



MINISTERIO
DE CIENCIA
Y TECNOLOGÍA

SECRETARÍA DE ESTADO
DE POLÍTICA CIENTÍFICA
Y TECNOLÓGICA

DIRECCIÓN GENERAL
DE INVESTIGACIÓN

SUBDIRECCIÓN GENERAL DE
PROYECTOS DE INVESTIGACIÓN

JORNADAS DE SEGUIMIENTO

PROYECTOS EN TECNOLOGÍAS DE LA INFORMACIÓN

DESCRIPCIÓN DE RESULTADOS

Referencia del proyecto: TEL1998-1020

Título: Infraestructuras de Seguridad en Internet e Intranet. Aplicación a Redes Públicas y Corporativas

Investigador principal: Fausto Montoya Vitini

**Dirección de contacto: Serrano nº144,
28006 Madrid**

Datos sobre el grupo investigador:

**Departamento de de la Información
Instituto de Física Aplicada, CSIC.**

¿Se trata de un proyecto coordinado?: NO

1. PROJECT OBJECTIVES

The aim of this project is to develop a High Security modular infrastructure (keys as long as desired) for Internet-like networks, both for public use (Internet itself) and for private use within a corporate network (Intranet).

High Security cryptographic protocols and cryptosystems will be used, without key length limitation. The design will be modular, so that secret key and public key commercial cryptosystems will be of use along with the cryptosystems designed in the project.

The system would be compatible and interoperable with low security structures of 40 and 56 bits legally exportable out of USA and available in the Spanish market.

Two different levels of implantation are scheduled: Electronic Mail application level security, for its public use in Internet by the Administration. It will provide Confidentiality, Authentication, Integrity, Non-repudiation, and Key Certification services. IP layer security, for its use by private corporate networks (secure virtual private network). It comprises all Internet applications (FTP, Telnet, E-mail, WWW, IRC, etc.) and provides Confidentiality, Authentication, and Key Certification services.

The work plan is divided in seven modules:

- 1.1 Design of a high security infrastructure for Internet.
- 1.2 IP Layer virtual private network.
- 1.3 Design of a secret-key cryptosystems based on unidimensional cellular automata.
- 1.4 Design of keystream generators using chaotic regions of non linear dynamical systems.
- 1.5 Implementation of the BBS public key cryptosystem.
- 1.6 Design of a elliptic curves public key cryptosystem.
- 1.7 Contribution to secure communications by means of digital chaotic codification.

2. LEVEL OF SUCCESS

2.1 Design of a high security infrastructure for Internet.

This module has been finished successfully and transferred to the EPO CTI-CSIC.

2.2 IP Layer Virtual Private Network.

The aim of this module was to overcome the export-import restrictions imposed by US and Canada governments on high security cryptosystems, with key-lengths of more than 40 / 56 bits. Our intention was to develop a Virtual Private Network (VPN) over Internet, using high security protocols over TCP/IP. Unfortunately in the mid's 2000 US government raised the mentioned restrictions. Now VPN, with high level security cryptography, is incorporated as a standard feature in today commercial operating systems. Hence our initial intention was of little value, for evident reasons. Our work has been reduced to mounting and evaluating an experimental network that implements a high security VPN, working under Windows2000.

2.3 Design of a secret-key cryptosystems based on unidimensional cellular automata.

Although several authors have forecasted good prospects for the use of CA in Cryptography, our experience points towards the opposite direction. After a detailed study of running-key generators based on Cellular Automata (CA), a clear conclusion was reached: our assumption of its usefulness, based on wide spread opinions, proved to be excessively optimistic and the truth is that they present a suboptimal behaviour for cryptographic purposes.

Due to the non-satisfactory results obtained from the CA, we focussed our attention on another more conventional class of running-key generators such as the *non-linear filters* applied to LFSRs. As is dealt with in the paragraph 4.3 of the detailed research results report, sections 1 and 2. Later and due to the arrival of Professor Slobodan Petrovic from the Institute of Applied Mathematics of the University of Belgrade (Yugoslavia), our efforts were mainly concentrated on the field of Cryptanalysis as it can be seen in sections 3 and 4 of this report.

2.4 Keystream generators using chaotic regions of non linear dynamical systems.

This module has been finished successfully.

2.5 Implementation of the BBS public key cryptosystem.

This module has been finished successfully.

2.6 Design of an elliptic curves public key cryptosystem.

This module has been finished successfully.

2.7 Contribution to secure communications by means of digital chaotic codification.

In recent years, chaotic communications systems, have attracted the attention of researchers from all around the world. As a result, a rich variety of chaotic cryptosystems for end to end communications have appeared. Taking in to account these tendencies, our intention was to develop a high security cryptographic chaotic system.

We have found that, the vast majority of these chaotic encryption systems relies on the unproven assumption that chaos lacks of order or structure. We have proven that chaos is highly predictable, thus insecure.

So we have rather preferred to cryptanalyze most of the chaotic cryptosystems described in the literature instead of designing a new one. Nevertheless we have provided some guidelines on how to design more secure chaotic encryption algorithms.

3. RESULTS

3.1 Design of a high security infrastructure for Internet.

The first and main achievement of the Module 1 has been the design, development and implementation of a **Public Key Infrastructure (PKI)** for the CSIC, as described in the paragraph 4.1 of the detailed report of research results.

This PKI has been transferred to the Centro Técnico de Informática of the CSIC, (EPO of this project) and responsible of the CSIC-PKI management. The CSIC-PKI will be started at the beginning of year 2002.

It allows to issue different classes of digital certificates for the staff, the servers and the certification authorities (CA) belonging to the CSIC. It is included in the certification authority pilot headed by RedIris.

Several schemes for CSIC-PKI were designed and evaluated but the present one was selected due to its adaptation to the complex structure of the CSIC. It is a modular and easily extensible to the geographical and administrative distribution of the CSIC. The information of the CSIC-PKI can be found in <http://acer.csic.es> and <http://www.cti.csic.es/OIDs>

The second achievement has been the development of a CryptoASP to add cryptographic strength to any web page based application, compatible with ActiveX. It allows to encrypt, decrypt, hash and generate pseudo random numbers. It works with any high security stream cipher algorithm of any key-length.

Publications: [ALV99], [ALV99a], [ALV99b], [ALV00], [ALV00a], [ALV00b], [ALV01], [ALV01a], [GUI00], [GUI01], [PEI99], [PEI99a], [ALV99e], [ALV00j], [ALV00k], [ALV00l], [ALV00m], [ALV00n], [ALV01j].

3.2 IP Layer virtual private network.

The work has consisted in mounting a laboratory equipped with hardware and software firewalls and several computers, simulating two private networks connected through a public network. We have established a high security VPN, working under Windows2000. We have tested the security simulating different kinds of attacks. It is implemented using Windows 2000, in few days will be migrated to Windows XP

Publications: [AC01], [ALV99c], [ALV00c], [ALV00o], [ALV00d], [ALV00e], [ALV00f], [AMO01], [MP01], [PEI00], [ALV00g], [ALV00h], [ALV01b], [ALV01c], [ALV01d], [ALV00i], [ALV99d]

3.3 Design of a secret-key cryptosystems based on unidimensional cellular automata.

As described in the detailed report of research results, paragraph 4.3, due to the non-satisfactory results obtained from the CA, we focussed our attention on other more conventional class of running-key generators such as the *non-linear filters* applied to LFSRs. This is the subject of sections 1 and 2 in this report, with the reasons given above (2.3). Later and due to the arrival of Professor Slobodan Petrovic from the Institute of Applied Mathematics of the University of Belgrade (Yugoslavia), our efforts were mainly concentrated on the field of Cryptanalysis as it can be seen in sections 3 and 4 of this report.

Publications: [G-VF99], [G-VF99a], [GP01], [FC00], [G-VF00], [PF00], [FG-V01], [FUS02], [FG-V00a], [G-VF99d], [G-VF99b], [G-VF99c], [FG-V99], [FC99], [FUS99], [G-MF00], [G-MFG01], [FG-M01], [PF02], [PFD01], [GP99], [PET00].

PhD. Thesis: Cotas de complejidad lineal para criptosistemas seguros en comunicaciones de banda ancha.

3.4 Keystream generators using chaotic regions of non linear dynamical systems.

We proposed to study the Misiurewicz points in order to use them as keystream generators of in stream cipher encryption. To study these Misiurewicz points we have used the real Mandelbrot map $x \rightarrow x^2 + c$, that is defined for the parameter values $-2 \leq c \leq 1/4$. In this segment of the real axis there are several types of points depending on the value of the multiplier, $\lambda = (d(f_c(x))/dx)_{x=x_i}$. If $\lambda = 1$, we have the non-hyperbolic points, and if $\lambda \neq 1$, we have the hyperbolic points.

The connected set of the c -values for which $f_c^k(0)$ converges to a k -cycle is a periodic *component* or *hyperbolic component*. These periodic hyperbolic components verifies $\lambda < 1$ which means they are stable. But there are points, the Misiurewicz points where $\lambda > 1$ which means they are instable. *Misiurewicz points*, owing to their being unstable, have a chaotic behaviour. Even though mathematically they have a preperiod and a period, after the orbit has run the preperiod and has eventually been caught up in the period, it finally falls into chaos. That is why the study of the Misiurewicz points, and to a less extent the study of the hyperbolic components, was the more important aim of our work.

Thus, we studied the patterns of the symbolic sequences of both Misiurewicz and superstable periodic points, and showed that a Misiurewicz point pattern can be obtained as the limit of the sum of a superstable periodic orbit pattern plus itself or some of its heredity transmitters repeated an infinite number of times. This work, "Misiurewicz point patterns generation in one-dimensional quadratic maps", was published in Physica A [PRAM01]. Likewise, we studied in a general way the preperiods and periods of the Misiurewicz points and the periods of the superstable periodic points, in the Mandelbrot set, and the results, "Shrubs in Mandelbrot set ordering", have been sent for publication to Physica D [PRAM01b]. We carried out a similar study in other two types of maps, "Growth in complex exponential maps" and "Snail-like pattern generation with the Hénon family of maps" both published in Computer & Graphics, [RPAM00, RBPAM00].

The external argument theory of Douady and Hubbard allows us to know both the potential and the field-lines outside the Mandelbrot set. Nonetheless, there are no explicit formulae to operate with external arguments, and the external argument theory is difficult to apply. We introduced some tools in order to obtain formulae to operate with external arguments in the Mandelbrot set antenna in "Operating with external arguments in the Mandelbrot set antenna", sent to Physica D [PRAM01a], and in "Argumentos externos del conjunto de Mandelbrot", published in "Revista Española de Física" [CRPAM01].

Publications: [CRPAM01], [RPAM00], [RBPAM00], [PRAM01], [PRAM01a], [PRAM01b].

3.5 Implementation of the BBS public key cryptosystem.

The basic properties of the Blum, Blum and Shub generator are well known. Because of its cryptographic security, the $x^2 \bmod n$ generator has been proposed for several applications; notably, pseudorandom bit generation, secret-key cryptography and public-key cryptography. In practical implementations however, two problems usually arise: first, to characterize moduli $n = p \cdot q$, producing orbits of maximal period, and second, to determine the seeds for which this maximal period is reached. In this work we found a sharp general upper bound for the period of any orbit, a characterization of the prime factors p , q reaching this bound for several classes of seeds, and the classification of the seeds providing orbits of maximal length. In fact, for any seed the exact length is obtained. The knowledge of the orbit lengths allows us to give an improvement of the public-key cryptosystem proposed by the authors and a digital signature protocol is developed.

The result is a practical efficient implementation of the BBS public key cryptosystem, that allows us to recover the original message without taking square roots.

Publications: [DHM00], [DMM99], [DMM99a], [HER99], [HM00], [HM00a], [MMP99], [MMP99a], [MP00], [PMM01], [PMMY01], [PEI00a], [PEI00b], [PMM99], [PM00], [QH01]

3.6 Study of a elliptic curves public key cryptosystem.

Our task in this project has been to study and to analyze the design of public key hyperelliptic cryptosystems, whose security is based on the discrete logarithm problem. To do this, we have studied the classification of hyperelliptic curves of genus 2 defined over finite fields of characteristic different from 2 and 5. The results that we have obtained, allow us to decide the number of isomorphism classes of such curves. This classification result states an important criterion to decide which hyperelliptic curves of genus 2 can be used in practical implementations, as this classification permits one to obtain the reduced equations explicitly.

A communication has been presented at The 5th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2001), organized by the "International Institute of Informatics and Systemics" (IIS). Moreover, a preliminary version of the results obtained can be seen in a Technical Report from the University of Waterloo, Canada (CORR 2001-26).

The research development has been carried out in collaboration with Professor Alfred Menezes from the Centre for Applied Cryptographic Research (CACR) in the University of Waterloo (Canada).

Publications: [HM01], [CM00], [CM99], [CM99a], [CM99b], [CMM99], [DM00], [FGM00], [GMM00], [GRM99], [MM00], [MP00], [MP99], [MS00], [MV99], [DGMM00], [MP00a], [RM99].

3.7 Contribution to secure communications by means of digital chaotic codification.

The growing cryptographic techniques demand has originated intense research activity and the search of new directions in cryptography. In recent years, chaotic communications systems, i.e., those making use on non-periodic chaotic carriers, have attracted the attention of researchers from all around the world, since they offer some important advantages over the traditional radio communications methods based on periodic carriers, as in mobile telephony or wireless LANs. As a result, a rich variety of chaotic cryptosystems for end to end communications have been put forward, whose robustness and privacy are equally diverse [AFG 99, AMP 99, AS 99,]. The vast majority of these chaotic encrypting systems have been developed by physicists, mathematicians and engineers lacking a sound cryptography background. Relying on the unproven assumption that chaos lacks order or structure, it is often naively assumed that simply because an encrypted chaotic sequence appears to be random it is actually secure.

Up to date, little or no critical analysis has been made about the security and cryptographic robustness of these algorithms [AMR 00a, AMR 00b, AMR 00c]. We have detected that a systematic approach to cryptanalysis and security evaluation is missing. To fill this void, in this project we have examined some of these algorithms from a cryptographic perspective. First, we have proposed some new analysis tools based on the theory of 1D quadratic maps, such as Gray codes [ARP 98a], an extension of the Myrberg method [ARP 98b] or the well known bifurcation diagrams. By means of these techniques, we have proved that the order underlying the apparent randomness in the proposed chaotic systems is enough to open vulnerabilities for attack.

Second, we have made use of these vulnerabilities to successfully attack the proposed cryptosystems. Depending of the cipher under study and its parameter configuration, some or all of the following attacks have proved to be successful, usually with a surprisingly low number of texts: ciphertext-only, known-plaintext, chosen plaintext, and chosen ciphertext.

Another question usually neglected in these chaotic cryptosystems, although of capital importance, is the key management procedure. In most cases no indication is given about how to choose suitable keys. Good keys are those giving rise to orbits of large period which visit the whole attractor under consideration, so that all possible subintervals are visited in a reasonable time. A bad choice of the key, related to the parameter of the map, translates into a poor security performance.

After our cryptanalysis, we conclude that most of the chaotic cryptosystems are very insecure and, thus, unreliable for secure applications. We also provide some guidelines on how to design good secure chaotic encryption algorithms [AMRP 00].

PhD. Thesis: *Contribución al estudio de la estructura interna del Conjunto de Mandelbrot y aplicaciones en Criptografía*

Publications: [AMRP 00], [ARP 98b], [AMR 00a], [AMR 00b], [AMR 00c], [AFG 99], [AMP 99], [AS 99].

3.8 Tools

We have developed a universal tool for testing the strength of any secret key cryptosystem. We call it CryptoBench that constitutes an integrated and flexible environment for the implementation and evaluation of cryptographic components by using an important battery of tests. Although there exists some other tools that can perform similar tests, such as CRYPT-X '98, by Queensland University of Technology, the strongest point of this program lies on its capability to define a programming interface for the fast development and further inclusion into the application of cipher algorithms and pseudo random number generators. In this way, CryptoBench provides an environment within development and evaluation tests of cryptographic components are fully integrated. [CA01]

3.9 Other related publications

[CHH01], [ALV00p], [ALV00q], [ALV01f], [ALV99f], [ALV99g], [HM99], [HER00], [HMM00], [PEI01], [GP01a], [CHH01a], [CHH00], [CHH00a], [CHP01], [RCHH99].

3.10 Summary of results

International publications: 32

National Publications: 42

Conference communications: 50

Books: 5

Web Pages: 1

Conference program committee member: 4

Conference chairman: 1

Lectures: 9

PhD. Theses: 3

Graduation Theses: 8

Courses: 10

Patents: 1

Industry Contracts: 4

Collaboration with international research groups: 9

Collaboration with national research groups: 1