION
EUROPEAN
SOCIAL FUND