

Criptografía y la I+D+i en seguridad de la información en España

Conferencia Jornada Académica del Máster Universitario en Ciberseguridad UPM

ETSISI – UPM. Madrid, 8 de marzo de 2018



Igualdad de género

8 de marzo
Día internacional de la mujer

Dr. Jorge Ramió Aguirre
Prof. Titular UPM – ETSISI
Director de CriptoRed



Breve introducción (*añadido después de la charla*)

La criptografía, con sus más de 5 siglos de historia, ha sido uno de los pilares de la seguridad informática. Si bien en los últimos 30 años esta ciencia ha ido perdiendo aquel papel preponderante que desempeñaba antaño, últimamente el interés por el estudio y la investigación en criptografía vuelve a resurgir con nuevos bríos, entre otras cosas por los interrogantes que nos plantean la seguridad real de las actuales operaciones de cifra (especialmente la asimétrica) ante los avances en computación cuántica y las cadenas de bloques, con las criptomonedas como ejemplo de aplicación real con gran impacto en la sociedad.

Ante este reciente interés, una primera pregunta sería cómo hacer llegar estos conocimientos a los futuros ingenieros y expertos en seguridad. Y surge así una segunda pregunta lógica: ¿qué se hace en I+D+i en criptografía en España?

Si conocemos cuántos grupos de investigación en seguridad de la información existen en España y cuántos de ellos se dedican preferentemente o tienen como línea principal de investigación a la criptografía, podríamos establecer en una primera aproximación qué importancia relativa tiene esta ciencia dentro del amplio espectro de la seguridad de la información.

Si nos permitimos ahora unir la investigación con la producción de tesis doctorales, una licencia a priori discutible si bien estas dos facetas no deberían estar demasiado desligadas, podríamos buscar por ejemplo cuántas tesis doctorales se han leído en España sobre criptografía y cuántas tesis en los demás campos de la seguridad de la información.

Cabe esperar, en este caso, que los datos obtenidos tendrán una relación directa con ese peso relativo antes comentado de la criptografía dentro de la seguridad de la información, pero no será así.

En esta conferencia se presentan dichos datos y se dejan abiertas las conclusiones que puedan derivarse de ello.

El papel de la criptografía en la enseñanza en España



¿Qué papel juega la criptografía en la ciberseguridad?

- No parece estar muy claro y en varios másteres de ciberseguridad la criptografía no aparece como asignatura. En este máster tampoco...
- Podrían existir varias justificaciones:
 - Ya se estudia en grado... al menos en España, sí es cierto.
 - Son las “matemáticas de la seguridad”, no cabe en un máster.
 - No se sabe bien qué impartir sobre criptografía en un máster.
 - No está claro su uso en la empresa, instituciones e industria.
 - No se ve como una necesidad a cubrir dentro de la ciberseguridad.
- Pero, con todo lo que se avecina en tecnologías blockchain, seguridad postcuántica, etc., posiblemente no sea una opción del todo acertada.
- Hay grupos de investigación en el sector empresarial (e.g. banca) que están apostando por la criptografía... ¡algo impensable hace tan sólo una década!





Montaña rusa en la enseñanza de la criptografía (1)

- **Años 1980/1990.** El génesis... “En el comienzo de todo...”. La criptografía lo era casi todo en la enseñanza de la seguridad.
- **Años 1990/2010.** Veinte años. En Seguridad Informática y en Seguridad de la Información (dos cosas distintas...) comienzan a aparecer nuevas líneas: SGSI, planes contingencia, análisis y gestión del riesgo, BCP, DRP, normas, legislación, programación segura, auditoría de máquina, seguridad en redes, IDS, forensia, reversing, análisis de malware, ICs, APTs, ...
- La criptografía pierde ese protagonismo. Era lo lógico y, además, **necesario**.
- **Años 2010/2020.** Ha nacido ya bitcoin y comienzan a salir otros sistemas similares basados en algoritmos criptográficos. Se observan grandes avances en computación cuántica, que pone en entredicho la seguridad actual de nuestros algoritmos para comunicaciones seguras,... **es decir...**



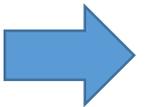
Montaña rusa en la enseñanza de la criptografía (2)

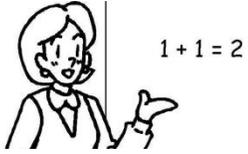
- Volvemos la mirada hacia la ciencia de la criptografía. Pero en cuanto a la enseñanza, lo haremos con una importante diferencia.
- Lo que hasta ahora era una enseñanza elemental, que requería de unos conocimientos muy básicos (elementales) de matemática discreta, etc., se volverá bastante más compleja (en matemáticas y en física).

Algunas preguntas abiertas:

- En 2030, ¿cómo se enseñará criptografía en las ingenierías y en másteres?
- ¿Los alumnos, que ya se quejan por matemáticas básicas, lo “aceptarán”?
- ¿Deberá tener otro perfil el futuro profesor de criptografía?

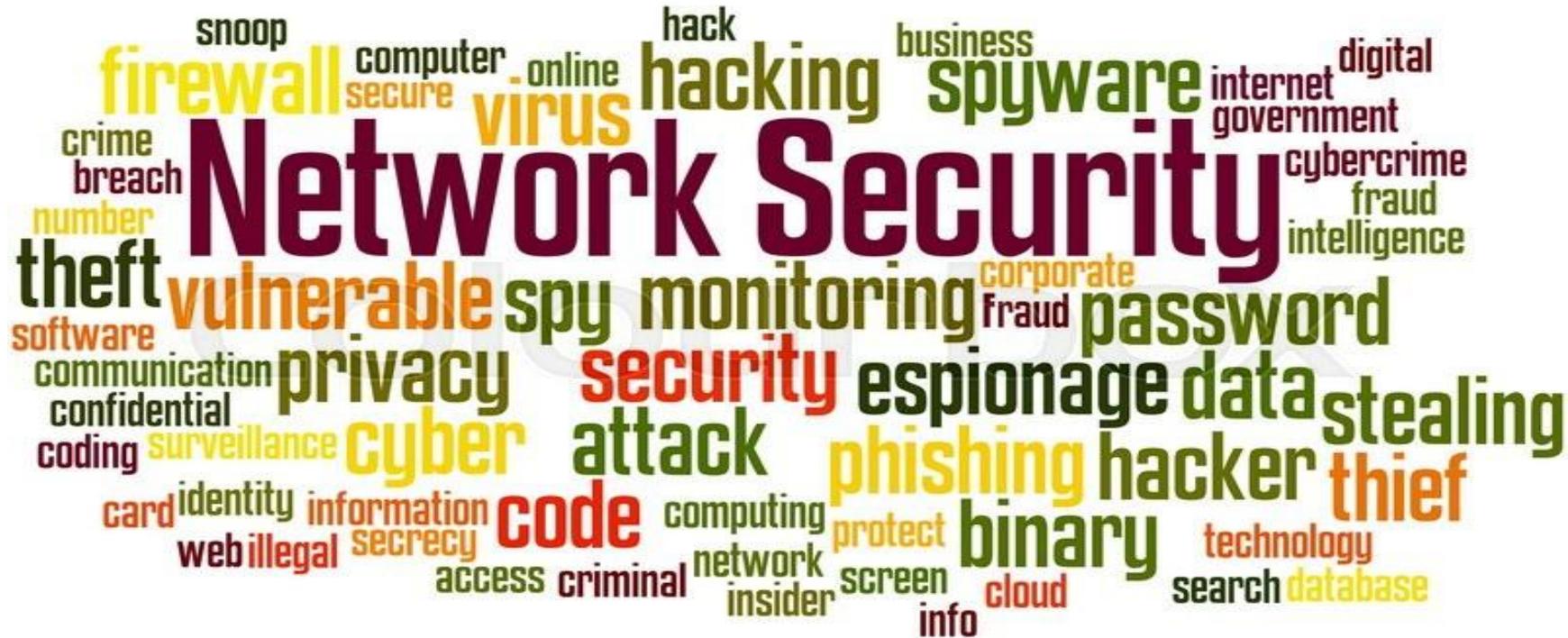
Veamos cómo se han ido orientando las enseñanzas en seguridad



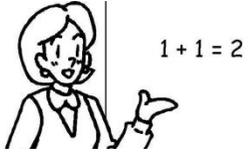


Las enseñanzas de la seguridad (2)

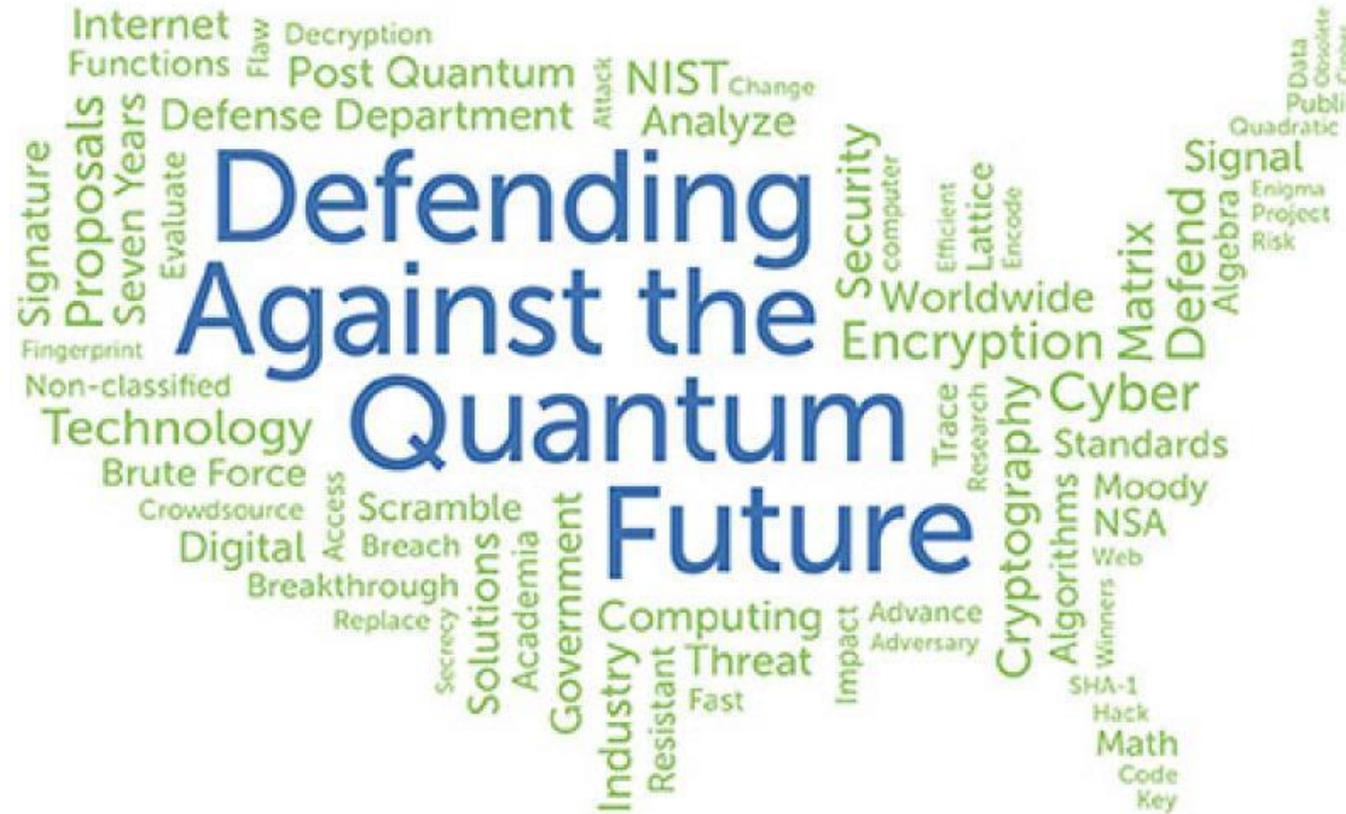
Orientación hacia la seguridad en redes



Y llegaron las redes...



Las enseñanzas de la seguridad (6) Orientación hacia las amenazas futuras



Y se acerca un futuro incierto...



¿Por qué no una ingeniería en seguridad teleinformática?

- Integrating Security into the Curriculum, Computer IEEE, 1998. Cynthia E. Irvine, Shiu-Kai Chin, Deborah Frincke.
- Introducción de las enseñanzas de Seguridad informática en los Planes de Estudio de las Ingenierías del Siglo XXI, JENUI 2001, Jorge Ramió.
- ¿Por qué no es posible? *In my humble opinion...*  “falta personal”
- ¿Qué solución se ha buscado? *In my humble opinion...* Posgrados 
- Oferta de másteres en seguridad informática en España (> 45)
- ¿Masoquismo? No. Ley del mercado. No eres nadie si no ofreces uno.

El papel de la criptografía en la I+D+i en España



El I+D+i en seguridad de la información en España

- Informe INCIBE RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad). Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad (2017).
- Detectados 104 grupos de investigación.
- 31 grupos incluyen a la criptografía como una de sus líneas de interés.
- Pero sólo 8 grupos incluyen criptografía en el nombre del grupo:
CSIC, UDL, UNIOVI, UPC, USAL, UVA, UNICAN, UOC.
- Excepto CSIC y UOC (KISON) que son centros de investigación, los 6 restantes están relacionados con Departamentos de Matemáticas... 



El I+D+i en criptografía en España (1)

- CSIC, UDL, UNIOVI y UPC muestran una actividad notoria en proyectos de investigación directamente relacionados con la criptografía.
- Hay otros grupos que no llevan en su nombre criptografía pero que también muestran cierta actividad en proyectos de investigación directamente relacionados con la criptografía (e.g. UC3M, UNILEON).
- Una docena de proyectos (quizás alguno(s) más, pero en general pocos).
- **Sin embargo**, en el apartado publicaciones (revistas, congresos,...) sí se observa una alta producción y difusión de resultados de muchos grupos.
- Por otra parte, en una infografía del Mapa I+D+i en Ciberseguridad en España (RENIC) se observa lo siguiente:

Criptografía en el puesto 8 de 12 temáticas de interés en los grupos.

El I+D+i en criptografía en España (2)

Adecuado 

Puesto 1	Sistemas Fiables y Actualizables
Puesto 2	Privacidad
Puesto 3	Procesado de Datos
Puesto 4	Infraestructuras Críticas
Puesto 5	Evaluación de Sistemas y Ciberriesgos
Puesto 6	Ataques y Defensa ante Amenazas
Puesto 7	Gestión de la Identidad
Puesto 8	Criptografía
Puesto 9	Fomento y Concienciación de la Seguridad
Puesto 10	Seguridad de Red
Puesto 11	Cloud Computing
Puesto 12	Internet of Things

 Llamativo...

Temáticas más frecuentes en grupos de investigación

- Hasta aquí, todo parece tener bastante sentido... la criptografía sigue ahí como un elemento más, ni es el **más** importante ni tampoco el **menos**.
- Dentro de la seguridad, podríamos decir que la criptografía hoy debería tener un peso relativo entre el 10% y el 20%. Es un valor *aceptable*, **PERO...**

Si la I+D+i pudiera asociarse con
la lectura de tesis doctorales...
¿podríamos inferir algo nuevo?
Búsquedas en TESEO: 01/10/17



Tesis doctorales en criptografía (1)

Búsquedas en el título:

- criptogra
- cryptogra
- esteganogra
- steganography
- criptolog
- criptoanálisis

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda

Número de registros encontrados: 24

Anterior 1 - 2 - 3 - Siguiente

Seleccionar todos Deseleccionar

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- ALGORITMOS CRIPTOGRÁFICOS Y APLICACIONES SEGURAS PARA ESCENARIOS DE TRANSPORTE
- FEEDBACK CLASIFICACIÓN DE SISTEMAS Y CÓDIGOS DE CONVOLUCIÓN. APLICACIONES EN CIBERNÉTICA, TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA
- ESTUDIO ESCALABILIDAD DE LA ARITMÉTICA DE CUERPOS FINITOS EN HARDWARE RECONFIGURABLE Y APLICACIONES CRIPTOGRÁFICAS,
- GENERACIÓN DE FALSAS CLAVES CRIPTOGRÁFICAS COMO MEDIDA DE PROTECCIÓN FRENTE A ATAQUES POR CANAL LATERAL
- DISTRIBUCIÓN DE CLAVES CRIPTOGRÁFICAS POR FIBRA ÓPTICA MEDIANTE TÉCNICAS CUÁNTICAS
- EVALUACION DE DESEMPEÑO DE PROCESOS DE CRIPTOGRAFIA COMO SERVICIO (CASS) EN LA NUBE: CASO DE ESTUDIO: SERVICIOS Y CUSTODIA DE CLAVES CRIPTOGRÁFICAS EN PROCESOS DE NOTARIADO ELECTRONICO
- CRIPTOGRAFIA CAOTICA: ESTUDIO, DISEÑO Y APLICACIONES
- DISEÑO AUTOMÁTICO DE FUNCIONES HASH NO CRIPTOGRÁFICAS
- VOLCANS DISOGÉNIAS DE CORBES ELÍPTICAS: APLICACIONES CRIPTOGRÁFICAS EN OBJETOS INTELIGENTES
- WI-CRIPTOFPGA: IMPLEMENTACIÓN DE ALGORITMOS CRIPTOGRÁFICOS MEDIANTE UNA ARQUITECTURA RECONFIGURABLE BASADA EN FPGAs, APLICACIÓN A REDES DE INTERCONEXIÓN INALÁMBRICA.

Anterior 1 - 2 - 3 - Siguiente

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por "*criptogra*": 24 tesis (página 1).



Tesis doctorales en criptografía (2)

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda Número de registros encontrados: 24

- Anterior - 1 2 - 3 - Siguiente

Seleccionar todos Deseleccionar [ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- SISTEMAS CRIPTOGRÁFICOS DE CURVA ELÍPTICA BASADOS EN MATRICES.
- PROTOCOLOS CRIPTOGRÁFICOS PARA CANALES DE COMUNICACIÓN ANÓNIMOS Y PROTECCIÓN DE ITINERARIOS EN AGENTES MÓVILES
- ANILLOS NO ASOCIATIVOS EN CODIFICACIÓN Y CRIPTOGRAFÍA
- NÚMEROS PRIMOS ESPECIALES Y SUS APLICACIONES CRIPTOGRÁFICAS
- DISEÑO, IMPLEMENTACIÓN Y OPTIMIZACIÓN DE ALGORITMOS CRIPTOGRÁFICOS DE GENERACIÓN DE ALEATORIOS Y FACTORIZACIÓN DE ENTEROS.
- DISEÑO DE PROTOCOLOS CRIPTOGRÁFICOS: NUEVAS PROPUESTAS BASADAS EN GRAFOS
- SÍNTESIS DEL MODELO DE AUTÓMATAS CELULARES EN PROTOCOLOS CRIPTOGRÁFICOS DE CIFRADO EN FLUJO Y ORIENTADO A REDES DE FEISTEL
- CONTRIBUCION AL ESTUDIO DE LA ESTRUCTURA INTERNA DEL CONJUNTO DE MANDELBROT Y APLICACIONES EN CRIPTOGRAFIA
- CORBES ELIPTIQUES MODUL N I APLICATIONS CRIPTOGRAFIQUES.
- ESTUDIO DE ALGORITMOS CRIPTOGRAFICOS DE CLAVE PUBLICA BASADOS EN EL PROBLEMA DEL LOGARITMO DISCRETO. UTILIZACION DE CURVAS ELIPTICAS EN CRIPTOGRAFIA.

- Anterior - 1 2 - 3 - Siguiente

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por "*criptogra*": 24 tesis (página 2).



Tesis doctorales en criptografía (3)

The screenshot shows the TESEO (Tesis Doctorales en Español) website interface. At the top, there is a header with the Spanish flag and the text 'GOBIERNO DE ESPAÑA' and 'MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE'. Below the header, a breadcrumb trail reads 'Está usted en: Portada > Universidades > Educación superior universitaria'. The main heading is 'Tesis doctorales: TESEO'. Underneath, it says 'Resultado de la búsqueda' and 'Número de registros encontrados: 24'. There are navigation links for 'Anterior', '1', '2', '3', and 'Siguinte'. Below this, there are checkboxes for 'Seleccionar todos' (checked) and 'Deseleccionar'. There are also buttons for 'ver Selección', 'Modificar Consulta', and 'Nueva Consulta'. The search results are listed in a table with three visible entries, each with a checkbox:

- ESTUDIO Y DESARROLLO DE UN ESQUEMA CRIPTOGRAFICO PARA REALIZAR VOTACIONES SEGURAS SOBRE UNA RED LOCAL.
- ALGUNAS APLICACIONES DE LAS CURVAS ELIPTICAS A LA CRIPTOGRAFIA.
- GENERADORES DE NUMEROS ALEATORIOS EN CRIPTOGRAFIA.
- DISEÑO DE METODOS CRIPTOGRAFICOS PARA LA PROTECCION DE LA INFORMACION EN SISTEMAS DE ORDENADORES.

At the bottom of the page, there is a footer with the text 'versión 4.1.10', '© Ministerio de Educación, Cultura y Deporte', and links for 'Aviso legal' and 'Accesibilidad'.

TESEO: Búsqueda por "criptogra": 24 tesis (página 3).



Tesis doctorales en criptografía (4)

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda Número de registros encontrados: 9

Seleccionar todos Deseleccionar [ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- CRYPTOGRAPHIC PROTOCOLS FOR PRIVACY-AWARE AND SECURE E-COMMERCE
- AUTOMATION AND MODULARITY OF CRYPTOGRAPHIC PROOFS IN THE COMPUTATIONAL MODEL
- VECTOR BOOLEAN FUNCTIONS: APPLICATIONS IN SYMMETRIC CRYPTOGRAPHY
- HARDWARE DESIGN OF CRYPTOGRAPHIC ALGORITHMS FOR LOW-COST RFID TAGS
- SOME ISSUES IN PUBLIC KEY CRYPTOGRAPHY: HARD-CORE RPEDICATES, DISTRIBUTED PROTOCOLS AND FUNCTIONAL ENCRYPTION
- LIGHTWEIGHT CRYPTOGRAPHY IN RADIO FREQUENCY IDENTIFICATION (RFID) SYSTEMS
- ENTANGLEMENT AND QUANTUM CRYPTOGRAHY
- NONLINEAR DYNAMICS OF SEMICONDUCTOR LASER SYSTEMS WITH FEEDBACK: APPLICATIONS TO OPTICAL CHAOS CRYPTOGRAPHY, RADAR-FREQUENCY GENERATION, AND TRANSVERSE-MODE CONTROL.
- APROXIMACION AL ORIGEN DE LA ESTRUCTURA INDUSIAL Y LA ANISOFILIA EN FILICOPHYTAS. ESTUDIO ANATOMO-HISTOLOGICO DE CRYPTOGRAMMA CRISPA (L.)R. BR.

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por “*criptogra*”: 9 tesis.



Tesis doctorales en criptografía (5)

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda

Número de registros encontrados: 2

Seleccionar todos Deseleccionar

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- DISEÑO DE UN NUEVO ALGORITMO ESTEGANOGRÁFICO EN EL DOMINIO ESPACIAL
- AUTOMATIZACIÓN DE PROCEDIMIENTOS EN ESTEGANOGRAFÍA Y ESTEGOANÁLISIS LINGÜÍSTICO UTILIZANDO LA LENGUA ESPAÑOLA

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por "esteganogra": 2 tesis.



Tesis doctorales en criptografía (6)

The screenshot shows the TESEO (Tesis Doctorales en Español) website interface. At the top, there is a header with the Spanish flag and the text 'GOBIERNO DE ESPAÑA' and 'MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE'. Below the header, a breadcrumb trail reads 'Está usted en: Portada > Universidades > Educación superior universitaria'. The main heading is 'Tesis doctorales: TESEO'. Underneath, it says 'Resultado de la búsqueda' and 'Número de registros encontrados: 2'. There are buttons for 'ver Selección', 'Modificar Consulta', and 'Nueva Consulta'. The search results are listed as follows:

- INFORMATION LEAKAGE AND STEGANOGRAPHY: DETECTING AND BLOCKING COVERT CHANNELS
- ON ADDITIVE BINARY NONLINEAR CODES AND STEGANOGRAPHY

At the bottom of the page, it says 'versión 4.1.10', '© Ministerio de Educación, Cultura y Deporte', and 'Aviso legal | Accesibilidad'.

TESEO: Búsqueda por "steganography": 2 tesis.



Tesis doctorales en criptografía (7)

The screenshot shows the TESEO (Tesis Doctorales en España) website interface. At the top, there is a header with the Spanish flag and the text 'GOBIERNO DE ESPAÑA' and 'MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE'. Below the header, a breadcrumb trail reads 'Está usted en: Portada > Universidades > Educación superior universitaria'. The main heading is 'Tesis doctorales: TESEO'. Underneath, it says 'Resultado de la búsqueda' with links for 'Ayuda' and 'Salir'. It indicates 'Número de registros encontrados: 2'. There are two search results listed, each with a checkbox and a 'ver Selección' button. The first result is 'TÉCNICAS DE INTELIGENCIA ARTIFICIAL EN CRIPTOLOGÍA' and the second is 'ASPECTOS JURIDICOS DE LA PROTECCION CRIPTOLOGICA DE LA INFORMACION Y LAS COMUNICACIONES.' At the bottom of the page, it shows 'versión 4.1.10', '© Ministerio de Educación, Cultura y Deporte', and links for 'Aviso legal' and 'Accesibilidad'.

TESEO: Búsqueda por "*criptolog*": 2 tesis.



Tesis doctorales en criptografía (8)

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda Número de registros encontrados: 5

Seleccionar todos Deseleccionar [ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- CONTEXTO, CRIPTOANÁLISIS Y PROPUESTA DE SOLUCIÓN DE LA INSCRIPCIÓN DE LA TALLA (ORIGINAL) DE LA VIRGEN DE CANDELARIA DE TENERIFE (CANARIAS, ESPAÑA)
- CONTRIBUCIÓN AL ESTUDIO DEL CRIPTOANÁLISIS Y DISEÑO DE LOS CRIPTO SISTEMAS CAÓTICOS
- AVANCES RECIENTES EN EL CRIPTOANÁLISIS DEL CRIPTO SISTEMA DE CHOR-RIVEST: APLICACIONES CRIPTOGRÁFICAS
- CRIPTOANÁLISIS DE GENERADORES NO LINEALES DE NÚMEROS PSEUDOALEATORIOS.
- ALGORITMOS GENÉTICOS Y CRIPTOANÁLISIS. APLICACIÓN DE NUEVOS MÉTODOS HEURÍSTICOS.

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por "*criptoanálisis*": 5 tesis.



Tesis doctorales en criptografía (9)

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

Está usted en: [Portada](#) > [Universidades](#) > [Educación superior universitaria](#)

Tesis doctorales: TESEO

[Ayuda](#) > [Salir](#)

Resultado de la búsqueda Número de registros encontrados: 9

Seleccionar todos Deseleccionar [ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

- CRITOSISTEMAS DE CIFRADO EN FLUJO BASADOS EN MATRICES TRIANGULARES CON MÚLTIPLES BLOQUES
- SISTEMAS NO LINEALES DE CIFRADO Y AUTENTICACIÓN DE IMÁGENES BASADOS EN EL CORRELADOR ÓPTICO DE TRANSFORMADAS CONJUNTAS (JTC)
- IMPLEMENTACIÓN EN TARJETAS INTELIGENTES JAVA CARD DE PROTOCOLOS DE CIFRADO Y DESCIFRADO BASADOS EN CURVAS ELÍPTICAS
- APLICACIONES DE LAS MATRICES POR BLOQUES A LOS CRITOSISTEMAS DE CIFRADO EN FLUJO.
- REBELDÍA, AMISTAD Y EROTISMO EN BALTASAR GRACIÁN. APROXIMACIÓN A UN PENSAMIENTO Y UN MUNDO CIFRADOS
- SÍNTESIS DEL MODELO DE AUTÓMATAS CELULARES EN PROTOCOLOS CRIPTOGRÁFICOS DE CIFRADO EN FLUJO Y ORIENTADO A REDES DE FEISTEL
- ESTUDIOS SOBRE EL DESCIFRADO DEL CÓDIGO ESTRUCTURAL DE LAS PROTEÍNAS. PROPENSIONES ESTADÍSTICAS E INFORMACIÓN MULTIRRESIDUAL
- METODOLOGÍA DE DISEÑO DE CIFRADORES DE BLOQUES CON DETECCIÓN CONCURRENTENTE DE FALLOS.
- CONTRIBUCIÓN AL DISEÑO Y EVALUACIÓN DE CIFRADORES EN FLUJO PARA COMUNICACIONES SEGURAS.

[ver Selección](#) [Modificar Consulta](#) [Nueva Consulta](#)

versión 4.1.10
© Ministerio de Educación, Cultura y Deporte
[Aviso legal](#) | [Accesibilidad](#)

TESEO: Búsqueda por "*cifrado*" sin otros términos: 4 tesis (marcadas).



Resumen tesis doctorales en criptografía

Tesis con “criptogra” en su título	24
Tesis con “cryptogra” en su título	9
Tesis con “esteganogra” en su título	2
Tesis con “steganography” en su título	2
Tesis con “criptolog” en su título	2
Tesis con “criptoanálisis” en su título	5
Tesis con solo “cifrado” en su título	4
Número total de tesis en TESEO	48

Búsquedas por temas de criptografía realizadas en TESEO.

- Posiblemente haya alguna(s) más. En *números redondos*: 50.
- Un número muy interesante... ¿es alto o bajo?
- ¿Qué relación guarda este número con las tesis doctorales que se han leído en seguridad informática y seguridad de la información?



Resumen tesis doctorales en seguridad sin criptografía

Tesis con "autenticación" en su título	15
Tesis con "seguridad en redes" en su título	7
Tesis con "detección de intrusos" en su título	7
Tesis con "seguridad de la información" en su título	6
Tesis con "seguridad informática" en su título	4
Tesis con "ciberseguridad" en su título	4
Tesis con "malware" en su título	3
Tesis con "biometría" en su título	3
Tesis con "firewall" en su título	2
Tesis con "secret sharing" en su título	2
Tesis con "digital signature" en su título	2
Tesis con "secretos" en su título	2
Tesis con "sistema operativo" en su título	1
Tesis con "protección de la información" en su título	1
Tesis con "certificados digitales" en su título	1
Tesis con "autoridades de certificación" en su título	1
Número total de tesis en TESEO	61

Búsquedas por temas de seguridad realizadas en TESEO.

Posiblemente haya alguna(s) más.

Pero, **cero** éxito al buscar por:

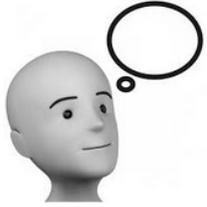
- Seguridad en sistemas operativos
- Seguridad en bases de datos
- Computer security
- Seguridad en Windows
- Seguridad en Linux
- Infraestructuras críticas
- Virus informáticos
- Ingeniería inversa
- Hacking (seguridad)





Entonces en I+D+i, ¿nos importa o no la criptografía?

- De 109 tesis doctorales leídas, 48 son sobre temas de criptografía.
- Casi la mitad de tesis doctorales (44%) son sobre temas directamente relacionados de la criptografía. Parece que sí importa.
- Pero hay algo que parece no cuadrar con la I+D+i en seguridad informática y seguridad de la información en España visto antes.
- De 104 grupos, menos del 30% declara interés por la criptografía.
- Y el 44% es un valor muy superior al peso que la criptografía en realidad debería tener en la I+D+i en España. Es prácticamente el triple.
- ¿Por qué no cuadran entonces los datos?
- Intentaremos encontrar alguna justificación... y sacar conclusiones.



Pensamientos en voz alta

- Aunque en España existen más bien pocos proyectos de investigación dedicados solamente a la criptografía, sí existe por el contrario un número muy alto de tesis doctorales en este campo. Tal vez excesivo.
- Posiblemente esto se deba al hecho de que la criptografía, sus algoritmos, su complejidad algorítmica, sus entornos matemáticos, nuevos sistemas de cifra, PKIs, protocolos, etc., sean temas de gran interés por parte de los doctorandos y también de los directores de tesis (*promoción por JCR*).
- Existen muchos congresos y publicaciones donde la criptografía juega un papel muy importante, lo que viene a justificar el interés por investigadores y directores, al tener un amplio abanico de opciones en donde poder publicar sus trabajos técnicos.
- ¿No se reconocen o no se pueden publicar otro tipo de trabajos?





Conclusiones con datos de octubre de 2017

- De los 104 grupos de investigación en seguridad de la información que hay en España, en 31 de ellos (el 29,8%) la criptografía aparece como una de sus líneas de interés y sólo 8 grupos (un 7,7%) la llevan en su nombre.
- La cantidad de proyectos de investigación desarrollados y que tengan su enfoque principal en la criptografía, posiblemente no llegue a 20. Se desconoce el número de proyectos de los 104 grupos, pero será muy alto.
- El número de tesis doctorales en las que dentro de su título aparecen palabras directamente relacionadas con la criptografía es igual a 48.
- El número de tesis doctorales en las que dentro de su título aparecen palabras o un conjunto de palabras relacionadas con la seguridad de la información, pero NO específicamente criptografía o esteganografía, es igual a 61.

Que cada un@ saque sus conclusiones



Referencias

- RENIC (2017). Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad, de la Red de Excelencia Nacional de Investigación en Ciberseguridad.
https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/201701_catalogo.pdf
- RENIC (2017) Infografía del Mapa I+D+I en Ciberseguridad en España on-line.
https://www.renic.es/sites/default/files/201701_RENIC_catalogo_infografia_0.pdf
- Base de datos de Tesis Doctorales (TESEO), consulta realizada el 20/09/17
<https://www.educacion.gob.es/teseo/irGestionarConsulta.do>
- Integrating Security into the Curriculum, Computer IEEE, 1998. Cynthia E. Irvine, Shiu-Kai Chin, Deborah Frincke.
<https://surface.syr.edu/cgi/viewcontent.cgi?article=1083&context=eecs>
- Introducción de las enseñanzas de Seguridad informática en los Planes de Estudio de las Ingenierías del Siglo XXI, JENUI 2001, Jorge Ramió.
<http://bioinfo.uib.es/~joemiro/aenui/procJenui/ProcWeb/actas2001/raint73.pdf>