Testimonio de medio siglo: de la Perlustración al Cifrado cuántico

Fausto Montoya Vitini

Instituto de Seguridad de la Información, Madrid
Consejo Superior de Investigaciones Científicas
fausto.montoya@iec.csic.es

XII Reunión Española sobre Criptología y Seguridad de la Información
Donostia-San Sebastián, 4-7 de Septiembre de 2012

La Criptografía es una ciencia muy especial

Hitos de la historia de la criptografía

Criptografía actual

Criptografía en España

Criptografía en el CSIC

Recetas

La criptografía es una ciencia muy especial

Tiene contados principios fundamentales, los básicos son:

- Principio de Kerckhoffs: La seguridad no debe depender del secreto, solo la clave es desconocida.

La criptografía es una ciencia muy especial

Tiene contados principios fundamentales, los básicos son:

- Principio de Kerckhoffs: La seguridad no debe depender del secreto, solo la clave es desconocida.
- El sistema de cifrado de Vernam es el único seguro matemáticamente.

La criptografía es una ciencia muy especial

Tiene contados principios fundamentales, los básicos son:

- Principio de Kerckhoffs: La seguridad no debe depender del secreto, solo la clave es desconocida.
- El sistema de cifrado de Vernam es el único seguro matemáticamente.
- Aportaciones básicas de Claude Shannon: cantidad de información, entropía, longitud mínima de clave y distancia de unicidad.

La criptografía es hija de la diosa Fortuna

La Fortuna gobierna mediante el AZAR, algo esencial en criptografia

La casi totalidad de los algoritmos y protocolos requieren números aleatorios:

La Fortuna gobierna mediante el AZAR, algo esencial en criptografia

La casi totalidad de los algoritmos y protocolos requieren números aleatorios:

- Algoritmos de cifrado: generación de claves simétricas y asimétricas; secuencias para cifrado en flujo.

La Fortuna gobierna mediante el AZAR, algo esencial en criptografia

La casi totalidad de los algoritmos y protocolos requieren números aleatorios:

- Algoritmos de cifrado: generación de claves simétricas y asimétricas; secuencias para cifrado en flujo.
- Firmas digitales: claves.

La Fortuna gobierna mediante el AZAR, algo esencial en criptografia

La casi totalidad de los algoritmos y protocolos requieren números aleatorios:

- Algoritmos de cifrado: generación de claves simétricas y asimétricas; secuencias para cifrado en flujo.
- Firmas digitales: claves.
- Protocolos criptográficos: contraseñas, números de un solo uso.

La Fortuna gobierna mediante el AZAR, algo esencial en criptografia

La casi totalidad de los algoritmos y protocolos requieren números aleatorios:

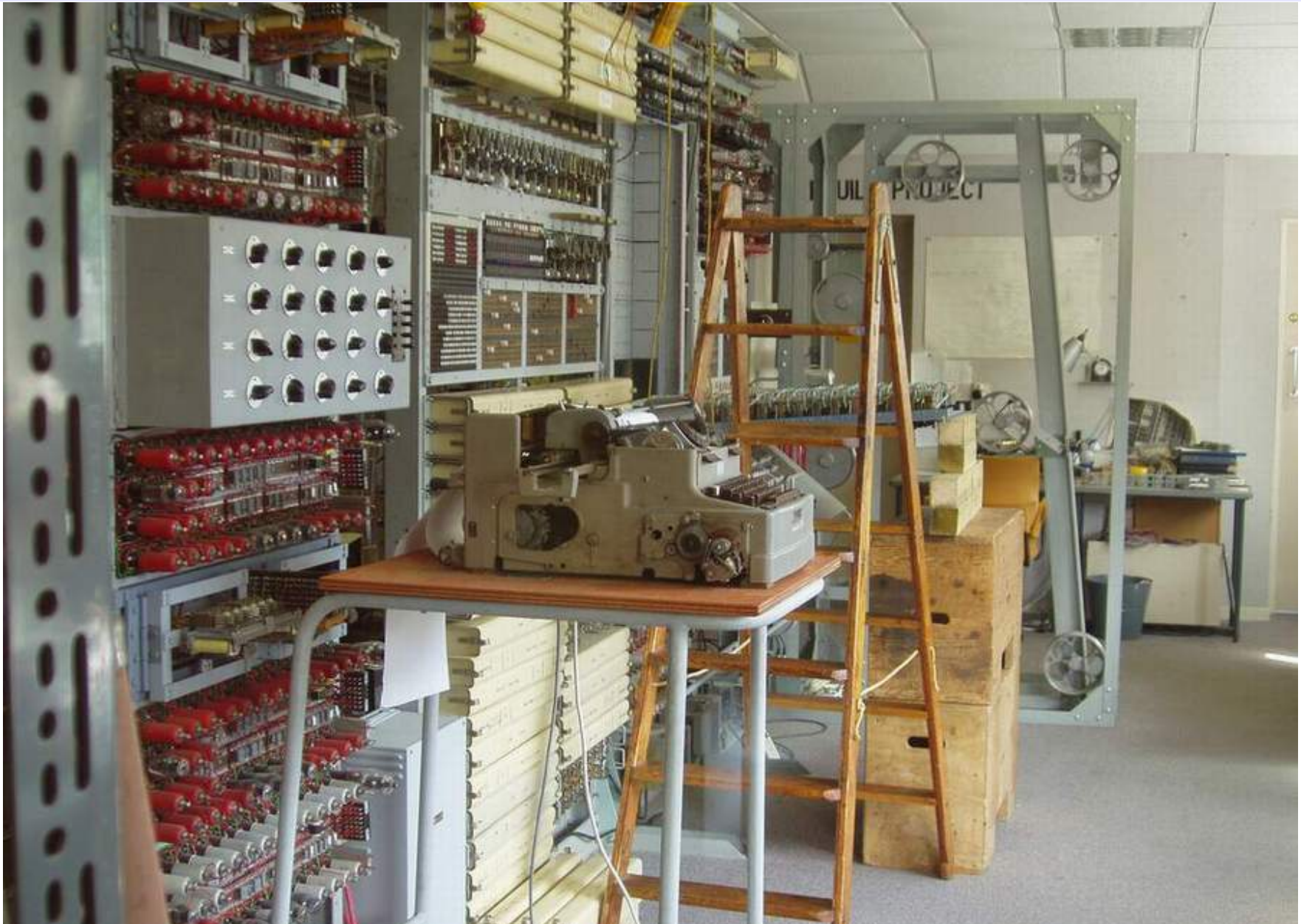
- Algoritmos de cifrado: generación de claves simétricas y asimétricas; secuencias para cifrado en flujo.
- Firmas digitales: claves.
- Protocolos criptográficos: contraseñas, números de un solo uso.

La seguridad de los esquemas criptográficos depende de la calidad de los generadores pseudoaleatorios (PRNG)

Y del dios Marte

La criptografía se parece al ajedrez: unos buscan ataques y otros encuentran defensas

Primer ordenador electrónico: Colossus (Bletchley Park, 1944). Criptoanálisis de la máquina Lorenz



Le aventajan en capacidad de cálculo los actuales smartphones

La criptografía es tan antigua como la escritura

Orígenes: Egipto, India, Mesopotamia, Persia, Esparta, Siam, Suecia...

Primer sistema matematico: Julio Cesar y Augusto.

Califato Abasida (750–1280), se inicia el criptoanálisis:

- al-Kindi (801–873): frecuencia de las letras y rotura cifrados de sustitución.

La criptografía es tan antigua como la escritura

Orígenes: Egipto, India, Mesopotamia, Persia, Esparta, Siam, Suecia...

Primer sistema matematico: Julio Cesar y Augusto.

Califato Abasida (750–1280), se inicia el criptoanálisis:

- al-Kindi (801–873): frecuencia de las letras y rotura cifrados de sustitución.

- ibn-Adlan (1187–1268) longitud mínima de un texto árabe para el criptoanálisis: 90 letras.

La criptografía es tan antigua como la escritura

Orígenes: Egipto, India, Mesopotamia, Persia, Esparta, Siam, Suecia...

Primer sistema matematico: Julio Cesar y Augusto.

Califato Abasida (750–1280), se inicia el criptoanálisis:

- al-Kindi (801–873): frecuencia de las letras y rotura cifrados de sustitución.
- ibn-Adlan (1187–1268) longitud mínima de un texto árabe para el criptoanálisis: 90 letras.
- ibn-al-Durayhim (1312–1361): análisis de 8 cifrados de sustitución, precursor de la tabla de Vigenere.

El Renacimiento despierta la criptografía en occidente

Florecimiento: Luchas entre Güelfos y Gibelinos; Cisma de Occidente.

Universalización en el siglo XVI, en todos los reinos cristianos.

- Leon Battista Alberti, *De Cifris*, 1466.

El Renacimiento despierta la criptografía en occidente

Florecimiento: Luchas entre Güelfos y Gibelinos; Cisma de Occidente.

Universalización en el siglo XVI, en todos los reinos cristianos.

- Leon Battista Alberti, *De Cifris*, 1466.
- Johannes Trithemius, *Poligraphia*, describe la *tabula recta*.

El Renacimiento despierta la criptografía en occidente

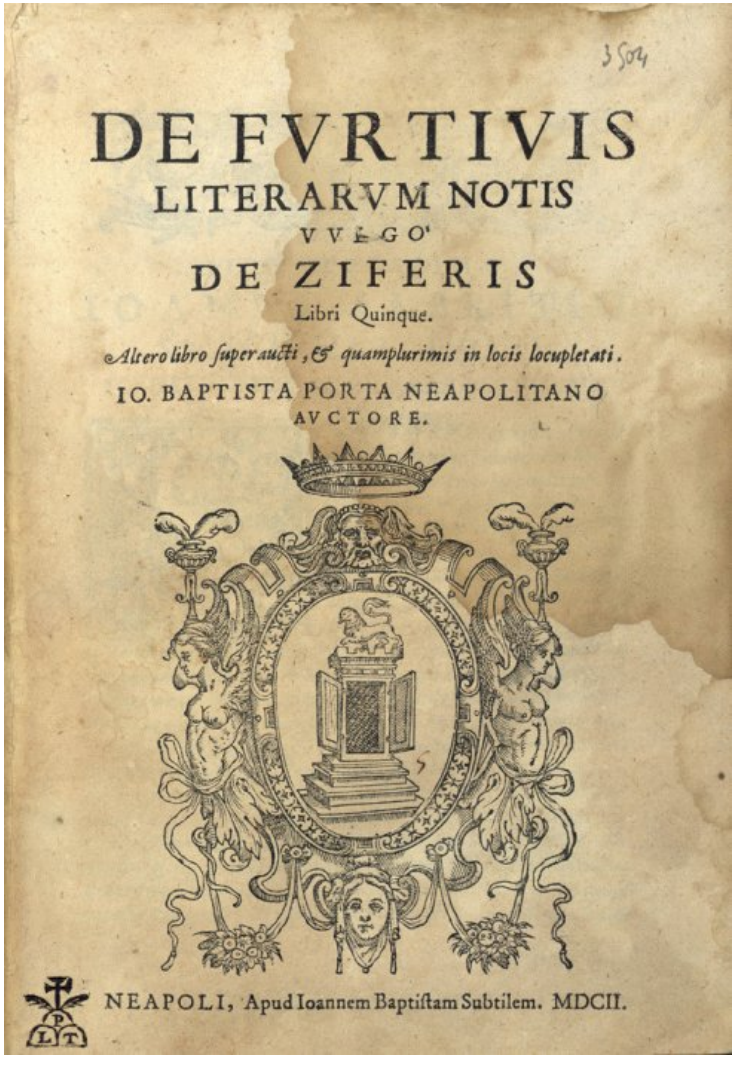
Florecimiento: Luchas entre Güelfos y Gibelinos; Cisma de Occidente.

Universalización en el siglo XVI, en todos los reinos cristianos.

- Leon Battista Alberti, *De Cifris*, 1466.
- Johannes Trithemius, *Poligraphia*, describe la *tabula recta*.
- Giovan Battista Belasso, *La cifra del Sig. Giovan Battista*, 1553 (cifrado de Vigenère).

Giambattista della Porta

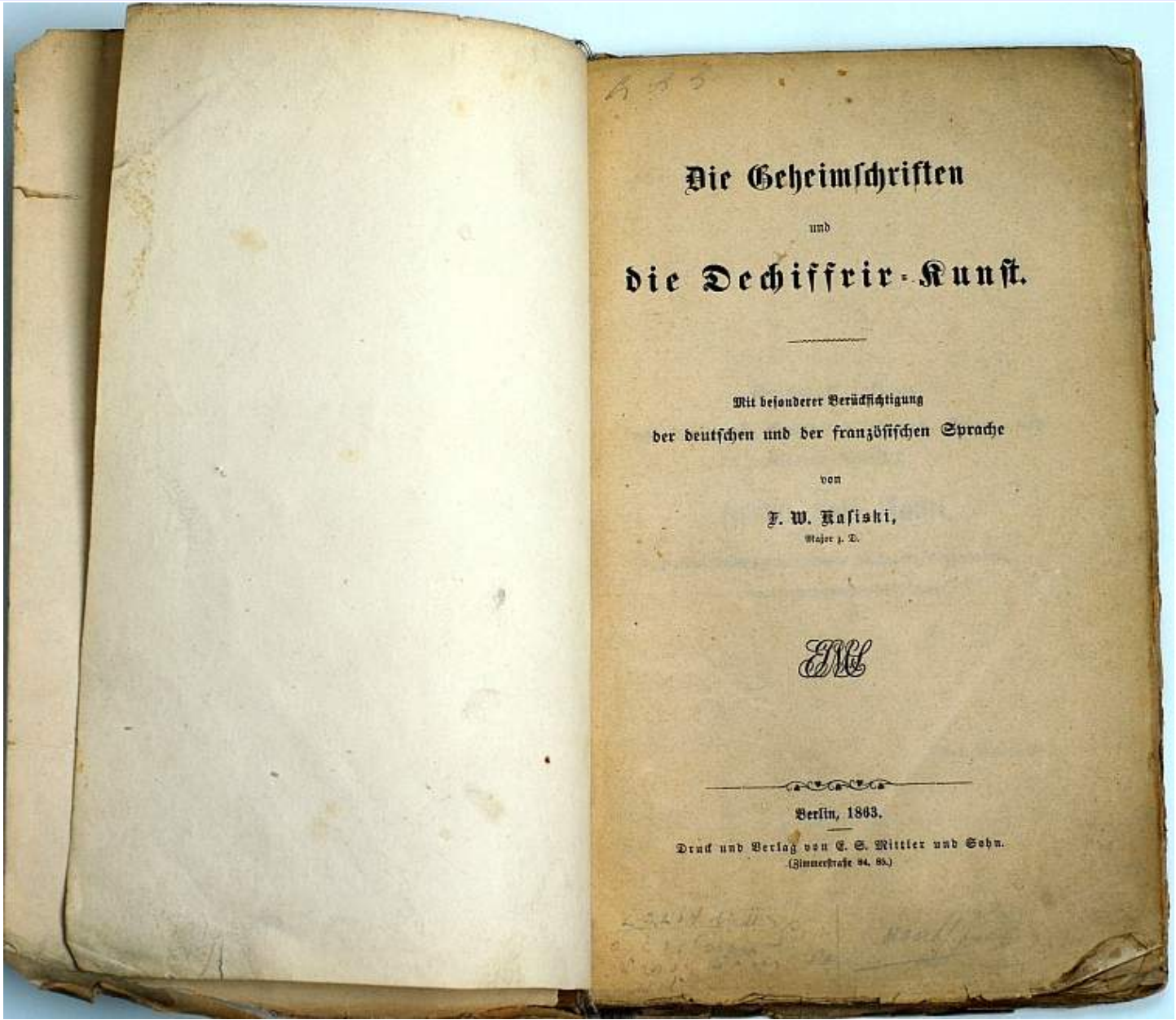
De Furtivis Literarum Notis, vulgo de Ziferis, 1602.
Analiza y clasifica los procedimientos de cifrado,
inicia las leyes del criptoanálisis, con características lingüísticas.



Por encargo de Francis Walsingham, Thomas Phelippes inventó un mensaje cifrado falso, que condujo al patíbulo a María Estuardo

Charles Babbage (1791–1871), rompe la cifra auto-clave de Vigenère

El mérito se lo llevó Friedrich Wilhelm Kasiski (1805–1881)



Die Geheimschriften

und

die Dechiffrir-Kunst.

Mit besonderer Berücksichtigung

der deutschen und der französischen Sprache

von

F. W. Kasiski,

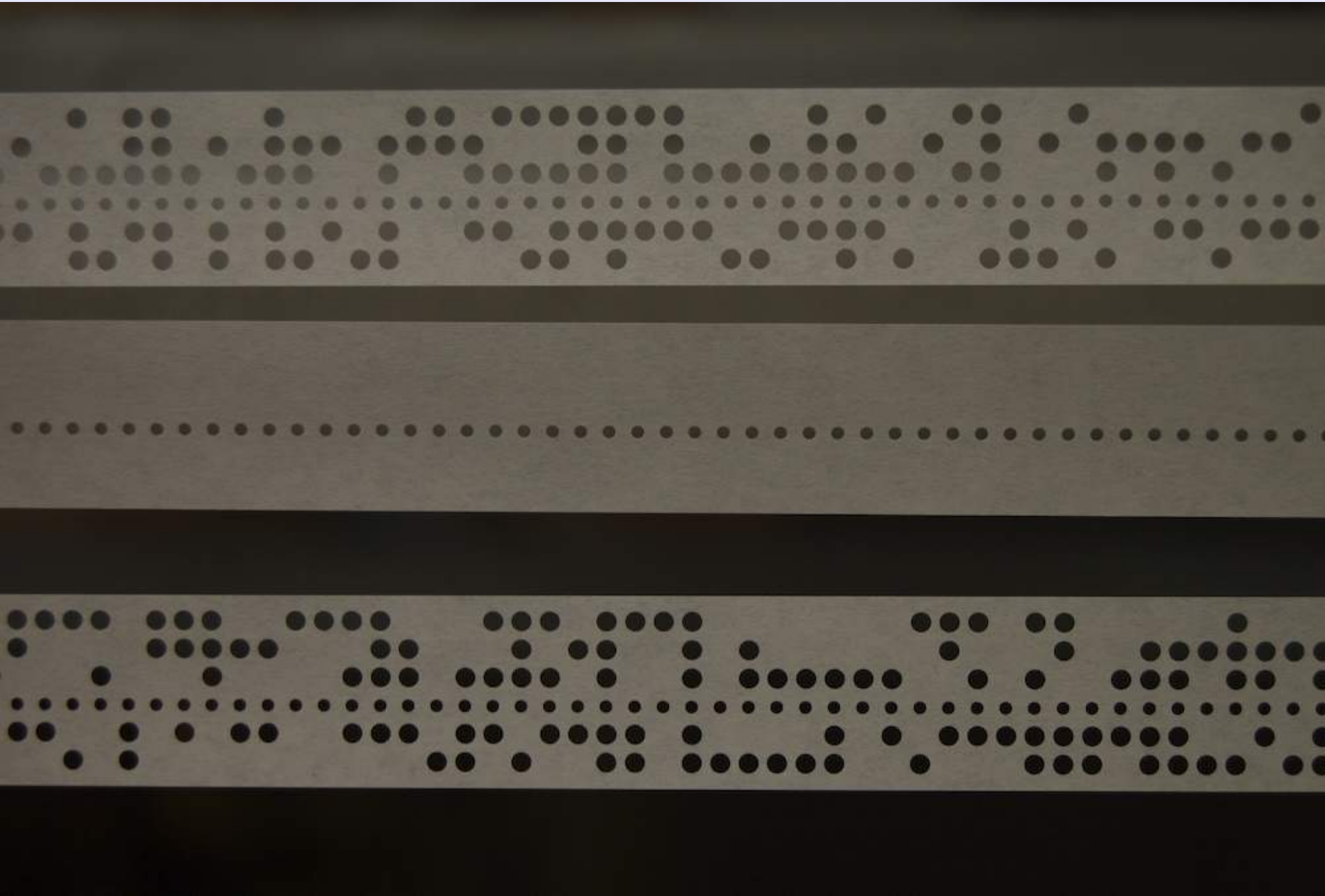
Major z. D.

Berlin, 1863.

Druck und Verlag von E. S. Mittler und Sohn.

(Zimmerstraße 94. 95.)

Gilbert Vernam y Joseph Mauborgne, 1920



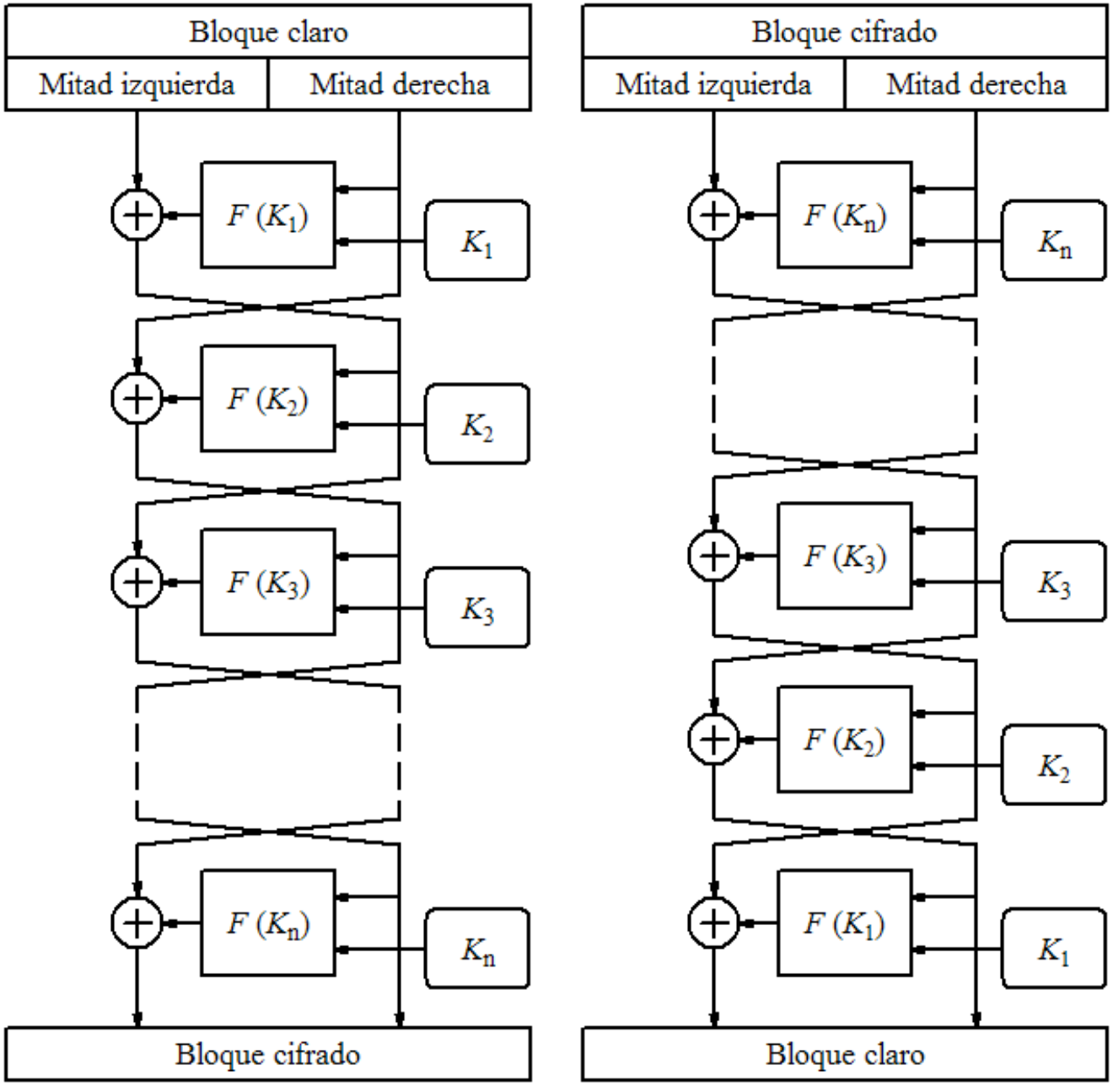
Cifrado electro-mecánico, II guerra mundial: Enigma, Purple, Typex, Sigaba

Rotura de la Enigma: Marian Rejewski y Alan Turing

Bletchley Park Park

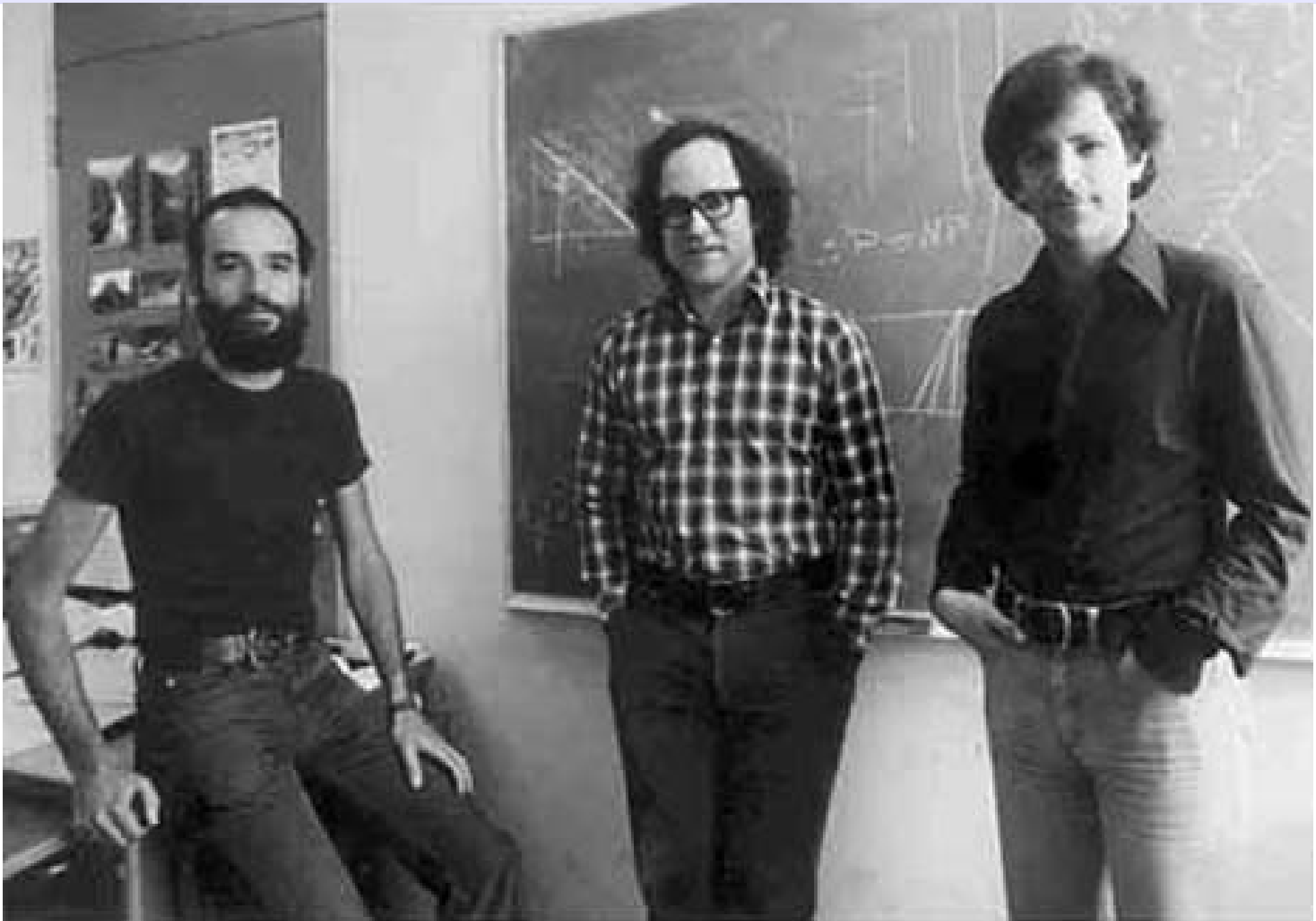
Palacio de Miramar

Data E

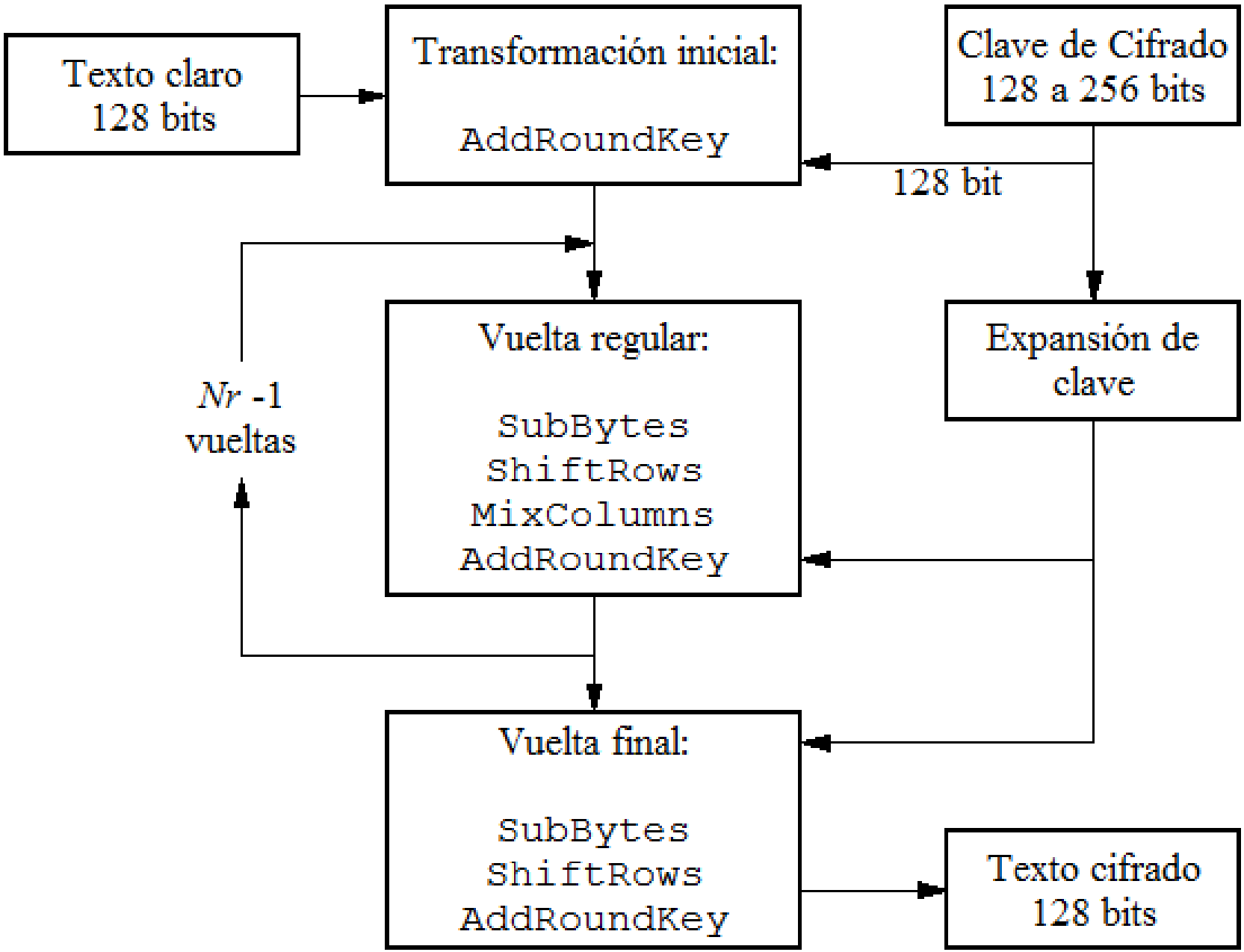

Bloque claro
Mitad izquierda
Mitad derecha
F (K1)
K1
F (K2)
K2
F (K3)
K3
F (Kn)
Kn
Bloque cifrado
Bloque cifrado
Mitad izquierda
Mitad derecha
F (Kn)
Kn
F (K3)
K3
F (K2)
K2
F (K1)
K1
Bloque claro

Establecimiento público de clave secreta: W. Diffie y M. Hellman, 1976

Cifrado asimétrico: Rivest, Shamir y Adleman, 1977



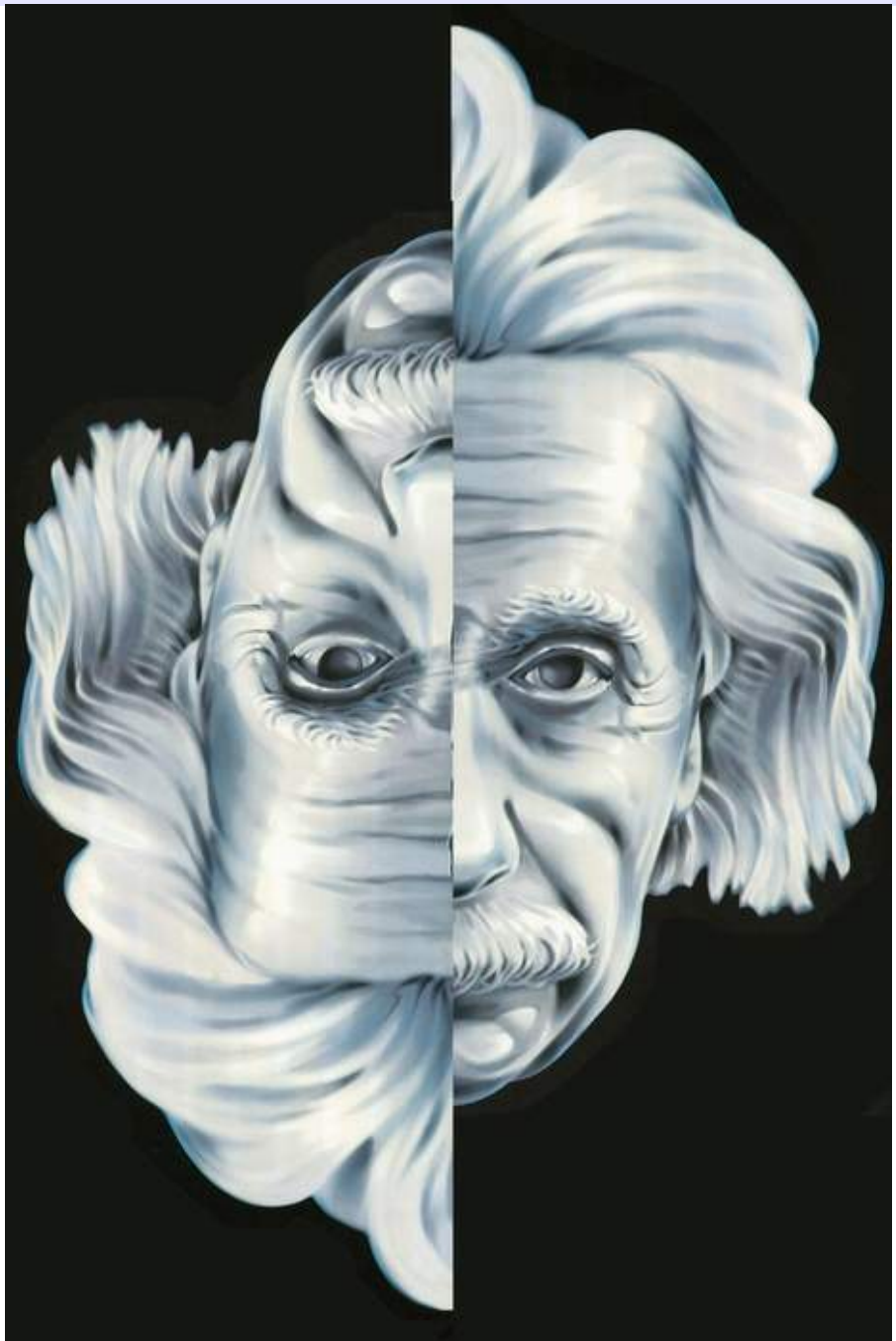
Advanced Encription Standard (AES), 2002



Cifrado en flujo: The eSTREAM Project, 2004/08

European Network of Excellence in Cryptology

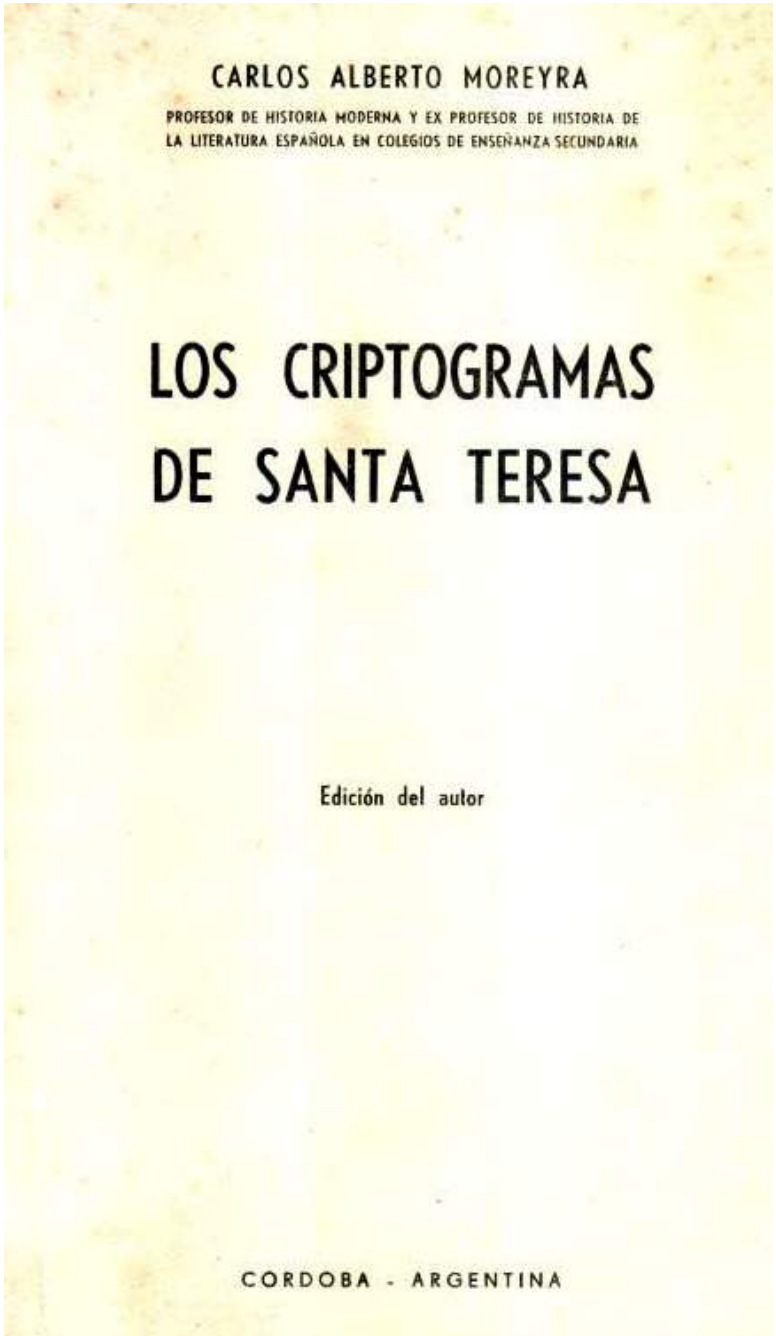
Criptografía cuántica, ¿el futuro?

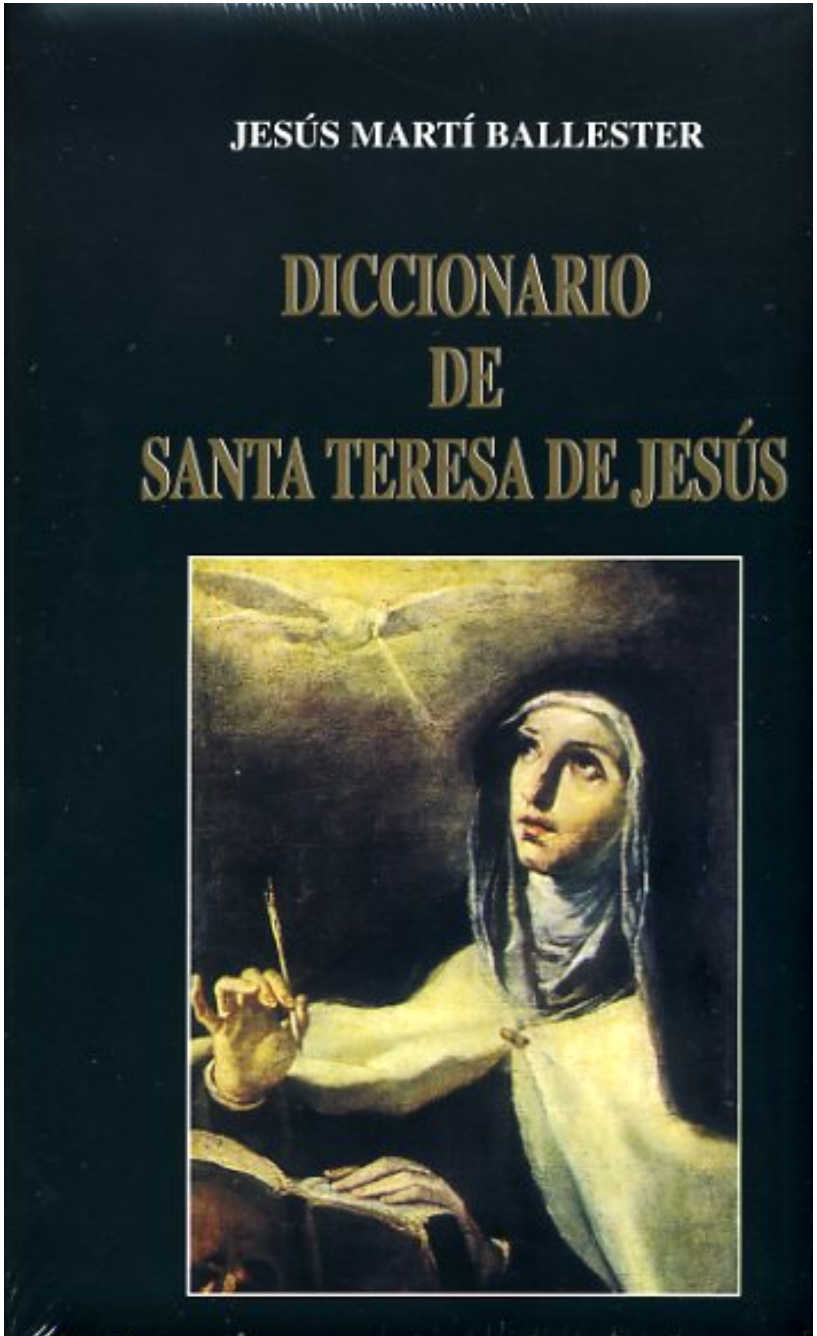


Criptografía en España

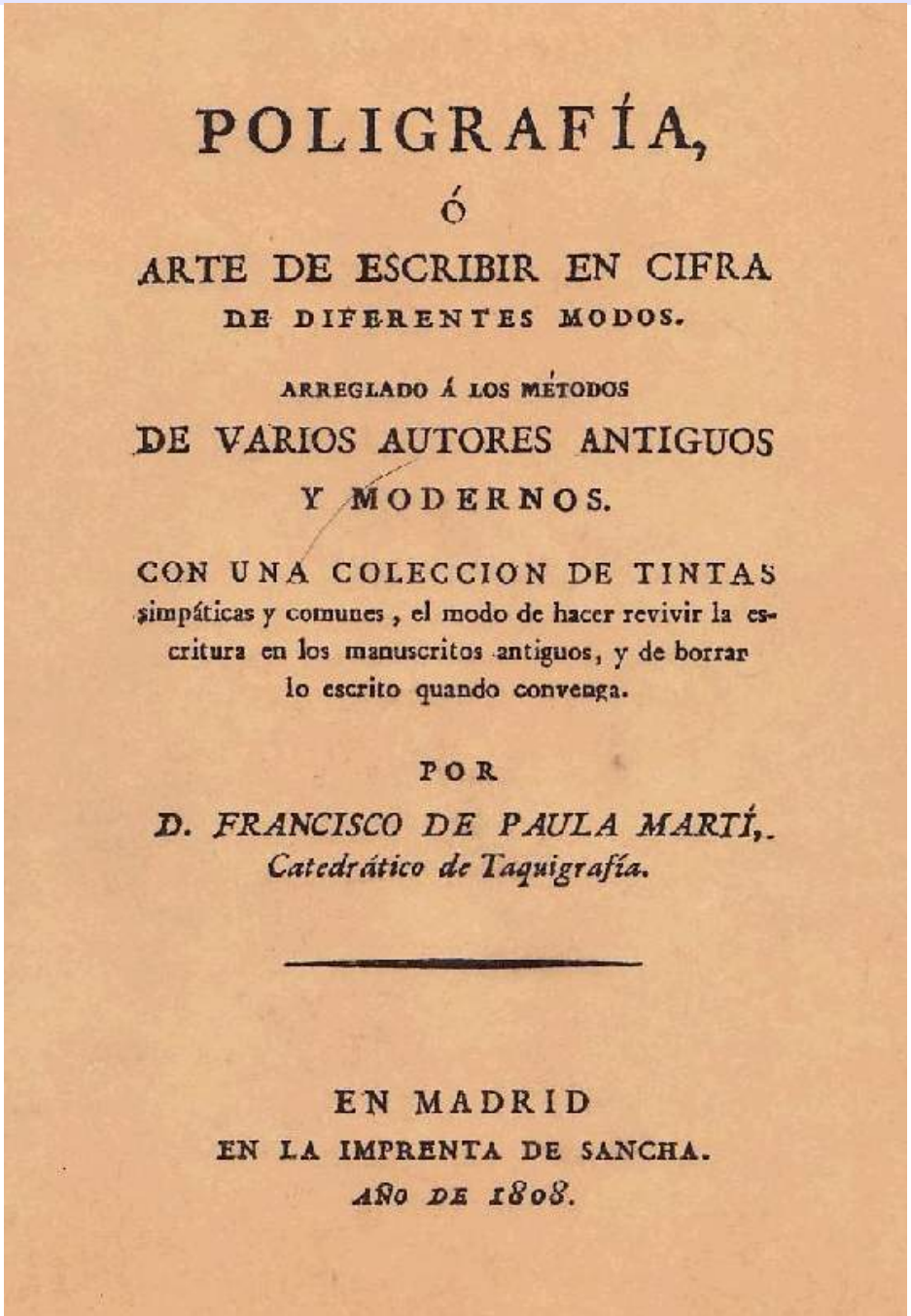
Nomenclator: Reyes Católicos, Carlos I, FelipeII

Tambien los santos cifraban





Francisco de Paula Martí, 1808



POLIGRAFÍA,

Ó

ARTE DE ESCRIBIR EN CIFRA

DE DIFERENTES MODOS.

ARREGLADO Á LOS MÉTODOS

DE VARIOS AUTORES ANTIGUOS

Y MODERNOS.

CON UNA COLECCION DE TINTAS simpáticas y comunes, el modo de hacer revivir la escritura en los manuscritos antiguos, y de borrar lo escrito quando convenga.

POR

D. FRANCISCO DE PAULA MARTÍ,

Catedrático de Taquigrafía.

EN MADRID

EN LA IMPRENTA DE SANCHA.

AÑO DE 1808.

Cesareo Huecas Carmona, 1894 (2011)

J. G. Carmona

Tratado de criptografía con aplicación especial al Ejército

MINISTERIO DE DEFENSA

TRATADO

DE

CRIPTOGRAFÍA

CON APLICACIÓN ESPECIAL AL EJÉRCITO

POR

CARMONA

PRIMER TENIENTE DE INFANTERÍA

(Primera obra de su género en español, premiada por el Ministerio de la Guerra.)

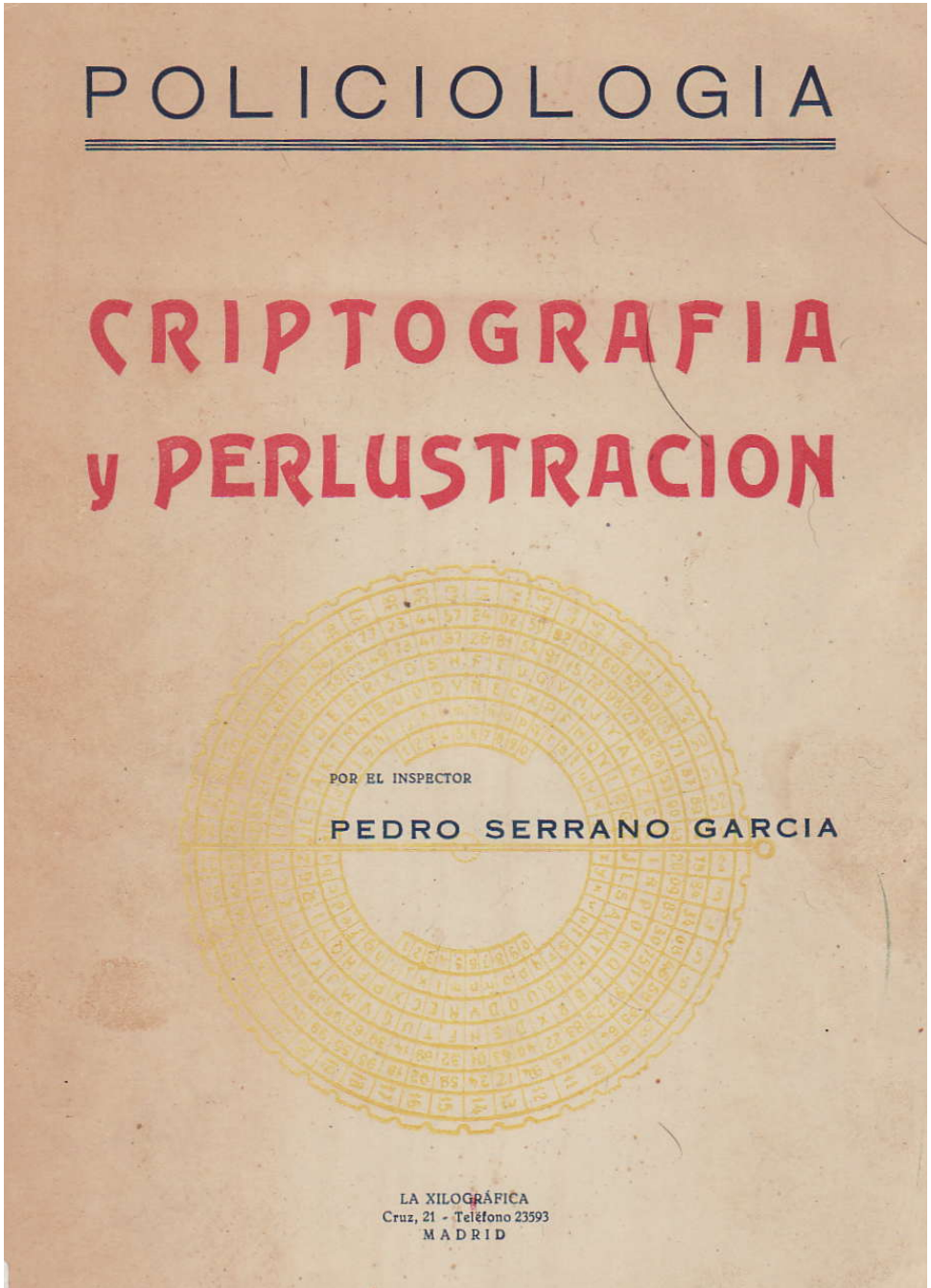
MADRID

EST. TIP. «SUCESORES DE RIVADENEYRA»

Paseo de San Vicente, 20.

1894

Criptografía y Perlustración, 1943



Enigma D comercial, 1936–1950

Hagelin CX-52, 1952

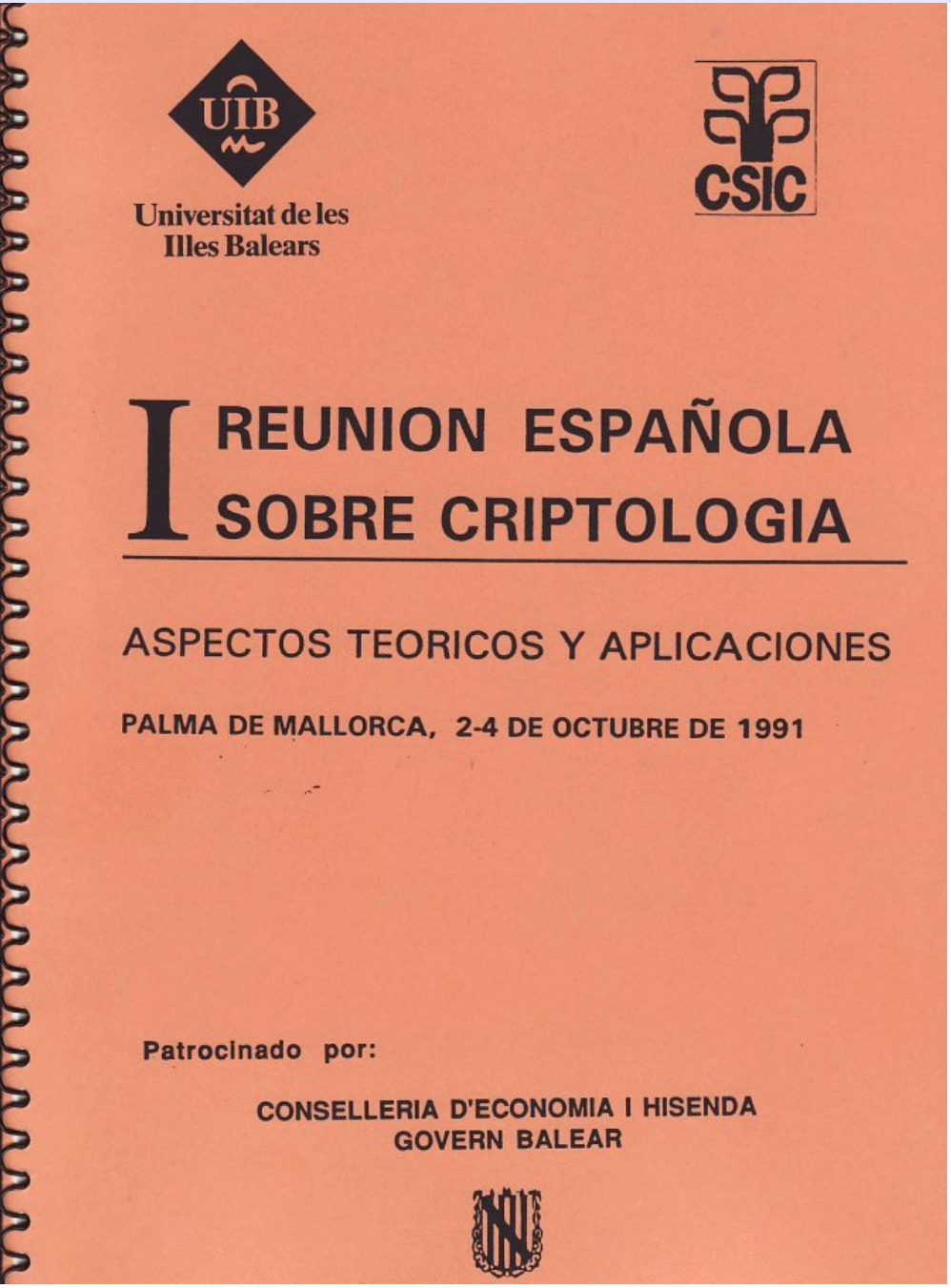
Hagelin C-52 OTP, 1952

Generador de cinta aleatoria: Mils Electronic, 1970-

Mezclador Siemens M 190

Secrafono inversor de banda ENSA 25A, 1960

Mayoría de edad de la criptografia española: 1991



COMITÉ ORGANIZADOR Y DE PROGRAMA

Llorenç Huguet i Rotger
Departament de Matemàtiques i Informàtica
Univesitat de les Illes Balears

Amparo Fúster Sabater
Laboratorio de Criptografía
Instituto de Electrónica de Comunicaciones
C.S.I.C.

Angel Rotger Mora
Departament de Matemàtiques i Informàtica
Univesitat de les Illes Balears

Dolores de la Guia Martínez
Laboratorio de Criptografía
Instituto de Electrónica de Comunicaciones
C.S.I.C.

Josep Blat Gimeno
Departament de Matemàtiques i Informàtica
Univesitat de les Illes Balears

Fausto Montoya Vitini
Laboratorio de Criptografía
Instituto de Electrónica de Comunicaciones
C.S.I.C.

Grace García Santos
Secretaria local de organización

Congreso en Mallorca, organizado por: Universidad de las Islas Baleares y CSIC

Participan:

- UNIVERSIDADES: Autónoma Barcelona, Islas Baleares, Politécnica de Cataluña, Politécnica de Madrid, Valladolid.
- CSIC: I. Electrónica de Comunicaciones.
- EMPRESAS: Control Sys, Europa MC, Omnisec, Penta3, Pitney Bowes, Técnicas de Cifra, Telettra.
- Ministerio Defensa: C. E. M., TYCE.
- Administración: Aserlocal, CEE Luxemburgo.

Investigación militar en el CSIC

Instituto Nacional de Electrónica.

- RADAR para uso general.
- Lupa de RADAR para artillería de costa costa.
- Detectores de minas para la guerra de Ifni 1957-58.

Lupa de RADAR de costa y RADAR para aviación

Criptografía en el CSIC

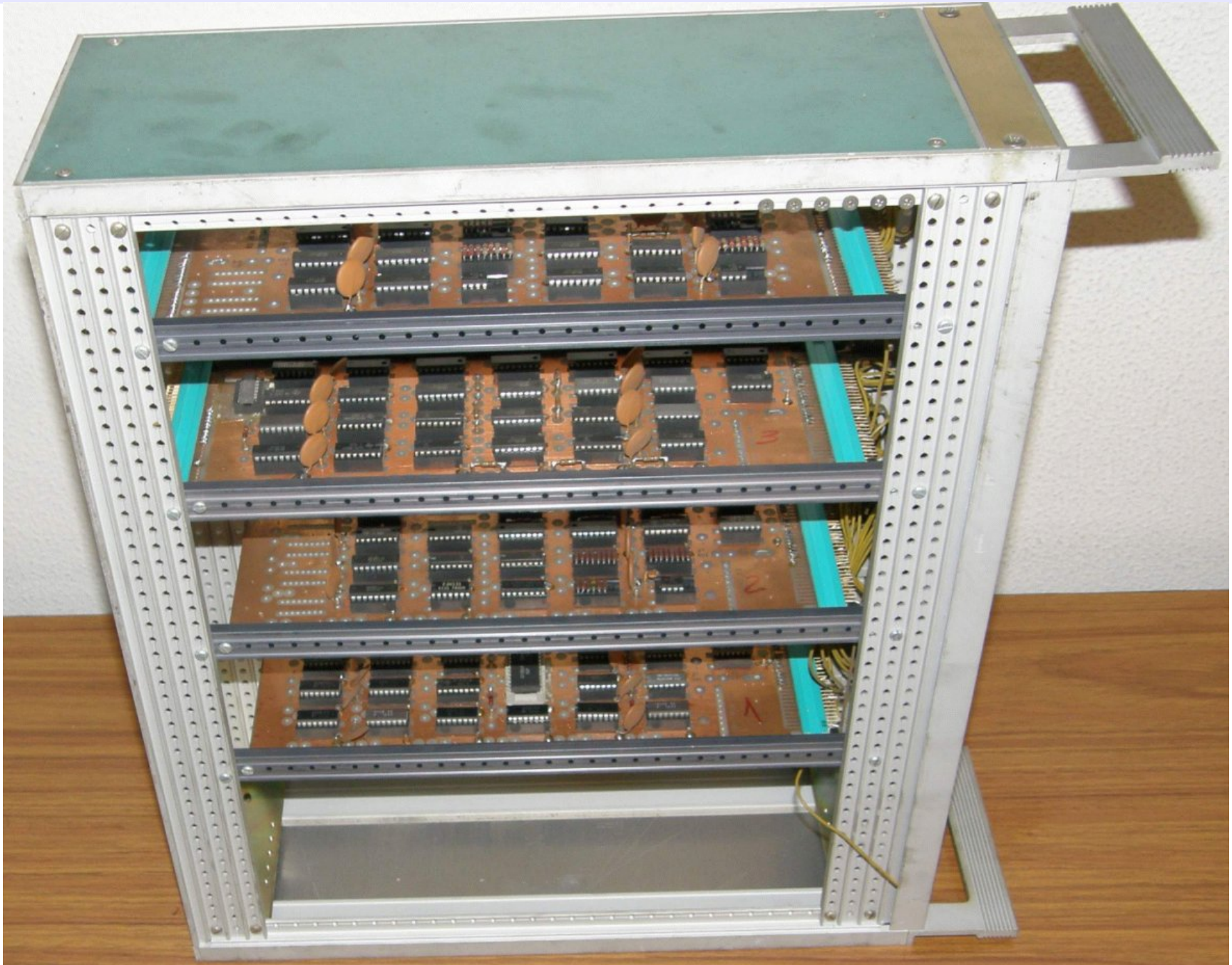
- Años 50: Inversión de banda de la voz (Gudar y Alía).
- Años 60: Subdivisión en 5 bandas parciales y permutación de voz (C. Schlayer).
- Años 60: Sistema de Vernam con transistores (C. Schlayer).
- Años 60: Transmisión de voz modulando un haz estrecho de Infrarrojos.

Grupo de Criptografía y Seguridad de la Información (GiCSI) del CSIC: década 70

- Tratamiento digital de la palabra y nuevo prototipo de secráfono (transposición en tiempo pseudoaleatoria de voz), 1975, CAICYT.
- Reducción del ancho de banda necesario para la transmisión digital de palabra e imagen (vocoder), 1976–78, CAICYT.
- Desarrollo de un prototipo de criptófono digital, 1976–78, Jefatura de Transmisiones del Ministerio del Aire.
- Cifrador y descifrador digital a 1.152 kbaudios, 1978, Marconi Española, S.A

Tecnología de los prototipos de los 70

Puros circuitos lógicos TTL en los 70



Grupo de Criptografía y Seguridad de la Información (GiCSI) del CSIC: década 80

- Criptófono digital de alta seguridad para teléfono, 1982–84, Dir. Investigación y Desarrollo, Ministerio de Defensa.
- Diseño de redes militares en los aspectos de conversión A/D y D/A, Criptofonía y Criptografía con enlaces multicanales y radioteléfonos de F.M, U.H.F., 1983–84, RADITE.
- Sistema de criptofonía para transmisión digital a baja velocidad, 1988, Dir. General de Armamento y Material, Ministerio de Defensa.
- Anteproyecto de equipo criptográfico para red integrada digital de comunicaciones tácticas, 1989, Marconi Española, S.A.
- Desarrollo de sistemas cifrados de comunicación y seguridad de datos, 1988–1991, CICYT.

Grupo de Criptografía y Seguridad de la Información (GiCSI) del CSIC: década 90 (subvencionado)

- Desarrollo de funciones y servicios de seguridad según las normativas X.400 y X.509 y su integración en entornos EDI, 1993–94, CDTI (PASO).
- Seguridad integral en redes de transmisión de datos, redes fijas de banda ancha y redes móviles, 1991–94, CICYT.
- Criptografía y protección integral de la información en el PLANBA, (Con CNM CSIC, Dto de Matemática Aplicada y Telemática UPC, Telesincro S.A.) 1994, Dir. Gral de Telecomunicaciones y CICYT.
- Sistema criptográfico de protección de datos para Red Digital de Servicios Integrados (RDSI), 1995–98, CICYT.
- Infraestructuras de Seguridad en Internet e Intranet, 1998–2001, CICYT.

Grupo de Criptografía y Seguridad de la Información (GiCSI) del CSIC: década 90 (contrato)

- Security evaluation of the VISA CASH electronic purse, Model TIBC, Designed by SERMEPA, 1998, VISA INTERNATIONAL, California, (USA).
- Security evaluation of the *Common Electronic Purse Specification* (CEPS), 1999, VISA INTERNATIONAL, California, (USA).
- Security evaluation of the version 2.1 of the *Common Electronic Purse Specifications*, developed by CEPSCO, 1999, VISA INTERNATIONAL, California, (USA).

GiCSI: siglo XXI (subvencionado)

1. Gestión del acceso seguro a redes abiertas de recursos distribuidos, 2002–04, MICYT.
2. Evaluación de protocolos y algoritmos de seguridad en sistemas de información (SEG2004-02418), 2005–07, MICYT.
3. Nuevos protocolos de seguridad y algoritmos criptográficos para la protección de servicios telemáticos, 2007–08, MEC.
4. CUántica y CaOs (CUCO):Algoritmos Criptográficos de Frontera, 2009–10, MEC.
5. EMOCION: rEconocimiento Mediante Olor Corporal en la Internet del futurO, 2009–11, Plan Avanza MITyC.
6. Criptografía cuántica a través del espacio libre, 2010, CSIC.
7. Identificación y autenticación seguras, 2010, MEC.
8. Secure Identification And Authentication In Electronic Communications (IDEASECE), 2012–14, MEC.
9. Malware Propagation Models Through On-line Social Networks (MARSOL), 2012–14, MEC.

Grupo de Criptografía y Seguridad de la Información (GiCSI) del CSIC: siglo XXI (contratos)

- Seguridad de los algoritmos de cifrado e identificación en telefonía GSM y recomendaciones para su mejora, 2000, Airtel Móvil SA.
- HESPERIA (Homeland sEcurity: tecnologíaS Para la sEguridad integRal en espaclos públicos e infrAestructuras), 2006-09, Soluciones Avanzadas de Control (CENIT, CDTI).
- SEGUR@: Seguridad y confianza en la sociedad de la Información, 2006–10, Telefónica I+D (CENIT, CDTI)
- Asistencia técnica en materia de evaluación de la seguridad de productos criptográficos, 2010–11, Ministerio de la Presidencia.

Criptografía cuántica

Para estar al día, publicar rápido y discutir artículos

Repositorios de preprints libres y gratis

Cryptology ePrint Archive.
http://eprint.iacr.org/
¡Lectura imprescindible!
Artículos desde 1966.

Apartados:
Mathematics,
Computer Science,
Cryptography and Security.

European Network of Excellence in Cryptology

ECRYPT II

- Informes anuales sobre avances de algoritmos y longitudes de clave.

European Network of Excellence in Cryptology

ECRYPT II

- Informes anuales sobre avances de algoritmos y longitudes de clave.
- Information & Communication Technologies (ICT) programme of the European Commission's Seventh Framework Programme (FP7).

European Network of Excellence in Cryptology

ECRYPT II

- Informes anuales sobre avances de algoritmos y longitudes de clave.
- Information & Communication Technologies (ICT) programme of the European Commission's Seventh Framework Programme (FP7).
- Información de talleres y reuniones Europeas.

European Network of Excellence in Cryptology

ECRYPT II

- Informes anuales sobre avances de algoritmos y longitudes de clave.
- Information & Communication Technologies (ICT) programme of the European Commission's Seventh Framework Programme (FP7).
- Información de talleres y reuniones Europeas.
- Laboratorios virtuales: SymLab (técnicas simétricas), MAYA (Multi-party and asymmetric algorithms), VAMPIRE (Virtual Applications and Implementations).

European Network of Excellence in Cryptology

ECRYPT II

- Informes anuales sobre avances de algoritmos y longitudes de clave.
- Information & Communication Technologies (ICT) programme of the European Commission's Seventh Framework Programme (FP7).
- Información de talleres y reuniones Europeas.
- Laboratorios virtuales: SymLab (técnicas simétricas), MAYA (Multi-party and asymmetric algorithms), VAMPIRE (Virtual Applications and Implementations).
- Se pueden presentar algoritmos para su evaluación.

citeulike

- Almacén de referencias encontradas por ti.

citeulike

- Almacén de referencias encontradas por ti.
- Almacén de tus PDF.

citeulike

- Almacén de referencias encontradas por ti.
- Almacén de tus PDF.
- Búsqueda de artículos y fuentes.

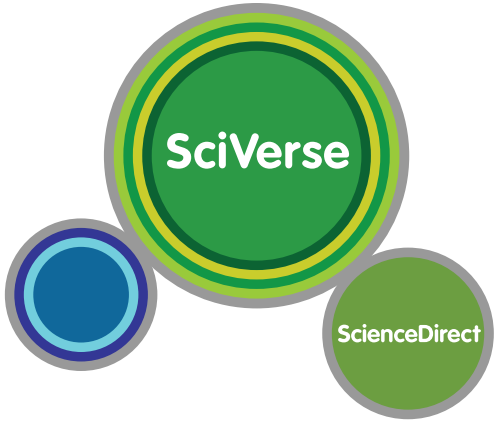
citeulike

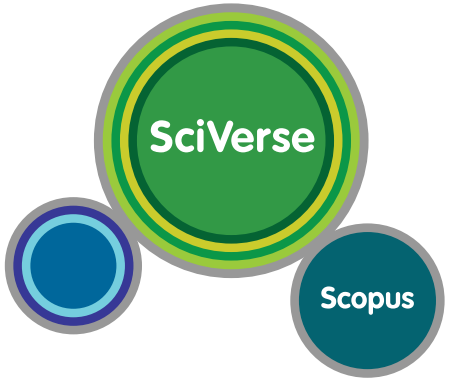
- Almacén de referencias encontradas por ti.
- Almacén de tus PDF.
- Búsqueda de artículos y fuentes.
- Recomendaciones automáticas.

citeulike

- Almacén de referencias encontradas por ti.
- Almacén de tus PDF.
- Búsqueda de artículos y fuentes.
- Recomendaciones automáticas.
- Comparte referencias con tus colegas.

SciVerse: Facilita el flujo de trabajo





- Interfaz intuitiva. Enlaces al texto completo de artículos.
- Identificador de autor. Índice h.
- Seguimiento de las citas en tiempo real.
- Identificador de organizaciones con su producción científica.
- Alertas, canales de información RSS.
- Descarga organizada de múltiples artículos.
- Exporta datos a través de RefWorks, EndNote y BibTeX.

Gestores de referencias bibliográficas

Permiten organizar la colección de libros, revistas, artículos y toda clase de información escrita o electrónica.

Funciona como una base de datos donde se añade la información mediante fichas. Incorpora enlaces a servicios de búsqueda en línea como IEEEXplore o arXiv. Licencia GPL. Código abierto. Java BibTeX manager.

Mendeley combina Mendeley Desktop gestión de PDFs y gestión de referencias (disponible para Windows, Mac y Linux) con Mendeley web: red social para investigadores. Escritorio y componentes Web para iPhone e iPad.

Software libre criptográfico irrenunciable

- Software que ilustra sistemas criptográficos.
- Perfecto para aprender criptografía real.
- Incluye más de 60 algoritmos de cifrado y criptoanálisis.

THE MARSAGLIA
RANDOM NUMBER CDROM
including the
DIEHARD BATTERY OF TESTS
OF RANDOMNESS

- Imprescindible para diseñar y evaluar generadores pseudoaleatorios.
- Cómodo de usar y de máxima calidad.
- Requiere secuencias de 100 Mbits.

Redes sociales científicas

- Red social de profesionales.
- Búsqueda y oferta trabajo.
- Problemas científicos.
- Problemas laborales y sociales.

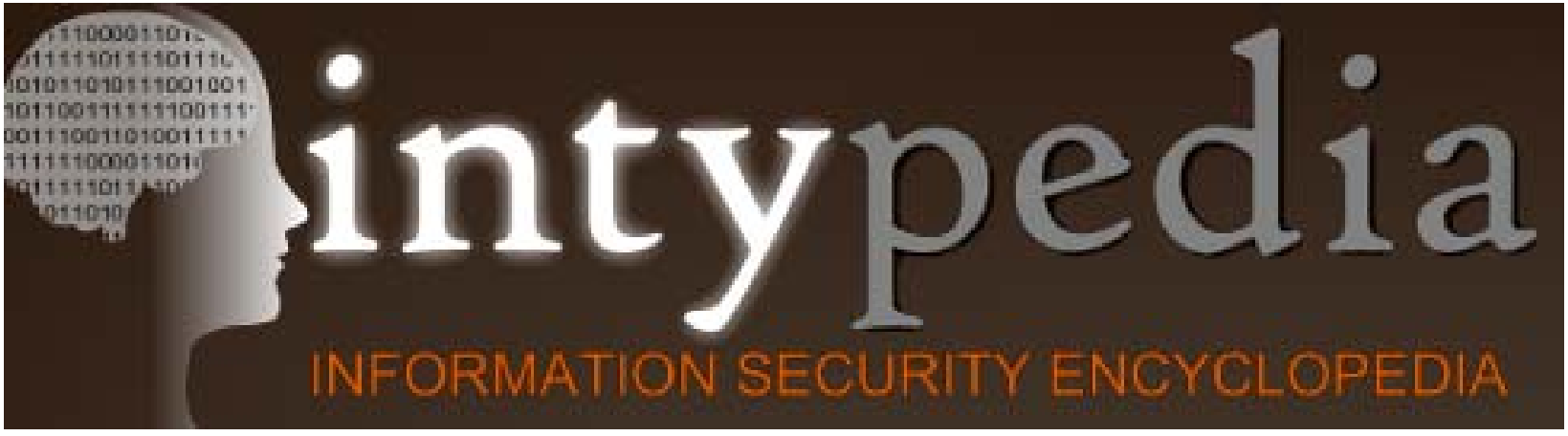
- Red social de científicos.
- Información sobre conferencias.
- Localización de artículos.
- Posibilita encontrar colaboradores en todo el mundo.
- Difunde tus artículos.

Foro de discusión científica

- Plataforma abierta para discutir las publicaciones, recogidas en su base de datos.
- Cargar el material adicional, resultados experimentales, presentaciones de PowerPoint.
- Registro de publicaciones y sus comentarios.

Divulgación de criptografía y seguridad de la información

INformation securi**TY** encyclo**PEDIA**



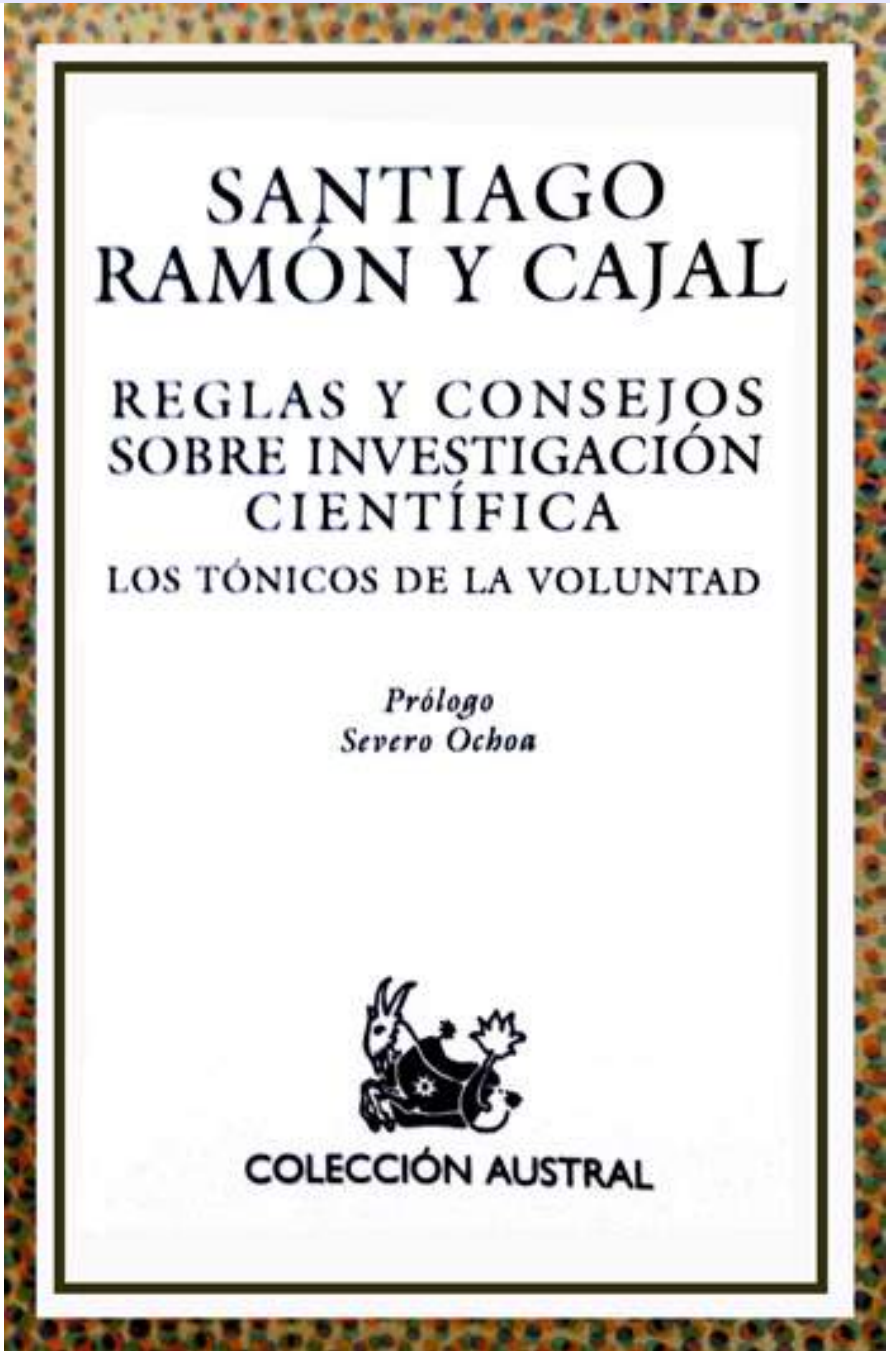
- Proyecto educativo sin ánimo de lucro.
- Enciclopedia visual de la seguridad de la información.
- Desarrollado por Jorge Ramió Aguirre, de la UPM.

http://www.criptored.upm.es/

- Todas las noticias necesarias de criptografía y seguridad de la información, para España e Iberoamérica.
- Desarrollado por Jorge Ramió Aguirre, de la UPM.

Sitios donde almacenar y compartir en la nube

Santiago Ramón y Cajal, ¡Sigue vigente!



GRACIAS