BOLETÍN ELECTRÓNICO

e-LECTURAS DE VERANO: INGENIER@S A LA BOLOÑESA

ENGLISH ZONE.

RAMA DE ESTUDIANTES IEEE-UNED

Septiembre-2008 (BOLETÍN Nº 10)

RAMA DE ESTUDIANTES IEEE-UNED
1-Septiembre-2008

COORDINADOR Y EDITOR:

Gloria Murillo (gmcordero@indra.es)
Sergio Martín (sergio.martin@ieee.org)

REVISIÓN:

Manuel Castro
Eugenio López
Gloria Murillo

DISEÑO PORTADA:

Gloria Murillo

AUTORES

Emilio Olías, José Antonio Cámara, Guillermo F. Lafuente, Germán Lado, Germán Carro, Gloria Murillo.

EN COLABORACIÓN CON EL CAPÍTULO ESPAÑOL DEL IEEE EDUCATION SOCIETY

AGRADECIMIENTOS

“Agradecemos a nuestro Catedrático de Tecnología Electrónica y profesor consejero de la Rama, Manuel Castro, todo el tiempo y la dedicación que nos presta, así como, el habernos dado la posibilidad de colaborar con el Capítulo Español del IEEE Education Society para la elaboración del mismo. Agradecemos a todos los autores, y a aquellos que han colaborado para hacer posible este Boletín Electrónico”.

ÍNDICE

CONTENIDO **PÁGINAS**

SUMARIO

Para comenzar el boletín electrónico nº 10, se presenta como en ediciones anteriores un primer apartado de **Información** general de la Rama y **URLs** de interés general propuestas por miembros de la rama.

El primer artículo de esta edición del boletín está escrito por Emilio Olías Ruiz, Director en funciones de la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, titulado "**e-Lecturas de Verano: Ingenier@s a la Boloñesa**" trata de arrojar un poco de luz sobre los nuevos planes de estudio de Bolonia que entrarán en funcionamiento en breve.

El artículo escrito por José Antonio Cámara sobre la "**Teoría de Juegos**" la cual se puede emplear en numerosos problemas cotidianos. En el presente artículo se intenta reflejar matemáticamente con soluciones visuales en MATLAB el problema del prisionero, o la elección cooperar o no para llegar a un final más económico para los dos jugadores. Este trabajo es claramente práctico, dónde se simulará un comportamiento aleatorio en contra de un modelo determinista que depende del anterior.

A continuación Guillermo Lafuente nos habla sobre las "**Redes Wi-MAX**". Esta tecnología es una de las innovaciones que han surgido en los últimos años sobre comunicaciones inalámbricas que más expectación está levantando. Esto es así, porque se trata de una tecnología que trata de proporcionar acceso de banda ancha inalámbrico para el acceso de última milla (o bucle de abonado: tramo existente entre la última central del operador de telecomunicaciones y la casa del usuario). Con esto se convierte en un excelente complemento para las redes Wi-Fi y en un competidor de las tecnologías 3G.

Seguidamente nos encontramos con el artículo "**Criptografía el poder de lo oculto**" escrito por Germán Carro. El conocimiento de ciertas informaciones nos lleva a la obligación de protegerla de observadores externos, y la importancia de esta protección es lo que nos ha llevado a la criptografía. En el artículo se nos introduce a la historia y las diferentes técnicas de criptografías desde sus orígenes hasta la actualidad, y como el mayor avance de esta ha venido de la mano del desarrollo de los ordenadores.

"**Modelos de Seguridad para Redes WIFI**" es el primero de los dos artículos de los escritos por Germán Lado sobre este tema, publicándose el siguiente artículo en el próximo Boletín. En este primer artículo se explica el funcionamiento de los principales modelos de seguridad en rede WIFI para, en el próximo exponer sus vulnerabilidades y poner en práctica lo expuesto hasta el momento.

"**English Zone**" es una nueva sección recientemente creada en anteriores Boletines con el objetivo de tratar de refrescar ciertos aspectos de la lengua

inglesa que hemos olvidado o así como adquirir nuevos conocimientos. Este artículo sigue en la línea del publicado en la anterior edición. En el cual se proponen una serie de actividades con sus correspondientes soluciones las cuales nos ayudaran a mejorar ciertos aspectos de la gramática. Tales como, una serie de “rompecabezas” en los que además de comprender la historia que nos están contando debemos de aplicar la lógica para resolver las situaciones que se nos plantean.

INFORMACIÓN Y URLS

A continuación se describen las actividades que se desarrollaran en los próximos meses en la rama, algunas de ellas surgidas a raíz del CNR 08 y otras ya planeadas con antelación por la Junta Directiva de la rama:

1. Seguir con el aumento en el número de miembros mediante la repetición de los talleres y cursos realizados anteriormente y la realización de otros nuevos:
   - Taller de Linux
   - Seminario/charla de Second Life
   - Taller de programación en .NET
2. Intentar llevar estas actividades a otros centros de la geografía española para continuar con nuestra expansión. La colaboración con el resto de ramas activas puede ser clave para conseguirlo.
3. Utilización de http://www.labloguera.net/ para la realización de discusiones técnicas. La idea es proponer un tema de moda y polémico para discutir sobre él durante un período que se fijará al inicio del debate. Al finalizar, un moderador hará un informe final con las conclusiones obtenidas y éste se publicará en el siguiente número del boletín electrónico.
4. Continuar con la preparación de un robot para presentar a concurso.
5. Iniciar la búsqueda de contactos para la organización del "I concurso de robótica de la UNED".
6. Preparación de un grupo para presentarse al concurso IEEEXtremme '09.
7. Diseño de una nueva página web de la rama y presentación de la misma al concurso del R8.
8. Continuar con la publicación de nuestro boletín e intentar conseguir un ISBN para el mismo.
9. Intentar conseguir speakers para realizar conferencias y seminarios (la web http://www.ieee.org/r8sac e http://www.isbir.org/ puede ayudar a conseguirlos). El formato de la UPM de las Discussion Boards son un modelo interesante para atraer el interés de la gente.
10. Intentar enviar artículos a *IEEE Potentials*.
11. Intentar publicar el artículo del grupo distribuido y virtual de robótica en una revista con índice de impacto.
12. Adición de algún Chapter a la rama como podría ser GOLD.
13. Enviar al SBC a un representante de nuestra rama (la plaza pagada por IEEE España será para el presidente, el resto de personas que quieran acudir deberán de pagar el viaje, estancia y comidas).
14. Enviar un informe de la rama a *Examplary SB award* con los logros de la rama en el último año (posibilidad de lograr un premio)
15. Pedir en la web http://www.ieee.org/r8sac merchandising para la rama.
16. Organización de una reunión de la rama en A Coruña (búsqueda de patrocinadores para el evento).

17. Publicación de todos nuestros eventos en el RSS del aLF para que aparezcan en la página del IEEE España (se nos ha pedido que usemos más esta página para que todas las ramas podamos compartir nuestro recursos)

18. Se podría intentar colaborar con la universidad de Sevilla en la próxima edición de imaginática (http://imaginatica.eii.us.es/2009/)

19. Continuar con el uso de la plataforma aLF para nuestras actividades.

Guillermo Lafuente
Coordinador Actividades Generales

PROMOCIÓN DE LA DIRECTIVA DE LA RAMA DE ESTUDIANTES IEEE-UNED AÑO 2008

Sergio Martín: Presidente de la rama de estudiantes IEEE-UNED. Ingeniero Informático y estudiante de doctorado en el DIEEC. Actualmente trabaja en el Departamento de Electricidad, Electrónica y Automática en proyectos de investigación. smartin@ieec.uned.es

Elio Sancristobal. Vicepresidente de la Rama de Estudiantes del IEEE-UNED. Ingeniero Informático y estudiante de Doctorado en el DIEEC de la ETSII de la UNED. Actualmente trabaja en el CSI de la UNED. En años anteriores ha colaborado con la junta directiva como secretario elio@ieec.uned.es>

Rosario Gil. Secretaria y Tesorera de la Rama de Estudiantes del IEEE-UNED, Ingeniera de Telecomunicaciones, actualmente trabaja como Becaria de Investigación en el DIEEC de la ETSII de la UNED. rgil@ieec.uned.es

Gloria Murillo. .Coordinadora del Comité del Boletín Electrónico. Ingeniero Técnico en Telecomunicaciones, y estudiante de Ingeniería Industrial por la UNED. En estos momentos trabaja en Indra. gmcordero@indra.es

Ángel Iglesias. .Responsable del Comité de Socios y Bienvenida. Estudiante de Informática de Gestión por la UNED. aiglesisascela@hotmail.com

Germán Carro. Coordinador del Comité de Actividades Generales. Estudiante de Ingeniería Técnica en Informática de Sistemas por la UNED. germancf@eresmas.net

Francisco Javier Magán. Responsable del Comité de Calidad Interna de la rama. Ingeniero Técnico de Telecomunicación, especialidad en Sistemas Electrónicos, por a Universidad Politécnica de Madrid (UPM). En la actualidad está cursando el segundo ciclo de Ingeniería Industrial, intensificación en Electrónica y Automática, y participa en proyectos de investigación en el DIEEC de la ETSII de la UNED. fjmagan@ieee.org

Igor Chávez. Técnico en Electrónica en la National Schools. Estudiante de Ingeniería Electrónica en la Pontificia Universidad Católica del Perú (PUCP). Actualmente alumno de Ingeniería Técnica Industrial especialidad Electrónica Industrial de la UNED. Miembro de la Rama Estudiantil del IEEE-UNED y del Grupo de Robótica del mismo. igorchavez@ieee.org

Alejandro Díaz. Antiguo Coordinador del Boletín Electrónico de la Rama de Estudiantes del IEEE-UNED, a partir de ahora colaborará con el resto de la junta directiva, especialmente con el Comité de Actividades Generales. Ingeniero Industrial por la ETSII de la UNED, y estudiante de doctorado del DIEEC de la escuela. Trabaja en General de Servicios Integrales (Grupo Acciona) en instalaciones eléctricas. adiazh@ieee.org

Manuel Castro. Profesor Consejero de la Rama de Estudiantes del IEEE-UNED. Catedrático de Tecnología Electrónica. Miembro Señor del IEEE y actual presidente del capítulo Español de la IEEE Education Society creada en España. mcastro@ieec.uned.es

Eugenio López. Mentor de la rama de estudiantes IEEE-UNED, y antiguo presidente de la rama de Estudiantes del IEEE-UNED. Ingeniero Industrial por ETSII de la UNED, y estudiante de Doctorado en el DIEEC de la Escuela. Actualmente trabaja en Niedax Kleinhuis. elopez@ieec.uned.es

e-LECTURAS DE VERANO: INGENIER@S A LA BOLOÑESA

Por: *Emilio Olías Ruiz*

Catedrático de Tecnología Electrónica
Director en funciones de la Escuela Politécnica Superior
Universidad Carlos III de Madrid.
E-mail: emilio.olias@uc3m.es

1. Presentación

Cuando mi buen amigo, el Prof. Dr. Manuel Castro Gil, me propuso escribir este artículo no fui consciente de la fecha en que estaba prevista su publicación. Sin pensarlo mucho y sin dudarlo, le dije que sí, que contara con esta modesta colaboración. Me pudieron más la amistad y los años de convivencia y trabajo juntos, cuando estudiábamos ingeniería industrial y cuando estábamos preparando nuestros respectivos trabajos de tesis doctoral y la excelente relación personal y profesional que mantenemos.

Ahora me doy cuenta de que estamos a finales de julio de 2008, que hace mucho calor y que si se quiere captar la atención de estudiantes de ingeniería sobre la situación de cara a la convergencia de los estudios con Europa hay que hacerlo en clave de verano, suponiendo al estudiante leyendo este documento cerca de una playa, una piscina, una montaña o, simplemente, que esté tratando de descansar durante el tiempo de sus vacaciones estivales, relajarse de un seguro duro esfuerzo durante el curso previo y cargar las pilas para el curso siguiente (o preparando sus exámenes de septiembre, que de todo habrá).

Por eso he buscado un título para este artículo que pretende ser relajante en sí mismo, captar la atención de lector@s curios@s y transmitir una reflexión optimista sobre la base de la experiencia llevada a cabo en la Escuela Politécnica Superior, de la Universidad Carlos III de Madrid, desde el pasado mes de julio de 2007, para tratar de cambiar todos los planes de estudios y hacerlos compatibles con la regulación del Gobierno de España que fue publicada en el pasado mes de octubre[1].

[1] *REAL DECRETO 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales. Ministerio de Educación y Ciencia*

2. Antecedentes

Quienes quieran conocer con detalle de dónde viene esto del Espacio Europeo de Educación Superior, EEES, oirán hablar de una ciudad italiana, cuna del saber universitario, Bolonia[2], que representa la primera cita de responsables educativos de la Unión Europea para tratar de alcanzar un acuerdo en materia de educación universitaria, que pudiera permitir una mayor movilidad de estudiantes y profesores entre los centros universitarios de Europa y una más fácil identificación de los títulos universitarios para poder desarrollar profesionalmente las habilidades que cada uno de ellos pudiera proporcionar, con un reconocimiento fácil, casi automático, de los contenidos estudiados durante sus carreras universitarias en cualquier país de la Unión Europea.

El horizonte de la Declaración de Bolonia parecía, cuando se firmó en 1999, muy lejano, aunque la fecha límite para proceder a la adaptación, ya fijada en aquellos documentos y mantenida en las posteriores reuniones de Ministr@s de Educación Universitaria, está cada vez más cerca. Se trata del año 2010.

Por tanto, desde Bolonia hasta hoy, 2008, han pasado ya nueve años y quedan sólo dos para cumplir con lo pactado y acordado (y también firmado).

Pero hay una pregunta clave: ¿cómo ven los estudiantes universitarios actuales y potenciales todo este largo camino recorrido hasta aquí?

Haciendo una clasificación de la población universitaria estudiantil respecto a esta importante transformación, podrían distinguirse tres grandes grupos, que trataré, no sin cierto riesgo, de ordenar de menor a mayor importancia.

El primer grupo lo constituyen los estudiantes anti-Bolonia, que, salvo en determinadas zonas geográficas, como Cataluña, comunidad autónoma en la que han hecho sentir su voz, llegando a provocarse disturbios de orden público en algunas universidades, parecen ser una minoría escasa, con también escaso poder de convocatoria y que, aunque generalizar siempre tiene sus inconvenientes, están creando un estado de “confinión” (confusión en la opinión), en base a argumentos muy poco sólidos y que tratan de acudir a la vieja estrategia del terror frente al cambio, que todos los cambios, por su propia naturaleza, incorporan,. A este grupo se han sumado algunos profesores universitarios, muy pocos, a decir verdad y puede que también se hayan utilizado estas voces discordantes como amplificadoras de la opinión de sectores muy conservadores, que no quieren (¡antes muertos!) cambiar nada de la realidad universitaria en la que viven.

El segundo grupo lo constituyen los pasotas, los escépticos, los “pasamos de todo”, que no tienen una preocupación suficiente sobre lo que un proceso de

[2] La expresión Espacio Europeo de Educación Superior, que actualmente se utiliza con generalidad en los documentos oficiales y en los estudios sobre la temática, tiene su origen en la Declaración de Bolonia, firmada en 1999 por los responsables de educación universitaria de la Unión Europea.

estas características supone, de cara a su propio futuro y, mucho más importante, de cara al futuro de la sociedad en la que se desarrollan como personas y en la que tendrán la oportunidad de actuar como profesionales en diferentes ámbitos, de acuerdo con su formación universitaria. Este grupo es algo más numeroso que el anterior, algo más influyente y requiere una acción de motivación para implicarles y que deseen participar activamente en el proceso. Normalmente no son estudiantes que pudiésemos clasificar como molestos o conflictivos. Sólo están de paso. Quieren terminar sus estudios universitarios y que no les compliquen la vida, que bastante complicada la tienen ya.

En el tercer grupo de estudiantes, los más numerosos, incluiré a la mayoría de los estudiantes universitarios y potenciales estudiantes universitarios y a la práctica totalidad de los estudiantes de ingeniería. ¿Por qué menciono expresamente a los estudiantes de ingeniería? Porque ellos perciben un cambio concreto, dado que el marco establecido por el RD 1393/2007 establece una duración, para cada uno de los estudios de grado, de cuatro años, frente a los cinco o tres que ofrecen actualmente la mayoría de las universidades que imparten, respectivamente, titulaciones de ingeniería o de ingeniería técnica. En los estudios relativos a Ciencias Sociales y Jurídicas (Derecho, Económicas, Empresariales, Estadística, …) o de Humanidades (Biblioteconomía, Periodismo, …), ya existe, en muchas universidades, una oferta clara con una duración prevista de los estudios en cuatro años, por lo que el cambio no es percibido por esta población estudiantil con la misma intensidad que puede percibirlo un estudiante o potencial estudiante de ingeniería.

También ha habido un movimiento social de cierta presión, promovido desde los intereses legítimos de colegios y asociaciones profesionales de ingenieros e ingenieros técnicos, que veían (y en algunos casos todavía ven) modificaciones de cierto riesgo en su *statu quo* de aplicarse el cambio. Afortunadamente, parece que la sensatez e inteligencia de algunas personas, participantes activos en este proceso, como Manuel Acero, anterior Decano del Colegio de Ingenieros Industriales de Madrid (COIIM) y Presidente de la Asociación de Ingenieros Industriales de Madrid (AIM) y hoy Presidente del Instituto de la Ingeniería de España, que engloba la representación de todas las Asociaciones de Ingeniería de España, para todas las ramas y en todo el territorio nacional, ha permitido un acercamiento de posturas e intereses y parece estar cada vez más cerca el día en que un documento legislativo atienda de forma explícita a los graduados en cada ingeniería, estableciendo sus competencias, derechos y limitaciones de sus respectivos títulos y evitando que la dialéctica de conflicto permanente, planteada por algunos sectores inmovilistas, que cada vez ven más reducido el eco de sus proclamas catastrofistas, suponga un retraso irreparable para la entrada con éxito de España en el EEES.

El riesgo real, en mi opinión, para España, sería, una vez más, la pérdida de una oportunidad de subirse al tren de la Educación Universitaria con mayúsculas, de no atender como se merece todo este proceso de transformación, cuando tenemos una juventud muy bien preparada y una

sociedad suficientemente bien alimentada (en todos los sentidos) para abordar este proceso de cambio con garantías de éxito.

3. Presente y Futuro de los estudios de ingeniería

En este próximo curso 2008/2009, apenas un 10% de los planes de estudio universitarios existentes en España estarán adaptados al EEES. Los que hemos vivido la emoción e intensidad del proceso de cambio recomendamos a tod@s que visiten nuestra página web para ampliar información y también estamos dispuestos a ayudar a quienes tengan dudas sobre el proceso[3].

El colectivo de los escépticos y los radicales que no aceptan ningún tipo de diálogo se está quedando cada vez más reducido. Y, por otra parte, cada vez son más los que ven el cambio como una necesidad y lo abordan con ilusión, haciendo acopio de las energías necesarias para afrontar el reto con las máximas garantías de éxito.

Quienes hemos tenido la oportunidad de trabajar en una universidad pionera, la Universidad Carlos III de Madrid, bajo el mandato de un Rector doctor ingeniero industrial, Daniel Peña, y el entusiasmo y paso firme de una Vicerrectora de Grado como Isabel Gutiérrez, estamos satisfechos del trabajo realizado, conscientes de lo importante de su puesta en marcha y del papel tan fundamental que tendrán los estudiantes en este proceso. Implantamos un nuevo modelo de enseñanza que va mucho más allá de la definición excesivamente simple de la duración de los grados en cuatro años. Hay nuevas metodologías docentes, nuevos métodos de evaluación, nuevos horarios y muchas cosas más.

Todo ello con la intención de alcanzar unos niveles de producción académica y también científica e investigadora del máximo nivel de excelencia, para que nuestros titulados puedan competir con el resto de europeos de tú a tú, sin complejos y con una formación sólida y bien valorada por la sociedad, que finalmente será la encargada de emplear a estos nuevos titulados y de valorar el trabajo realizado con ellos y por ellos.

No quisiera dejar de mencionar lo importante que resulta para todos el proceso de internacionalización. La enseñanza en idioma inglés, cada vez más generalizada, requiere de un sobreesfuerzo que muchas universidades están afrontando sin ningún apoyo económico adicional. Cuando pensamos en estudios preuniversitarios (bachillerato o ESO en España) asumimos perfectamente que si alguien quiere enseñanza en una lengua distinta de las que se reconocen como oficiales en España ha de pagar por ello un plus y así ocurre habitualmente cuando se recibe enseñanza en un colegio inglés o americano y también cuando se recibe en un colegio francés o alemán. Sin embargo, cuando en la universidad se hace un esfuerzo por impartir enseñanza en inglés, con una calidad contrastada y contrastable, no hay apenas, por parte

[3] www.uc3m.es o enviar un correo eletrónico a emilio.olias@uc3m.es si están interesados en lanzar alguna pregunta o consultar alguna duda.

de los organismos encargados de la financiación de la enseñanza, una sensibilidad respecto a estos temas y me temo que sólo con la buena voluntad de los dirigentes universitarios y de los profesores no será suficiente para desarrollar este proceso con éxito. Se requiere una mayor atención a este aspecto y no sólo desde el punto de vista presupuestario, sino también en cuanto a visibilidad del trabajo, publicidad y buenas prácticas, para que estudiar en España en lengua inglesa se perciba por parte de profesores y potenciales alumnos que no sean españoles, como una ventaja competitiva importante de cara a realizar su elección sobre dónde y qué estudiar. De no hacerse así, podemos caer en una situación que alimente sólo a intereses internos, autóctonos, sin atraer a estudiantes extranjeros a las propuestas de grado y postgrado que se desarrollen.

Por último, a los futuros estudiantes que quieran estudiar ingeniería, debiéramos plantearles una cuestión. ¿Qué es mejor: elegir una titulación adaptada ya a la convergencia con el Espacio Europeo o elegir una titulación no adaptada? Habrá opiniones para todos los gustos, unas más interesadas que otras, pero a poco que se sepa valorar la natural inteligencia de un joven potencial estudiante universitario, se reconocerán criterios para elegir adecuadamente. Hemos, sin duda, de dejarles elegir; es su vida, su futuro y su responsabilidad. Y nuestra obligación como profesores universitarios debería ser la de atenderles en sus dudas y contestar sus preguntas con la mayor claridad, para que, una vez dispongan de la información completa, puedan tomar correctamente sus decisiones.

Los que estudiamos con sistemas de enseñanza anteriores, el Prof. Manuel Castro y yo mismo, sin ir más lejos, deberemos adaptarnos a los nuevos tiempos, a los nuevos métodos y a las nuevas necesidades, para permitir que nuestra sociedad avance hacia un mayor nivel de desarrollo, que deberá atenderse como una necesidad colectiva, más allá de intereses estrictamente individuales.

Actuando de esta forma, podremos dar un valor añadido a la Educación Universitaria, más allá de planteamientos concretos. Se trata de una aptitud, que ha de ir acompañada de una actitud, mezcladas ambas de manera óptima, medida y adaptada a los distintos gustos y necesidades sociales; en un entorno abierto, de libre competencia, basada en la excelencia contrastable.

Y para terminar reflexionando sobre el éxito de la tarea, podremos decir que no depende únicamente de quienes podamos jugar un papel de promotores del cambio. El papel fundamental lo van a jugar los futuros estudiantes, porque Bolonia les coloca como auténticos protagonistas, definiéndoles como el centro del proceso educativo. De ellos, de vosotros, de todos, en definitiva, será el mérito del éxito. Buena suerte a tod@s.

Teoría de juegos

Por: *José Antonio Cámara Madrid*

Estudiante de Ingeniería Industrial.
Miembro de Student Branch IEEE – UNED.
E-mail: joseacamara@ieee.org

1. Introducción

A todo el mundo le sonará la teoría de juegos de la película, “Una mente maravillosa” en la cuál narran la vida de Nash, pero la teoría de juegos es algo más, se puede emplear en numerosos problemas cotidianos.

En el presente trabajo he intentado reflejar matemáticamente con soluciones visuales en MATLAB el problema del prisionero, o la elección cooperar o no para llegar a un final más económico para los dos jugadores. Este trabajo es claramente práctico, dónde se simulará un comportamiento aleatorio en contra de un modelo determinista que depende del anterior.

Normalmente, se supone que la matriz de beneficios/pérdidas es constante, pero qué pasaría si fuese aleatoria, se va a contraponer los resultados y se analizarán los resultados en las conclusiones, por lo tanto, el trabajo se resume a la exposición del problema (muy conocida en la literatura), un modelo de pesos constante, otro aleatorio y sacaré las conclusiones.

Considero que si se extrapola a otros campos tiene bastante aplicación práctica (por ejemplo en la automatización de industrias), robótica, dirección de operaciones.

2. Dilema del prisionero

Vamos a comenzar explicando un juego clásico, que es el dilema del prisionero, que es original de A. W. Tucker.

La mencionada historia es la siguiente. Dos prisioneros incomunicados en celdas individuales han cometido dos crímenes, uno leve y otro grave. Existen pruebas suficientes para que les condenen por el primero, pero no por el segundo, a menos que alguno confiese haberlo cometido. El fiscal visita a uno de los prisioneros y le dice: "Tengo una buena noticia y una mala noticia para usted. La buena noticia es que si ninguno de ustedes confiesa su grave crimen, sólo podremos condenarles a dos años por su primer crimen y si usted confiesa, yo convenceré al jurado de que es usted un hombre arrepentido y de que el perverso es su compañero, de modo que usted quedaría libre en un año y él permanecería en prisión 10 años. La mala noticia es que voy a hacerle la

misma oferta a su compañero". "¿Y que ocurriría si ambos confesásemos?", pregunta el prisionero. "Entonces no tendré razón para beneficiar a ninguno de ustedes, dejaré que la justicia tome su curso y, como el crimen es grave, estimo que les condenarán al menos a 8 años". Así, los prisioneros se encuentran ante el siguiente dilema:

		EL OTRO	
		confiesa	no confiesa
YO	confieso	8 años cada uno	1 año para mi 10 para el
	no confieso	10 años para mi 1 para el	2 años cada uno

FIGURA 1: DILEMA DEL PRISIONERO.

Cada uno piensa que sólo pueden pasar dos cosas: que el otro confiese o que no confiese. "Si confiesa, es mejor que yo también lo haga, porque de lo contrario me quedaré 10 años en la cárcel. Si no confiesa y yo sí, entonces podré beneficiarme de la oferta del fiscal y quedaré libre en un año". La conclusión es que haga lo que haga el otro, lo mejor es confesar. Ambos razonan de igual modo, con lo cual ambos confiesan y se quedan en la cárcel mucho más tiempo del que les habría tocado, si hubiesen cooperado entre sí y ninguno de los dos hubiese confesado.

Este es un juego de dos personas, pero podría darse entre *n* personas, por ejemplo, en el caso de una huelga, que puede entenderse como un *bien público* (* tragedia de los comunes). Cada trabajador puede pensar: "o bien hay bastantes trabajadores que vayan a la huelga y consiguen el objetivo de esta acción colectiva (por ejemplo, un ascenso salarial, una reducción de la jornada laboral o una mejora en las condiciones de trabajo), o bien esto no ocurre. En el primer caso, de todas formas voy a beneficiarme del éxito de la huelga, y si me quedo, puedo, además, seguir cobrando y quizá mejore mis relaciones con mis superiores. Y si los demás no van a la huelga, lo mejor es que yo tampoco vaya, porque estaré pagando en vano los costes de mi contribución a esta acción colectiva que va a fracasar".

El problema es que lo individualmente racional conduce al fracaso colectivo. Lo mismo puede ocurrir en el caso de muchas otras acciones colectivas (manifestaciones, revoluciones, guerras, votaciones, etc.) y en muchos otros contextos, por lo que este juego ha resultado útil en una gama muy amplia y variada de investigaciones en Ciencias Sociales.

3. Modelo del dilema con recompensas constantes

Una vez explicado y conocido el dilema, vamos a modelizarlo. Se ha realizado un modelo del dilema del prisionero con una matriz de recompensas, tal como se ve en el código.

El programa en MATLAB implementado es el siguiente:

```
n = 50;
while n > 1
ab1(n)=5;
ab2(n)=5;
ac1(n)=8;
ac2(n)=2;
bb1(n)=2;
bb2(n)=8;
bc1(n)=0;
bc2(n)=0:
```

Ahora generamos la estrategia de 1 que va a ser aleatoria.

```
x(n)=rand(1);

if x(n)<= 0,5
%fila 1
   y(n)= 0
else 0,5
%fila 2
y(n) = 1
end
```

Ahora generamos la estrategia de 2, que va a ser la de "tiquitaca"

```
if  n == 50
   z(n)=1
elseif y(n-1)==1
   z(n)=1
else
   z(n)=2
%fila 2
end
```

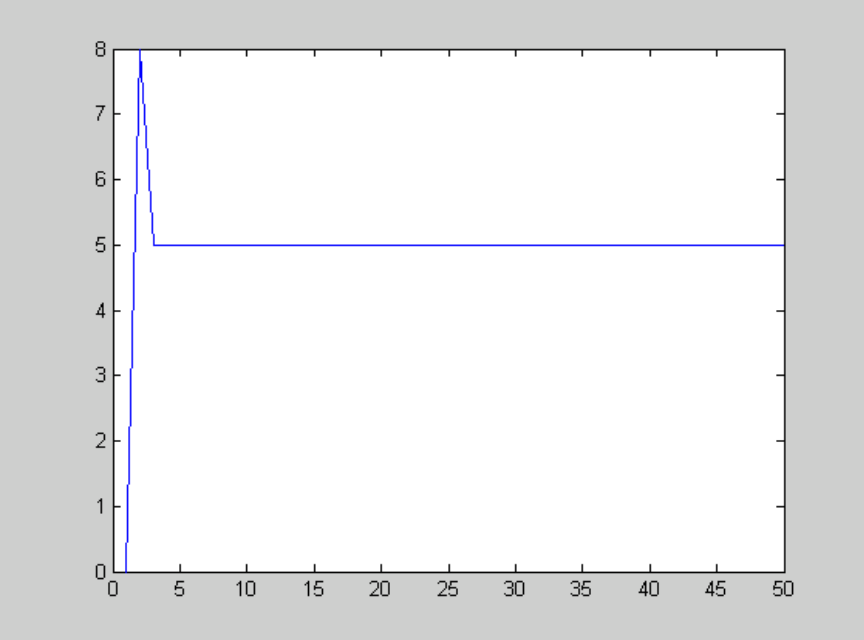
Visualizamos las ganancias de ambos y la diferencia

```
if y(n)==1 & z(n)==1
suma1(n)=ab1(n)
suma2(n)=ab2(n)
elseif y(n)==2 & z(n)==1
suma1(n)=bb1(n)
suma2(n)=bb2(n)
elseif y(n)==1 & z(n)==2
suma1(n)=ac1(n)
suma2(n)=ac2(n)
elseif y(n)==2 & z(n)==2
suma1(n)=bc1(n)
suma2(n)=bc2(n)
end

n = n - 1;
end
```

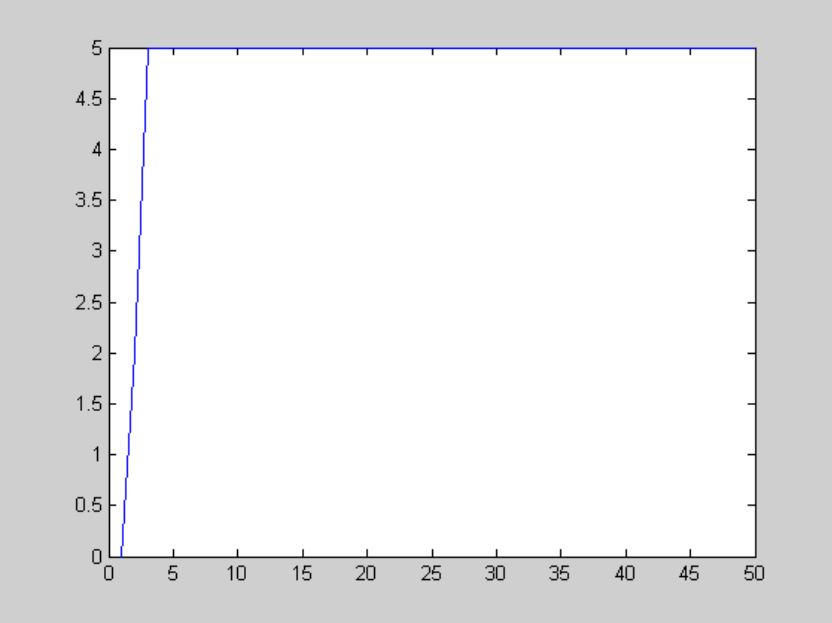
Calculamos el valor medio, para ver que media tiene y poder ver el resultado medio esperado:

```
mean(suma1)

ans =

    4.9600

>> mean(suma2)

ans =

    4.8400
```

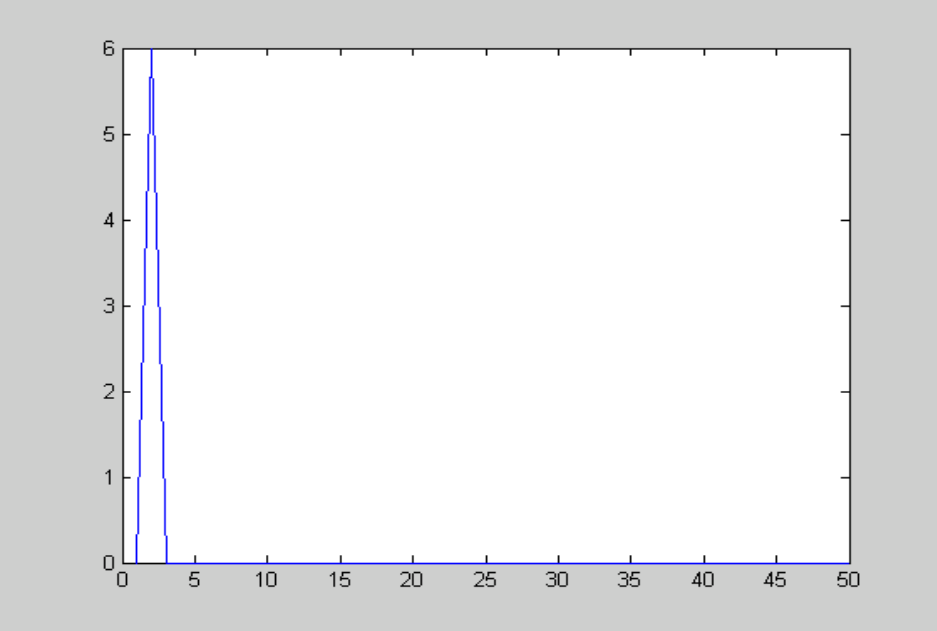
Veamos ahora el resultado de las 50 elecciones a ver qué conclusiones vemos:



Vemos al jugador 2:



Veamos ahora la diferencia entre ambos:



4. Modelo del dilema con recompensas aleatorias

Ahora suponemos que la matriz de pesos cambia con el tiempo, es más se debería de hacer muchas pruebas (ya que cada una sería distinta), para ver si podemos encontrar una estrategia mejor que la bautizada “tiquitaca” (una adaptación personal de tit-tat), ya que las recompensas son desconocidas, pero tienen una ponderación superior, me explico, ab1 es aleatorio, pero entre 0 a 5, es un detalle importante.

El programa en MATLAB implementado es el siguiente:

Código implementado en matlab:

```
n = 50;
while n > 1
ab1(n)=5*rand(1);
ab2(n)=5*rand(1);
ac1(n)=8*rand(1);
ac2(n)=2*rand(1);
bb1(n)=2*rand(1);
bb2(n)=8*rand(1);
bc1(n)=0;
bc2(n)=0;
```

Ahora generamos la estrategia de 1 que va a ser aleatoria.

```
x(n)=rand(1);

if x(n)<= 0,5
%fila 1
    y(n)= 0
else 0,5
%fila 2
y(n) = 1
end
```

Ahora generamoa ls estrategia de 2, que va a ser la de "tiquitaca"

```
if  n == 50
    z(n)=1
elseif y(n-1)==1
    z(n)=1
else
    z(n)=2
%fila 2
end
```

Visualizamos las ganancias de ambos y la diferencia aleatoria:

```
if y(n)==1 & z(n)==1
suma1(n)=ab1(n)
suma2(n)=ab2(n)
elseif y(n)==2 & z(n)==1
suma1(n)=bb1(n)
suma2(n)=bb2(n)
elseif y(n)==1 & z(n)==2
suma1(n)=ac1(n)
suma2(n)=ac2(n)
elseif y(n)==2 & z(n)==2
suma1(n)=bc1(n)
suma2(n)=bc2(n)
end
n = n - 1;
end
mean(suma1)
ans =

    2.7250
mean(suma2)

ans = 2.6290
```

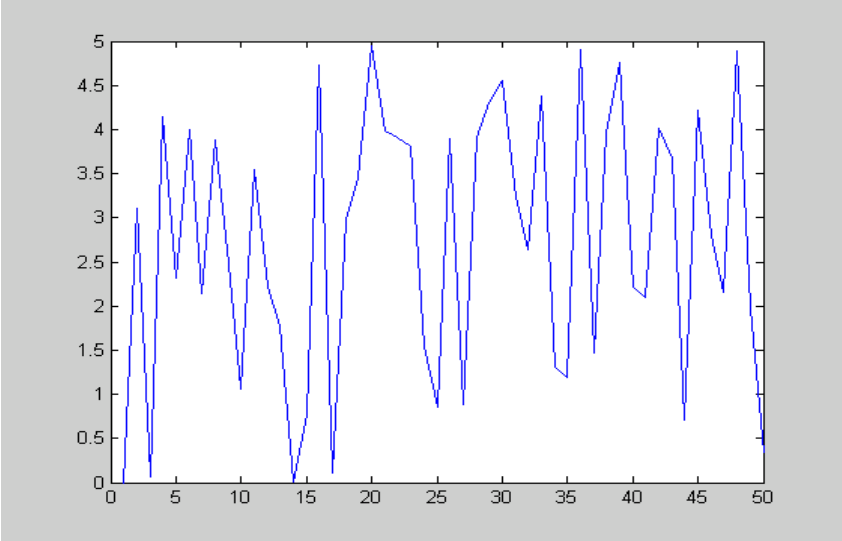


FIGURA 4: ESTRATEGIA ALEATORIA.

Variación de pesos en B según la estrategia "tiquitaca"

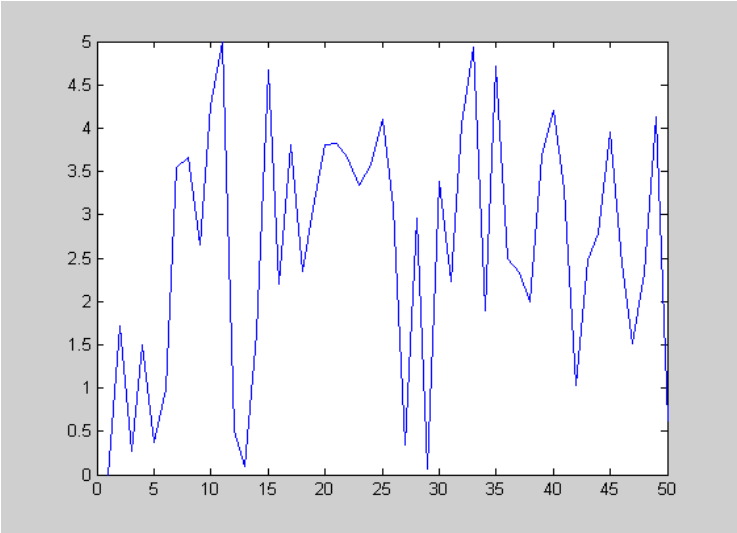


FIGURA 5: ESTRATEGIA TIQUITACA.

Diferencia de pesos x1-x2:

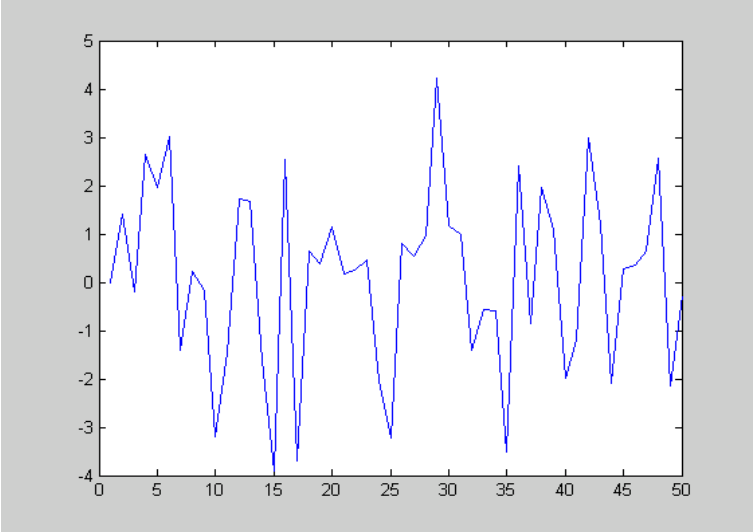


FIGURA 6: DIFERENCIA DE PESOS.

5. Conclusiones

Cómo se ha comprobado en los modelos anteriores, la cooperación en actuaciones aleatorias es indiferente, ya que el jugador no conoce realmente lo que le puede suceder, si fuesen los pesos años en la cárcel, los presos estarían menos tiempo en prisión y cooperarían más, cómo se ve en el primer estudio, no se cooperaría, sólo al principio y la estrategia del “tiquitaca” no cooperaría.

Espero que el trabajo sea del interés del lector, y no haber cometido algún error en la programación, la verdad es que me esperaba estos resultados. Se puede cambiar los algoritmos de los jugadores para ver qué estrategias son mejores, en este caso he cambiado las reglas del juego para ver que influencia tendría en las decisiones de los jugadores.

Redes Wi-MAX

Por: Guillermo Lafuente

Estudiante de Ingeniería Informática.
Miembro de Student Branch IEEE – UNED.
E-mail: guiye1984@hotmail.com

1. Introducción: ¿Qué es Wi-MAX?

Wi-MAX es el acrónimo de *Worldwide Interoperability for Microwave Access*. Esta tecnología es una de las innovaciones que han surgido en los últimos años sobre comunicaciones inalámbricas que más expectación está levantando. Esto es así, porque se trata de una tecnología que trata de proporcionar acceso de banda ancha inalámbrico para el acceso de última milla (o bucle de abonado: tramo existente entre la última central del operador de telecomunicaciones y la casa del usuario). Con esto se convierte en un excelente complemento para las redes Wi-Fi (cuyo objetivo es dar conectividad inalámbrica en redes LAN) y en un competidor de las tecnologías 3G.

Dentro del IEEE, Wi-MAX está especificada en el estándar 802.16 y fue publicado en el 2002. Sin embargo, es el Wi-MAX forum (http://www.wimaxforum.org/) el encargado de promover el estándar, de realizar los test de interoperabilidad y de proporcionar un proceso de certificación estándar para los equipos que empleen esta tecnología. El Wi-MAX forum es una industria independiente formada por más de 500 compañías, entre las que se pueden destacar, entre otras, a Fujitsu, Motorola y Siemens.

Resumiendo, Wi-MAX es una tecnología que proporciona conexión inalámbrica capaz de cubrir radios de varios kilómetros con precios muy competitivos. Las velocidades de transmisión que proporciona son elevadas (pueden alcanzar los 100 Mbps) y las antenas no necesitan visión directa. Todo esto lleva a que las empresas de telecomunicación puedan plantearse el uso de esta tecnología para dar acceso a Internet de banda ancha en zonas donde el despliegue del cableado supone costes excesivos, como por ejemplo, zonas rurales. Para las empresas también supone un hándicap, ya que los enlaces T1 o E1 suelen resultar caros, y el uso de Wi-MAX como sustituto de estos, puede suponer un coste hasta 10 veces menor.

2. Características de Wi-MAX

Wi-MAX es una tecnología que se basa en el uso de la tecnología RF (*Radio Frecuency*) con modulación OFDM (*Orthogonal Frequency Division*

Multiplexing), con 256 subportadoras, o con modulación OFDMA (*Orthogonal Frequency Division Multiple Access*) con 2.048 subportadoras.

Puede alcanzar velocidades de 100 Mbps en canales con anchos de banda de 28 MHz y de 70 Mbps operando en rangos de frecuencia más bajos. Además, facilita el uso tanto de bandas bajo licencia (10 a 66 GHz) y bandas de uso común libres de licencia (2,4 y 5 GHz).

Para permitir que cada fabricante pueda diferenciar sus productos de los de la competencia, la capa MAC (*Media Access Layer*) está definida de forma que soporte múltiples enlaces físicos.

Las medidas de seguridad que define el estándar contemplan el uso de medidas para la autenticación de usuarios y la encriptación de datos mediante los algoritmos RSA y triple DES.

Wi-MAX es una tecnología independiente de protocolo, esto quiere decir, que puede transportar tanto IP, como ATM, como Apple Talk, etc.

La tecnología Wi-MAX también se caracteriza por su gran escalabilidad, ya que permite la adición de nuevos canales fácilmente y maximiza las capacidades de las células. Además, el ya comentado uso de bandas de frecuencia en espectros tanto licenciados como no licenciados, proporciona anchos de banda flexibles.

3. Estándares Wi-MAX

802.16a: Especificación para los casos en los que no se dispone de visión directa entre transmisor y receptor. El rango de frecuencias que define esta entre 2 y 11 GHz. La velocidad que puede conseguir es de hasta 75 Mbps con anchos de canal que van de 1.5 a 20 MHz. El tamaño máximo de la celda ronda los 50 Km.

802.16b: Aporta calidad de servicio (QoS), por lo que permite la transmisión de voz y video. Usa las bandas de 5 y 6 GHz.

802.16d: Es una tecnología de acceso inalámbrico fijo. Utiliza OFDM para servir a múltiples usuarios. Se usa como competencia de redes DSL o líneas T1/E1. Usa las frecuencias de 2 a 66 GHz.

802.16e: Añade movilidad al estándar, permitiendo las comunicaciones a velocidades de hasta 120 Km/h. Utiliza OFDMA y puede servir a múltiples usuarios en forma simultánea asignando grupos de “tonos” a cada usuario. Puede alcanzar velocidades de 15 Mbps con canales de 5 MHz.

4. Wi-MAX en España

En España ya existen implementaciones experimentales y comerciales de redes Wi-MAX.

El primer ejemplo que nos encontramos, se trata del Ayuntamiento de Gavá, en Barcelona. Con esta medida, se trataba de dotar a la ciudad de conexión a Internet evitando los costes del cableado. También aprovecharon el despliegue de la red Wi-MAX para unir las cámaras de tráfico con el centro de control y unir los edificios municipales con VOIP (*Voice Over IP* – voz sobre IP).

En el País Vasco, la compañía Euskaltel ya tiene desplegadas redes de este tipo. Además, el gobierno vasco aprobó ayudas de financiación del 100% de los costes a quien lleve Wi-MAX a las zonas donde las líneas tradicionales de cobre no pueden llegar (o resulta excesivamente costoso hacerlo).

Más ejemplos de redes Wi-MAX implementadas en España se pueden encontrar en Cádiz, Sevilla, Alicante, Bullas (Murcia), etc.

5. Wi-Fi vs Wi-MAX ¿son competencia?

Cuando se diseñó Wi-Fi, la idea era dar cobertura a redes de área local (LAN). Por ello, el estándar sólo recoge coberturas de unos 100 m (aunque las nuevas revisiones del estándar tratan de ampliar estos radios de acción). Debido a estas limitaciones, serían necesarios un alto número de AP's para cubrir zonas extensas como podría ser una ciudad entera. También hay que tener en cuenta la cantidad de usuarios que cada AP es capaz de soportar, ya que el uso de CSMA/CA en el estándar Wi-Fi, hace que se desperdicie mucho ancho de banda para evitar las colisiones, y un número alto de usuarios (más de 20 personas) degradan en exceso el uso de la red. Todas estas consideraciones hacen que el uso adecuado de las redes Wi-Fi quede limitado a redes LAN.

Wi-MAX, por el contrario, nació con intención de convertirse en una solución de última milla, y por tanto, está diseñada para soportar a grandes cantidades de usuarios en distancias largas. Las redes Wi-MAX son capaces de transportar paquetes IP, pero se contempló como un estándar independiente de protocolo, y esto le permite soportar servicios conmutados como ATM y Frame Relay. Las coberturas que soporta una antena Wi-MAX es de alrededor de 50 km y proporciona un ancho de banda mayor que Wi-Fi. Las características de este protocolo lo hacen adecuado para soluciones MAN o WAN.

Resumiendo, estas dos tecnologías no suponen una competencia entre ellas, si no que son complementarias. Wi-Fi estará destinada a cubrir el acceso de usuario final, dando cobertura a redes LAN, mientras que Wi-MAX, proporcionará un acceso inalámbrico de última milla, permitiendo a los ISP dar servicios de Internet sin necesidad de cablear las ciudades.

En la figura 1 se ve que las antenas Wi-MAX formarán una red WAN que cubrirá la ciudad y proporcionarán cobertura a todo el área metropolitana. En cada casa podrá haber un AP que proporcione la conectividad inalámbrica (red LAN).

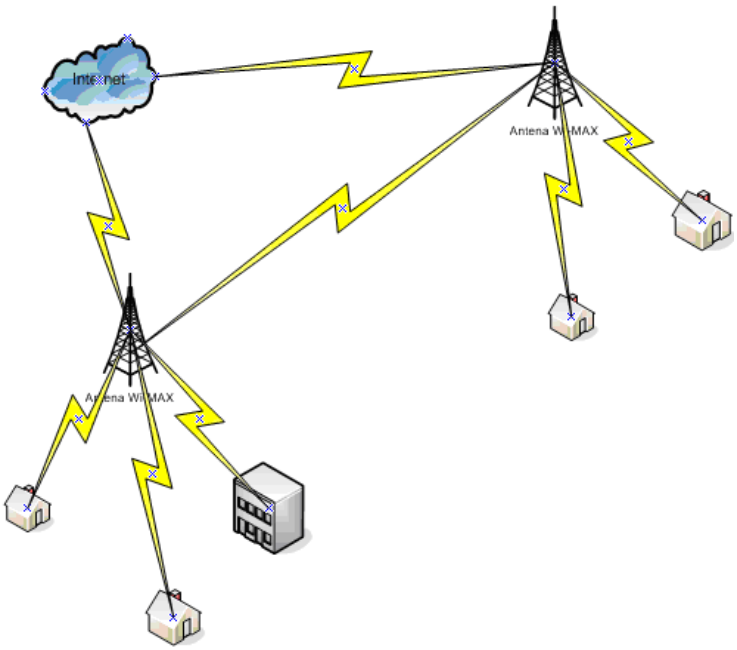


FIGURA 1. Red WAN de antenas Wi-MAX.

6. Wi-MAX: rival de UMTS

Como se apuntó en el punto anterior, Wi-MAX no compite con Wi-Fi para hacerse con una cuota de mercado. Entonces, ¿Quién es su rival? Para encontrarlo tenemos que mirar al padre de las comunicaciones inalámbricas: la telefonía móvil. Uno de los servicios que han empezado a ofrecer en los últimos años las operadoras de telefonía móvil es el acceso a Internet, especialmente para aplicaciones multimedia en la que los anchos de banda de descarga necesarios son más exigentes. Esto ha sido posible gracias a lo que se ha conocido como la tecnología 3G y que consiste en el uso de UMTS, lo cual requiere cambios en las antiguas antenas GSM.

Wi-MAX se puede convertir en un serio rival para la red UMTS, ya que esta, se está desplegando con cierta lentitud y aporta algunos problemas técnicos, en los que cabe destacar que la señal no es capaz de traspasar el hormigón y requiere de repetidores en el interior de los edificios. Wi-MAX rompe este inconveniente por ser capaz de trabajar con frecuencias inferiores a 11 GHz, ya que no se ven tan alteradas por muros o por las condiciones climáticas. También es de considerar la diferencia en el ancho de banda, ya que Wi-MAX es capaz de ofrecer velocidades de 100 Mbps, mientras que UMTS se queda en 14 Mbps.

A pesar de lo anterior, hay que observar que las operadoras han hecho un gran desembolso para desplegar la red 3G, y no están dispuestas a dejarse sobrepasar por Wi-MAX hasta haber recuperado toda esa inversión. Por ello, ya ha nacido la evolución de la red 3G denominada Súper 3G, capaz de ofrecer anchos de banda 10 veces superiores que su predecesora. Sin embargo, esto no va a frenar la inminente expansión de Wi-MAX, ya que cuenta con el apoyo de empresas como Cisco Systems, Intel, Fujitsu, Motorola, etc. De estas compañías, merece especialmente el caso de Intel, ya que está trabajando

para lanzar chips que incluyan Wi-MAX. Hay que tener en cuenta, que una producción en masa de chips con Wi-MAX haría bajar su precio y lo harían mucho más asequible.

Del párrafo anterior, se puede sacar la siguiente conclusión: las operadoras de telefonía móvil no están interesadas en el despliegue de Wi-MAX ya que les interesa amortizar el despliegue de la red 3G. Esto va a hacer que Wi-MAX no pueda competir con UMTS en cuanto a movilidad se refiere, ya que es difícil que llegue a cubrir la totalidad del territorio, al menos, a corto plazo. Por otro lado, en las áreas metropolitanas, sí que será un serio competidor gracias a la gran capacidad de las antenas Wi-MAX. Debido a esto, se pueden encontrar comentarios acerca de que los competidores reales de Wi-MAX son las tecnologías cableadas de banda ancha (cabe y DSL).

7. Seguridad en redes Wi-MAX

Uno de los principales lastres que han frenado la expansión de las redes inalámbricas ha sido la preocupación por la seguridad que estas son capaces de ofrecer. La seguridad que ofrece el estándar IEEE 802.11 (Wi-Fi) es vulnerable y es un aspecto que siempre ha preocupado a los usuarios.

Para el estándar IEEE 802.16, el IEEE junto con el Wi-MAX forum, ha trabajado para conseguir definir un sistema de seguridad más robusto. Esto se ha conseguido con el uso de encriptación basada en certificados. Los sistemas Wi-MAX han de garantizar la privacidad de los usuarios finales y prevenir el acceso a información confidencial o sensible a personas no autorizadas. Esto se vuelve más complicado al usarse, como en todas las comunicaciones inalámbricas, un medio de libre acceso como es el aire para realizar la comunicación.

Los principales riesgos de seguridad que hay que cubrir serán los siguientes:

- Sniffing: un usuario no autorizado realiza un monitoreo de todos los paquetes de información que circulan por la red mediante un sniffer, con la posibilidad de obtener claves, cuentas de correo o datos personales.
- Privacidad: Asegurar que la información transmitida es leída sólo por los destinatarios.
- MAC Spoofing: evitar que un atacante robe las direcciones MAC de CPE legítimas para conseguir acceso a la red.
- Robo del servicio: Se debe prevenir que los agresores accedan a la red gratuitamente usando CPE robadas.
- Rogue Base Stations: Consiste en engañar al usuario autorizado con una estación falsa para que se conecte a esta en vez de a la correcta.

Para prevenir la utilización clandestina de la conexión wireless, es necesario disponer de una encriptación adecuada. En este sentido Wi-MAX soporta dos estándares de encriptación de calidad: DES3 y AES.

Para asegurarse que el suministro de servicio se realiza a usuarios finales específicos, se usa autenticación basada en certificados digitales X.509, incluida en la capa MAC, y da a cada usuario receptor su propio certificado, más otro para el fabricante. Esto permite a la estación base autorizar al usuario final.

Sobre la seguridad en redes Wi-MAX se podrían citar más detalles técnicos que quedan fuera del alcance de lo que pretende este artículo. Para terminar, indicar que Wi-MAX ofrece muchas más funcionalidades de seguridad que el estándar Wi-Fi. Además, se basa es estándares robustos y flexibles, lo que da opción a que los vendedores que ofrezcan esta tecnología en sus productos, puedan incorporar características adicionales que doten a las redes Wi-MAX de mecanismos de seguridad 100% fiables.

8. Bibliografía

- http://www.iese.edu/es/files/5_13661.pdf
- http://www.borrmart.es/articulo_redseguridad.php?id=1088&numero=23
- http://www.networkworld.com/columnists/2006/121106-wireless-security.html
- http://www.motorola.com/networkoperators/pdfs/Wi4-the-promise-article.pdf

Modelos de Seguridad para Redes WIFI

Por: Germán Lado Insua

Estudiante de Ingeniería Técnica Informática de Sistemas
Miembro de la rama UNED-IEEE
E-mail: germanlado@gmail.com

1. Introducción

Este es el primero de dos artículos enfocados exclusivamente al análisis de la seguridad en redes WIFI. Como tal, obviaré datos irrelevantes para dicho objetivo tales como la introducción e historia de este sistema así como cualquier enfoque básico.

A través de este artículo explicaré el funcionamiento de los principales modelos de seguridad en redes WIFI para, en el próximo artículo, exponer sus vulnerabilidades y poner en práctica lo expuesto hasta el momento. De este modo, seguiré el siguiente esquema:

Artículo 1: Modelos de seguridad para redes WIFI.
Artículo 2: Vulnerabilidades y tipos de ataques en redes WIFI.

Tras la publicación de estos dos artículos cabe la posibilidad de la ampliación a un tercer artículo con las novedades en el terreno, así como el posterior estudio del futuro sucesor de este tipo de redes: WiMAX, el cual por sus características y novedades, aún siendo parte del estándar 802.16 (frente al 802.11 de WIFI) se considerará por separado.

Para finalizar este prólogo, he de destacar que este artículo está ubicado en el tiempo con respecto a la tecnología inalámbrica, en la transición entre 802.11g y 802.11n del cual aún no hay publicado un estándar definitivo y las empresas que lanzan productos englobados en este último, lo hacen basándose en borradores del estándar definitivo (y muy probablemente compatible con estos). Se empiezan a vislumbrar también diferentes aproximaciones del sucesor WiMAX en ciertas poblaciones, y aún bajo pruebas pero augurando un futuro prometedor.

2. Modelos de Seguridad para redes WIFI

Existen diversas formas y modelos de seguridad aplicados a las redes WIFI, que van desde las estructuras más sencillas a las más complicadas. El modelo más sencillo contempla la utilización de encriptación mediante WEP, y la autentificación se realiza mediante el filtrado de direcciones MAC, que

consideran la deshabilitación de la identificación del AP (SSID). Por otra parte, uno de los modelos de seguridad propietario más popular es el que utiliza el protocolo LEAP (*Lighweight Extensible Authentication Protocol*) [2], que requiere de recursos adicionales para su implementación. Debido a que se trata de un protocolo propietario, los fabricantes han puesto gran esfuerzo en el desarrollo y mejoras de la seguridad de los sistemas WIFI. La ventaja más obvia del protocolo LEAP es la de proveer una seria mejora a la seguridad incorporando el concepto de una llave específica de encriptación por cada sesión; a diferencia de la encriptación estática y "Shared Key", que están expuestas a la amenaza "WEP Cracking" [3]. Adicionalmente, la llave es generada una vez que el acceso ha sido exitoso, la cual puede ser implementada usando una base de datos local de autentificación.

Algunos de los beneficios del protocolo LEAP son los siguientes [4]:

- Autentificación mejorada para los clientes wireless: Utiliza una llave de encriptación por sesión.
- Administración centralizada de usuarios y llaves.
- Reducción de la exposición de la llave de encriptación: En el caso de LEAP la llave es una por sesión, a diferencia de WEP que es una para todas las sesiones.
- Permite ser implementado utilizando las bases de datos existentes para la autentificación de los usuarios.

Otro importante modelo de seguridad para las redes WiFi es la implementación de Autentificación WLAN y Administración de llaves mediante RADIUS para el protocolo EAP-TLS. El protocolo EAP (*Extensible Authentication Protocol*) es una estructura diseñada para la autentificación de redes Ethernet basada en puertos de red. Fue originalmente creada para exigir a los usuarios autentificarse antes de obtener los privilegios de red; sin embargo, esta fue adaptada para ser utilizada en este tipo de ambiente. El protocolo inalámbrico EAP ha sido mejorado para incluir la encriptación en la capa de transporte y administración de llaves. Esta nueva característica es importante ya que elimina el riesgo de la administración estática de las llaves por parte de WEP. EAP utiliza un servidor RADIUS para administrar de manera centralizada las credenciales y los registros de usuarios (*Accounting*). Esta administración centralizada elimina la necesidad de los administradores para realizar actualizaciones manuales de las llaves estáticas, como en el protocolo WEP y de las direcciones MAC de numerosos AP.

Algunos de los tipos de EAP [5] son los siguientes:

- EAP-MD5: Provee un robusto mecanismo de autentificación utilizando el algoritmo hash MD5, en vez de una clave en texto plano.
- EAP-TLS: Provee la administración de las llaves para la encriptación de la capa de transporte.

- EAP-TTLS: Es similar al modelo EAP-TLS, pero utiliza servidores certificados (*Server Certificates*).

Algunos de los beneficios de este modelo son los siguientes:

- Reducción o eliminación de las vulnerabilidades de WEP.
- Administración centralizada de las direcciones MAC y de los usuarios.
- Registros log de actividades (*Accounting*) acerca de las actividades de acceso y autorización.
- Interoperatividad: RADIUS [6] es soportado por una gran cantidad de fabricantes de AP y clientes wireless.

Finalmente, uno de los modelos que presenta un gran nivel de seguridad y compatibilidad es el llamado Acceso Wireless mediante IPSEC [7], también denominado Wireless VPN. Debido a la gran popularidad en redes cableadas, IPSEC es normalmente recomendado como una solución para resolver las implementaciones de seguridad que presentan anomalías en redes wireless. Muchas organizaciones utilizan IPSEC debido a que cuentan con la infraestructura adecuada y disponible para implementar un cliente remoto utilizando VPN, puesto que los costos y las horas de configuración utilizadas son mínimos. Los beneficios de la aplicación de IPSEC en redes WiFi son los siguientes:

- Provee un alto nivel de seguridad con funcionalidades que chequean la integridad, autentificación mutua y anti-replay.
- Permite interoperatividad: A diferencia de otros sistemas, hoy en día IPSEC es un estándar maduro y de alto grado de utilización.
- Repara los errores del diseño de redes WIFI: Sin duda, VPN Wireless es la mejor opción para remediar la seguridad en redes WLAN, ya sea por un mal diseño o porque los estándares de diseños no son los adecuados, esta opción permite eliminar cualquier problema de seguridad sin tener que realizar inversiones por dispositivos adicionales.
- Hoy en día, de acuerdo a la tecnología punta de los sistemas VPN, existe una nueva forma de establecer túneles mediante los llamados “Clientless” VPN, los cuales no requieren implementar IPSEC en los clientes, sino que existe un sólo mecanismo centralizado que realiza esta función, dejando la tarea de encriptación por parte del cliente a aplicaciones de capa superiores.

2.1 Cómo funciona WEP

Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (*Wired Equivalent Privacy*) [1]. WEP intenta proveer de la seguridad de una red con cables a una red Wireless, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace).

El protocolo WEP está basado en el algoritmo de encriptación RC4 [8], y utiliza claves de 64bits o de 128bits. En realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV). Se utiliza un checksum para prevenir que se inyecten paquetes spoofeados. A continuación veremos más a fondo como funciona la encriptación WEP.

2.1.1.- Llaves

La llave de 40 o 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente. La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente. A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP [9 -11].

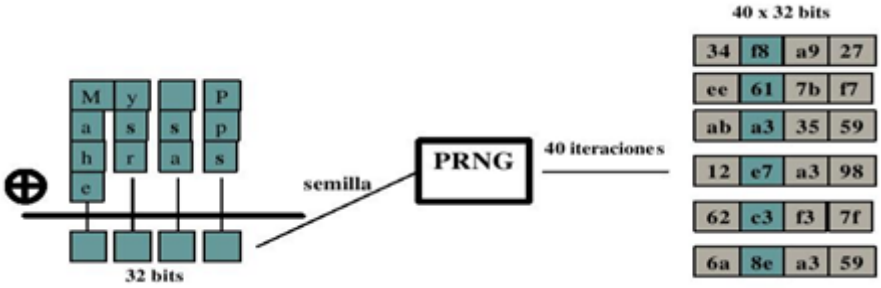


FIGURA 1: PROCESO PARA LA GENERACIÓN DE LLAVES.

Este es el proceso que se realiza para generar las llaves:

Se hace una operación XOR con la cadena ASCII (My Passphrase) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudo-aleatorios (PRNG) para generar 40 cadenas de 32 bits cada una. Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP como veremos a continuación.

2.1.2.- Encriptación

Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como valor de chequeo de integridad (ICV: *Integrity Check Value*) (Figura 2):

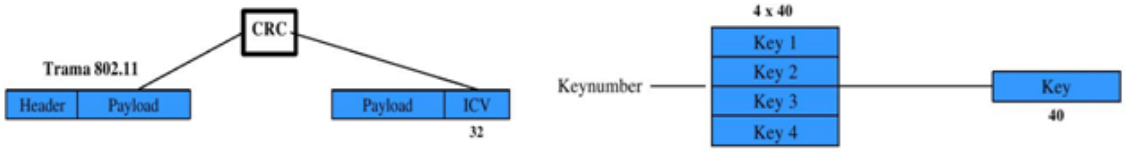


FIGURA 2. Chequeo de integridad.

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles y añadimos el Vector de Inicialización (IV) de 24 bits al principio de la llave seleccionada (Figura 3):

FIGURA 3. Campos de la llave.

El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave. Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado (Figura 4):

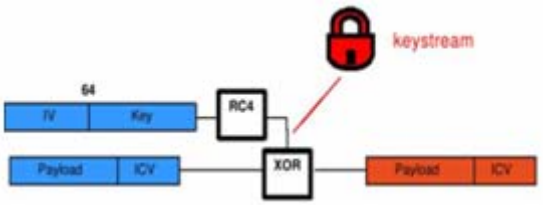


FIGURA 4. Encriptación.

Se utiliza el IV y la llave para encriptar el Payload + ICV.

Después se añade la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada (Figura 5):

FIGURA 5. Trama definitiva.

El proceso de encriptación en conjunto se ve resumido en el esquema (Figura 6).

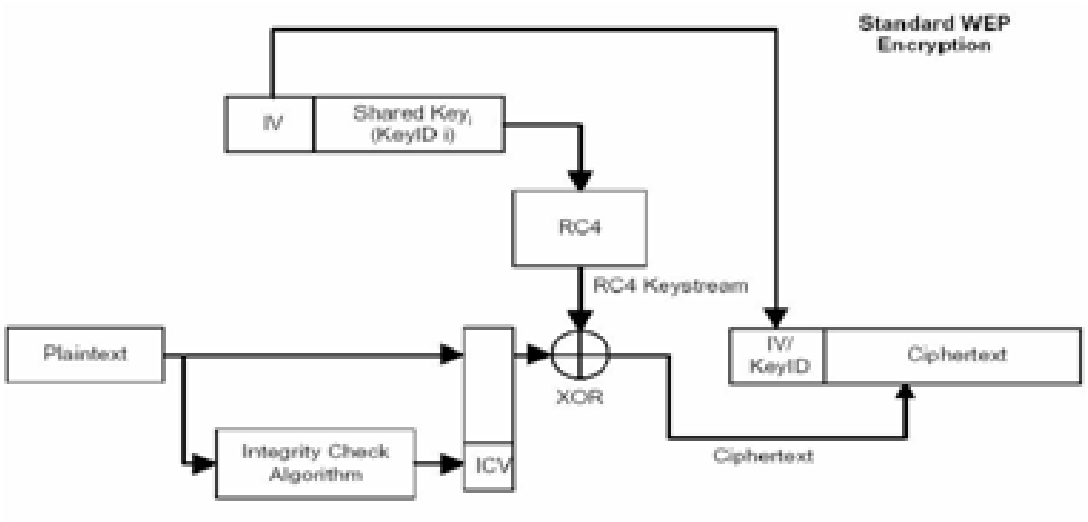


FIGURA 6. Proceso de encriptación.

2.1.3.- Desencriptación

Ahora se va a ver el proceso que se realiza para desencriptar una trama encriptada con WEP: Se utiliza el número de llave que aparece en claro en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado para cifrar la trama.

Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64 bits de llave. Aplicando RC4 a esta llave obtenemos el keystream válido para obtener la trama en claro (plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación (Figura 7).

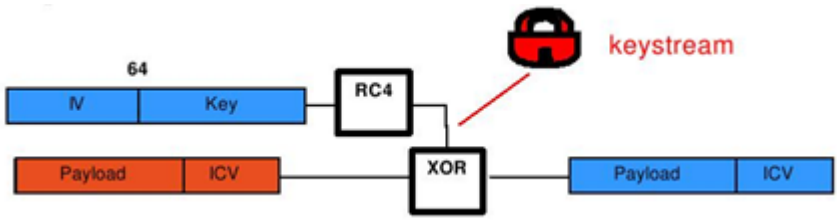


FIGURA 7. Desencriptación,

Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original. El proceso completo puede verse en el esquema de la Figura 8.

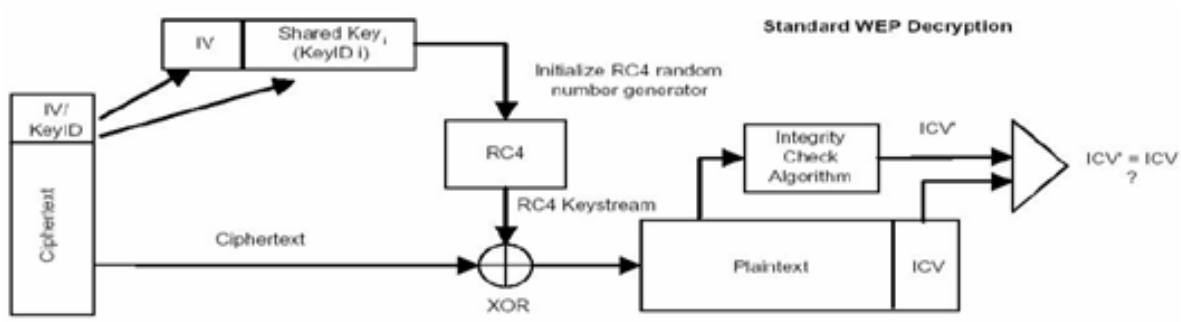


FIGURA 8. Proceso de desencriptación.

2.2 Cómo funciona WPA/WPA2

2.2.1.- Fase 1- Acuerdo sobre la política de seguridad

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar [12-14]. Las políticas de seguridad soportadas por el punto de acceso son mostradas en un mensaje Beacon o Probe Response (después de un *Probe Request* del cliente). Sigue a esto una autentificación abierta estándar (igual que en las redes TSN, donde la autentificación siempre tiene éxito).

La respuesta del cliente se incluye en el mensaje de *Association Request* validado por una *Association* Response del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (*Information Element*) y detalla:

- Los métodos de autentificación soportados (802.1X, *Pre-Shared Key* (PSK))
- Protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.) Suit criptográfica basada en pares
- Protocolos de seguridad para el tráfico multicast (CCMP, TKIP, etc.) Suit criptográfica de grupo
- Soporte para la pre-autentificación, que permite a los usuarios pre-autenticarse antes de cambiar de punto de acceso en la misma red para un funcionamiento sin retrasos.

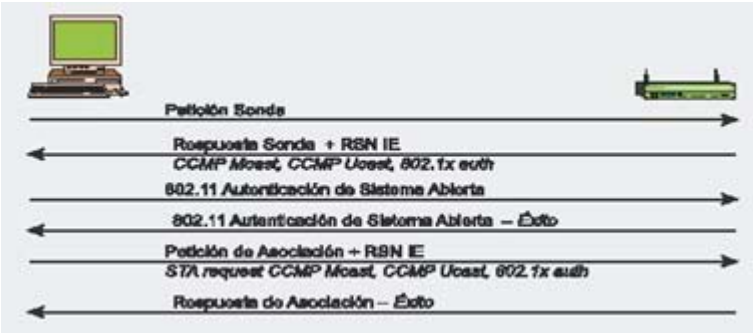


FIGURA 9 . FASE 1.

2.2.2.- Fase 2- Autentificación 802.1X

La segunda fase es la autentificación 802.1X basada en EAP [15] y en el método específico de autentificación decidido: EAP/TLS con certificados de cliente y servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP para autentificación híbrida (con certificados sólo requeridos para servidores), etc. La autentificación 802.1X se inicia cuando el punto de acceso pide datos de identidad del cliente, y la respuesta del cliente incluye el método de autentificación preferido. Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autentificación para generar una clave maestra común (MK). Al final del proceso, se envía desde el servidor de autentificación al punto de acceso un mensaje Radius Accept, que contiene la MK y un mensaje final EAP Success para el cliente.

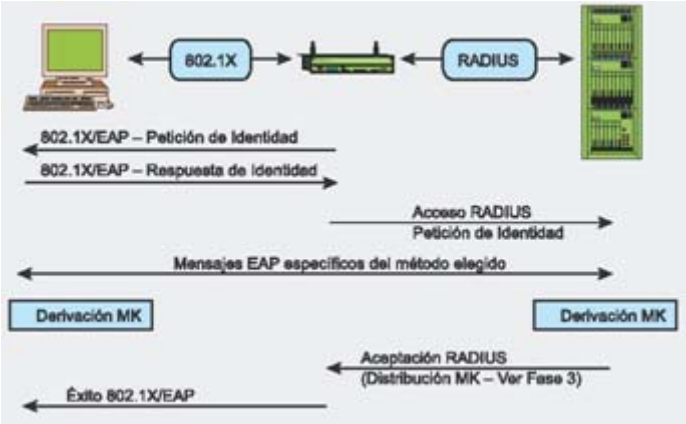


FIGURA 10. FASE 2.

2.2.3.- Fase 3- Jerarquía y distribución de claves

La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autentificación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La generación y el intercambio de claves es la meta de la tercera fase. Durante la derivación de la clave, se producen dos handshakes.

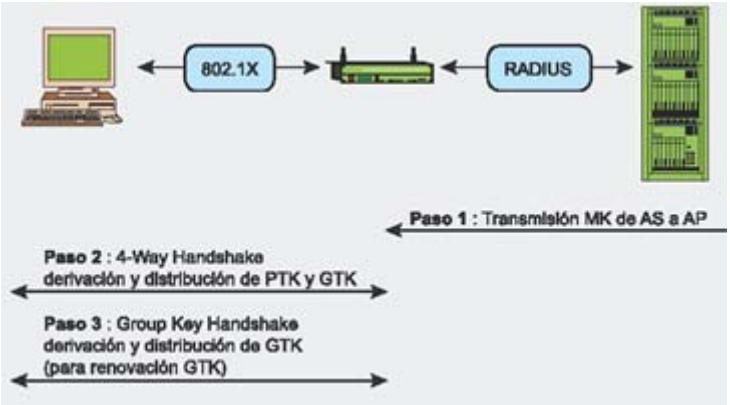


FIGURA 11 FASE 3.

- 4-Way Handshake [16] para la derivación de la PTK (*Pairwise Transient Key*) y GTK (*Group Transient* Key).
- *Group Key Handshake* para la renovación de GTK.

La derivación de la clave PMK (*Pairwise Master Key*) depende del método de autentificación:

- Si se usa una PSK (*Pre-Shared Key*), PMK = PSK. La PSK es generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256-bits y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autentificación.
- Si se usa un servidor de autentificación, la PMK es derivada de la MK de autentificación 802.1X.

La PMK en si misma no se usa nunca para la encriptación o la comprobación de integridad. Al contrario, se usa para generar una clave de encriptación temporal – para el tráfico unicast esta es la PTK (Pairwise Transient Key). La longitud de la PTK depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. La PTK consiste en varias claves temporales dedicadas:

- KCK (*Key Confirmation Key* – 128 bits): Clave para la autenticación de mensajes (MIC) durante el 4-Way Handshake y el Group Key Handshake.
- KEK (*Key Encryption Key* – 128 bits): Clave para asegurar la confidencialidad de los datos durante el 4-Way Handshake y el Group Key Handshake.
- TK (*Temporary Key* – 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP).
- TMK (*Temporary MIC Key* – 2x64 bits): Clave para la autentificación de datos (usada sólo por Michael con TKIP). Se usa una clave dedicada para cada lado de la comunicación.

Esta jerarquía se resume en la figura 12.

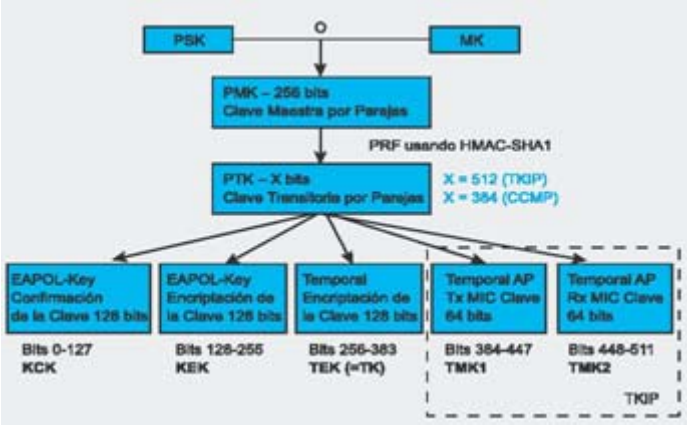


FIGURA 12 JerarquíaPMK.

El 4-Way Handshake, iniciado por el punto de acceso, hace posible:

- Confirmar que el cliente conoce la PMK
- Derivar una PTK nueva
- Instalar claves de encriptación e integridad
- Encriptar el transporte de la GTK
- Confirmar la selección de la suite de cifrado.

Se intercambian cuatro mensajes EAPOL-Key [16-17] entre el cliente y el punto de acceso durante el 4-Way Handshake. Esto se muestra en la figura 13.

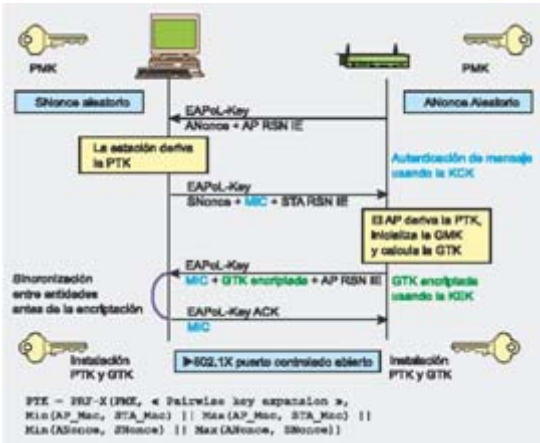


FIGURA 13 Intercambio de mensajes.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (ANonce y SNonce, generados por el autentificador y el suplicante, respectivamente). El punto de acceso inicia el primer mensaje seleccionando el número aleatorio ANonce y enviándoselo al suplicante, sin encriptar el mensaje o protegerlo de las trampas. El suplicante genera su propio número aleatorio SNonce y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el SNonce y la clave MIC calculada del segundo mensaje usando la clave KCK. Cuando el autentificador recibe el segundo mensaje, puede extraer el SNonce

(porque el mensaje no está encriptado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor de MIC en el segundo mensaje y estar seguro de que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

El tercer mensaje enviado por el autentificador al suplicante contiene el GTK (encriptada con la clave KEK), derivada de un GMK aleatorio y GNonce (ver siguiente figura), junto con el MIC calculado del tercer mensaje utilizando la clave KCK.

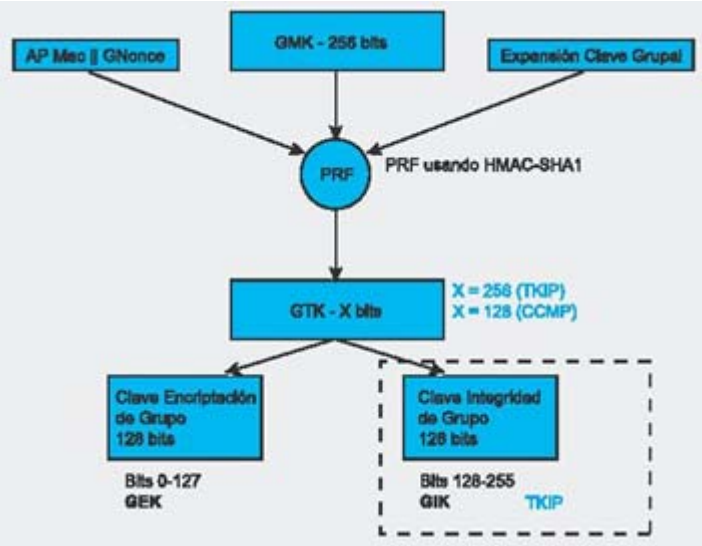


FIGURA 14: FASE 3, Jerarquia de grupos.

Cuando el suplicante recibe este mensaje, el MIC se comprueba para asegurar que el autentificador conoce el PMK y ha calculado correctamente la PTK y derivado claves temporales.

El último mensaje certifica la finalización del handshake e indica que el suplicante ahora instalará la clave y empezará la encriptación. Al recibirlo, el autentificador instala sus claves tras verificar el valor MIC. Así, el sistema móvil y el punto de acceso han obtenido, calculado e instalado unas claves de integridad y encriptación y ahora pueden comunicarse a través de un canal seguro para tráfico unicast y multicast.

El tráfico multicast se protege con otra clave: GTK (Group Transient Key), generada de una clave maestra llamada GMK (Group Master Key), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio GNonce. La longitud de GTK depende del protocolo de encriptación – 256 bits para TKIP y128 bits para CCMP. GTK se divide en claves temporales dedicadas:

- GEK (Group Encryption Key): Clave para encriptación de datos (usada por CCMP para la autentificación y para la encriptación, y por TKIP).
- GIK (Group Integrity Key): Clave para la autenticación de datos (usada solamente por Michael con TKIP).

Se intercambian dos mensajes EAPOL-Key entre el cliente y el punto de acceso durante el Group *Key Handshake*. Este handshake hace uso de claves temporales generadas durante el 4-Way Handshake (KCK y KEK). El proceso se muestra en la figura 15.

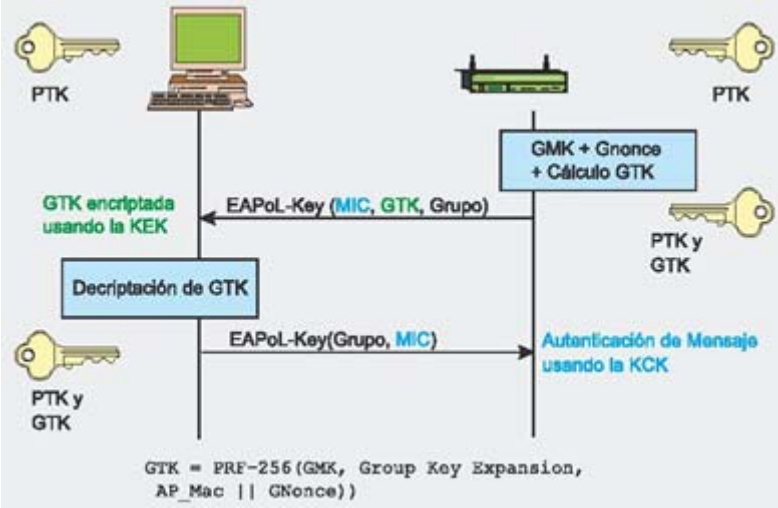


FIGURA 15. Handshake.

El *Group Key Handshake* sólo se requiere para la disasociación de una estación o para renovar la GTK, a petición del cliente. El autentificador inicia el primer mensaje escogiendo el número aleatorio GNonce y calculando una nueva GTK. Envía la GTK encriptada (usando KEK), el número de secuencia de la GTK y el MIC calculado de este mensaje usando KCK al suplicante. Cuando el mensaje es recibido por el suplicante, se verifica el MIC y la GTK puede ser desencriptada.

El segundo mensaje certifica la finalización del Group Key Handshake enviando el número de secuencia de GTK y el MIC calculado en este segundo mensaje. Al ser recibido este, el autenticador instala la nueva GTK (tras verificar el valor MIC).

También existe un STAkey Handshake, pero no lo vamos a tratar aquí. Soporta la generación de una clave, llamada STAkey, por el punto de acceso para conexiones ad-hoc.

2.2.4.- Fase 4- Confidencialidad e integridad de datos RSNA

Todas las claves generadas anteriormente se usan en protocolos que soportan la confidencialidad e integridad de datos RSNA [17]:

- TKIP (Temporal Key Hash)
- CCMP (Counter-Mode / Cipher
- Block Chaining Message Authentication Code Protocol)
- WRAP (Wireless Robust Authenticated Protocol)

Hay un concepto importante que debe ser entendido antes de detallar estos protocolos: la diferencia entre MSDU (MAC *Service Data Unit*) y MPDU (MAC *Protocol Data Unit*).

Ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación, mientras las MPDUs son múltiples unidades de datos tras la fragmentación. La diferencia es importante en TKIP y en el protocolo de encriptación CCMP, ya que en TKIP el MIC se calcula desde la MSDU, mientras que en CCMP se calcula desde MPDU.

Al igual que WEP, TKIP está basada en el algoritmo de encriptación RC4, pero esto es así tan sólo por un motivo: permitir a los sistemas WEP la actualización para instalar un protocolo más seguro. TKIP se requiere para la certificación WPA y se incluye como parte de RSN 802.11i como una opción. TKIP añade medidas correctoras para cada una de las vulnerabilidades de WEP descritas anteriormente:

- Integridad de mensaje: un nuevo MIC (*Message Integrity Code*) basado en el algoritmo Michael puede ser incorporado en el software para microprocesadores lentos.
- IV: nuevas reglas de selección para los valores IV, reutilizando IV como contador de repetición (TSC, o TKIP *Sequence Counter*) e incrementando el valor del IV para evitar la reutilización.
- *Per Packet Key Mixing*: para unir claves de encriptación aparentemente inconexas.
- Gestión de claves: Nuevos mecanismos para la distribución y modificación de claves

TKIP *Key-Mixing Scheme* se divide en dos fases. La primera se ocupa de los datos estáticos – la clave TEK de sesión secreta, el TA de la dirección MAC del transmisor (incluido para prevenir colisiones IV) y los 32 bits más altos del IV. La fase 2 incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo Per Packet Key para cada nuevo IV. El valor IV siempre empieza en 0 y es incrementado de uno en uno para cada paquete enviado, y los mensajes cuyo TSC no es mayor que el del último mensaje son rechazados. El resultado de la fase 2 y parte del IV extendido (además de un bit dummy) componen la entrada para RC4, generando un flujo de clave que es XOR-eado con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP (ver Figura 12).

La computación del MIC utiliza el algoritmo Michael de Niels Ferguson. Se creó para TKIP y tiene un nivel de seguridad de 20 bits (el algoritmo no utiliza multiplicación por razones de rendimiento, porque debe ser soportado por el viejo hardware de red para que pueda ser actualizado a WPA). Por esta limitación, se necesitan contramedidas para evitar la falsificación del MIC. Los fallos de MIC deben ser menores que 2 por minuto, o se producirá una desconexión de 60 segundos y se establecerán nuevas claves GTK y PTK tras ella. Michael calcula un valor de comprobación de 8 octetos llamado MIC y lo añade a la MSDU antes de la transmisión. El MIC se calcula de la dirección origen (SA), dirección de destino (DA), MSDU de sólo texto y la TMK apropiada

(dependiendo del lado de la comunicación, se utilizará una clave diferente para la transmisión y la recepción).

CCMP se basa en la suite de cifrado de bloques AES (*Advanced Encryption Standard*) en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP, pero al contrario que TKIP, que se diseñó para acomodar al hardware WEP existente, CCMP no es un compromiso, sino un nuevo diseño de protocolo. CCMP utiliza el counter mode junto a un método de autentificación de mensajes llamado *Cipher Block Chaining (*CBC-MAC) para producir un MIC.

Se añadieron algunas características interesantes, como el uso de una clave única para la encriptación y la autentificación (con diferentes vectores de inicialización), el cubrir datos no encriptados por la autentificación. El protocolo CCMP añade 16 bytes al MPDU, 8 para el encabezamiento CCMP y 8 para el MIC. El encabezamiento CCMP es un campo no encriptado incluido entre el encabezamiento MAC y los datos encriptados, incluyendo el PN de 48-bits (Packet Number = IV Extendido) y la Group Key KeyID. El PN se incrementa de uno en uno para cada MPDU subsiguiente.

La computación de MIC utiliza el algoritmo CBC-MAC que encripta un bloque nonce de inicio (computado desde los campos de Priority, la dirección fuente de MPDU y el PN incrementado) y hace XORs sobre los bloques subsiguientes para obtener un MIC final de 64 bits (el MIC final es un bloque de 128-bits, ya que se descartan los últimos 64 bits). El MIC entonces se añade a los datos de texto para la encriptación AES en modo contador. El contador se construye de un nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementado para cada bloque.

El último protocolo es WRAP, basado también en AES pero utilizando el esquema de encriptación autenticada OCB (Offset Codebook Mode – encriptación y autentificación en la misma operación). OCB fue el primer modo elegido por el grupo de trabajo de IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias. Entonces se adoptó CCMP como obligatorio.

Referencias

[1] Web de IEEE sobre proyecto 802.11 (Especificaciones + Papers):
http://grouper.ieee.org/groups/802/11/main.html
Web de la Wi-Fi Alliance (Especificaciones + Papers):
http://www.wi-fi.org/opensection/protected_access.asp

[2] Carlos Aracena Urrutia y Cristian Araya Valenzuela: **“**Seguridad en redes WiFi”.

[3] Web de Hispasec sobre seguridad informática: http://www.hispasec.com

[4] Briant Carter, Russell Shumway: “Wireless Security End to End”, Willey Publishing, Inc, 2002, pp.11-36, 123-139

[5] Deploying 802.1X for WLANs: EAP Types By Lisa Phifer September 10, 2003

[6] RFC 2865 (autentificación y autorización) y RFC 2866 (*accounting*).

[7] http://es.wikipedia.org/wiki/IPSEC + RFCs

[8] Jason Liu, “The Security of WEP Wired Equivalent Privacy”, CSE525 Advanced Networking, http://www.cse.ogi.edu
S. Fluhrer, I. Mantin, y A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, Agosto 2001:
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[9] Nikita Borisov, Ian Goldberg, David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11". Retrieved on 2006-09-12

[10] Andrea Bittau, Mark Handley, Joshua Lackey. "The Final Nail in WEP's Coffin". Retrieved on 2008-03-16.

[11] IEEE 802.11-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. J. Walker, “Unsafe at any key size: an analysis of the WEP encapsulation”. Documento IEEE 802.11-00/362, Octubre 2000.

[12] Web de la Wi-Fi Alliance: WPA –
http://www.wifi.org/knowledge_center/wpa/

[13] Wi-Fi Alliance. (2003). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks. March 1, 2004.

[14] IEEE Std. 802.11i-2004 –
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[15] Wireless security - 802.1x and EAP types –
http://www.intel.com/support/wireless/wlan/sb/cs-008413.htm

[16] http://en.wikipedia.org/wiki/IEEE_802.11i

[17] 802.11i Parte 11: Wireless LAN Medium Access Control (MAC) and Physical Layer specifications –
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

Criptografía: El poder de lo oculto (I)

Por: Germán Carro Fernández

Estudiante de Ingeniería Técnica en Informática de Sistemas.
Miembro de Student Branch IEEE – UNED.
E-mail: germancf@eresmas.net

1. Introducción

Ya en la antigüedad encontramos razones que nos impulsan a comprender una evidencia que si cabe en nuestros días no es desdeñada ya por nadie: ***el conocimiento es poder***.

Pero esta misma característica hace precisamente que el hecho de poseer una información determinada lleve implícita la obligación de protegerla de observadores externos.

De manera recurrente la importancia de esta protección asentó los primeros pasos de lo que se ha venido en llamar criptografía. Etimológicamente la palabra "criptografía" proviene del griego y aúna la descripción completa del término, por una parte "*kryptos*" que significa "ocultar", y por otra "*graphos*", o lo que es lo mismo "escribir". Ambos verbos articulan la actividad protagonista de este artículo. Como ya adelantábamos, la criptografía busca garantizar el secreto en las comunicaciones entre dos personas o entidades. Su labor asume también la responsabilidad de verificar que el emisor o receptor del mensaje son quiénes dicen ser, y que el contenido de aquél no ha sido modificado en el proceso de envío.

Si bien no podemos olvidar que dentro de las técnicas de ocultación de información tenemos a la *esteganografía*, es importante reseñar que ésta y la criptografía son dos sistemas diferentes, aunque complementarios. La esteganografía busca ocultar "físicamente" un mensaje, bien sea camuflándolo dentro de un archivo de imagen, dentro de un sonido, o a través de diferentes técnicas, en algunos casos incluso químicas (como podría ser el uso de la tinta invisible). Ambos sistemas van a fortalecer, si cabe, la protección de la información que se desea emitir o salvaguardar.

Hoy en día y en una sociedad globalizada e interconectada como en la que vivimos, la criptografía forma parte esencial de nuestras vidas. Bien a través de operaciones de comercio electrónico, o de nuestras propias conexiones a Internet, estamos enviando datos que son encriptados y desencriptados con una mayor o menor eficacia, y que son susceptibles de ser robados por individuos u organizaciones que podrían permitirse hacer un uso deshonesto de los mismos.

Sistemas criptográficos que se desarrollan en la actualidad con una gran importancia son, por poner un ejemplo, los de la firma electrónica, los de encriptación de datos para la transmisión segura de los mismos en redes Wi-Max o Wi-Fi, los relacionados con las transacciones seguras en el comercio electrónico, o el propio DNI electrónico que ya se utiliza en nuestro país.

Si bien la seguridad de muchos de estos sistemas está entredicho y se defiende que aún no están lo suficientemente desarrollados para garantizar una total protección, al menos si garantizan cierta eficiencia a la hora de utilizarlos en combinación con otras técnicas de identificación biométricas como la huella dactilar, el análisis del iris y la retina ocular o el reconocimiento facial.

A lo largo de este artículo y los que le seguirán, intentaremos ir desgranando la historia, evolución y características más relevantes que rodean a la criptografía, sus aplicaciones actuales y la implementación algorítmica de sus fórmulas matemáticas más habituales. Es difícil reducir a unas pocas palabras un mundo tan inmenso e intenso como el criptográfico, pero este acercamiento nos permitirá apreciar la importancia que no sólo la información tiene en nuestros días, sino; y con más énfasis; lo necesario que es la protección segura de la misma.

2. Desde la "escítala"....

Ya en siglo V antes de J.C. los espartanos utilizaban un mecanismo para cifrar sus mensajes. Envueltos en permanentes guerras con los pueblos vecinos y defendiéndose de manera constante de asaltos al poder, este pueblo griego desarrollo un peculiar sistema para cifrar sus mensajes: la “*escítala*”.

El artilugio en cuestión era bien sencillo. Lo formaban dos varas de igual grosor, y una tira de cuero o papiro en la que se escribía el mensaje. El procedimiento era también simple, pero efectivo. El emisor del mensaje enrollaba la tira alrededor de la vara, una vez hecho esto procedía a escribir el mensaje sobre la tira enrollada de manera que se grababa una letra en cada vuelta de la tira. Una vez grabado el mensaje se procedía a rellenar la tira con caracteres de manera aleatoria. A continuación se procedía a desenrollar la tira y se procedía a enviar la misma por medio de un mensajero hasta el receptor. Éste a su vez tenía la otra vara, de igual grosor que la primera, en su poder. Cuando el mensajero llegaba con la tira en la que iba escrito el mensaje, sólo tenía que volver a enrollarla en la vara y leer consecutivamente los caracteres escritos.

La eficacia de este método radicaba precisamente en que sólo con una vara de igual grosor se podía leer el mensaje de manera correcta. De no tenerla, el enemigo que hubiera interceptado el mensaje no sería capaz de descifrar su contenido.

FIGURA 1. EXCÍTALA CLÁSICA.

En la imagen se puede apreciar claramente la distribución longitudinal de los caracteres que forman el mensaje a cifrar. A pesar de lo rudimentario del sistema era lo suficientemente efectivo como para iniciar la ciencia de la encriptación de datos; y por supuesto también el arte de la desencriptación de los mismos.

En los siglos venideros estas técnicas se fueron perfeccionando y diseñando otras nuevas, como ejemplo de las mismas podríamos citar las siguientes:

- **El cifrado de Polybios** (s. II a.c.): que utilizaba una tabla para realizar la combinación de letras y cifrar así cada carácter del alfabeto:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

TABLA 1: TABLA DE POLYBIOS.

De esta manera, la palabra “HOLA” se cifraría como “BCCDCAAA”. A pesar de lo ingenuo que pueda parecer este sistema, ha sido la base para lo modernos cifradores polígráficos[1] del siglo XIX.

- **El cifrado del César** (s.I a.c.): que introdujo el principio de transposición en el texto para cifrarlo. En este caso utilizaba un desplazamiento de tres letras para diseñar el texto cifrado. De esta forma el alfabeto quedaba reorganizado de la siguiente manera:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

TABLA 2: CIFRADO DEL CÉSAR.

Así, y continuando con el ejemplo anterior, la palabra “HOLA” se cifraría como “KRÑD”.

Ambos ejemplos reflejan la premura con la que las diferentes sociedades desarrolladas iban incorporando nuevos sistemas de cifrado a la actividad; sobre todo política y militar; de la época.

Volviendo de nuevo a retomar la senda de los “mecanismos” o útiles para encriptación, podemos reseñar alguno de los ya desarrollados en siglos más recientes, como pueden ser:

- **El cilindro de Jefferson** (1795): diseñado por el propio Thomas Jefferson[2], considerado el padre de la criptografía americana. Constaba de 26 discos, cada uno de los cuales tenía las letras del alfabeto escritas de manera aleatoria sobre su superficie. Esa disposición estructural le permitía utilizar la combinación de los 26 discos para cifrar y descifrar mensajes en base a los distintos alfabetos que lo formaban.

FIGURA 2. CILINDRO DE JEFFERSON.

- **El cifrador de Bazeries** (finales del s.XIX): Étienne Bazeries[3] perfeccionó el cilindro de Jefferson incluyendo en su sistema inicial un disco conteniendo cifras. Eso permitía asignar los movimientos para cada disco indicando +1,+2,+3… ó -1, -2, -3… en función de si deberían girarse 1, 2 , 3 … caracteres en el sentido de las agujas del reloj o en sentido contrario respectivamente.

Pero estos artilugios eran sólo un pequeño ejemplo de lo que se podía llegar a diseñar combinando la perspicacia combinatoria y la técnica. El siguiente paso llegó en pleno siglo XX.

3. ...hasta "Enigma"

Es aquí dónde debemos de hacer un alto en camino para hablar de la máquina de cifrado por antonomasia para todos aquellos que quieren adentrarse en el mundo de la criptografía.

- **Enigma** (desde 1919 hasta 1945): Si hay un artilugio mecánico con historia propia con independencia de su creador, ese es sin duda la máquina de cifrado Enigma. Comenzó utilizándose como un sistema comercial de cifrado para empresas y acabó decidiendo el futuro de la Segunda Guerra Mundial. El descubrimiento de su sistema de cifrado, y la posterior lectura de la información

que contenían los mensajes alemanes supuestamente protegidos, es considerado, a veces, como la causa de haber podido concluir esta guerra, al menos, un año antes de lo que hubiera acaecido sin su descifrado.

La máquina Enigma era un dispositivo electromecánico, lo que significa que utilizaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba constituido fundamentalmente por un teclado, similar al de las máquinas de escribir, que controlaba una serie de interruptores eléctricos y un engranaje mecánico.

La parte eléctrica consistía en una batería que se conectaba a una de las lámparas, que representaban las diferentes letras del alfabeto. Se puede observar en la parte inferior de la imagen que aparece más abajo, el teclado, siendo las lámparas los minúsculos círculos que se encuentran encima de éste.

El corazón de la máquina Enigma era mecánico y constaba de varios ***rotores*** conectados entre sí. Un rotor era un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto de una cara estaba conectado o cableado a un contacto diferente de la cara contraria. Por ejemplo, en un rotor en particular, el contacto número 1 de una cara podía estar conectado con el contacto número 14 en la otra cara y el contacto número 5 de una cara con el número 22 de la otra. Cada uno de los rotores proporcionados con la máquina Enigma estaba cableado de una forma diferente y los rotores utilizados por el ejército alemán poseían un cableado distinto al de los modelos comerciales.

Dentro de la máquina había, en la mayoría de las versiones, tres ranuras para poder introducir los rotores. Cada uno de los rotores se encajaba en la ranura correspondiente de forma que sus contactos de salida se conectaban con los contactos de entrada del rotor siguiente. El tercer y último rotor se conectaba, en la mayoría de los casos, a un ***reflector*** que conectaba el contacto de salida del tercer rotor con otro contacto del mismo rotor para realizar el mismo proceso pero en sentido contrario y por una ruta diferente. La existencia del reflector diferencia a la máquina Enigma de otras máquinas de cifrado basadas en rotores de la época. Este elemento, que no se incluía en las primeras versiones de la máquina, permitía que la clave utilizada para el cifrado se pudiera utilizar en el descifrado del mensaje. Se pueden observar en la parte superior de la imagen los tres rotores con sus correspondientes y delgadas protuberancias dentadas que permitían girarlos a mano, colocándolos en una posición determinada.

Si bien este sistema de tres rotores fue el predominante en sus inicios, durante la Segunda Guerra Mundial se llegaron a diseñar máquinas Enigma con cinco rotores, lo cual dificultaba aún más el descifrado de los mensajes cifrados por ellas.

El descifrado de Enigma viene precedido por trabajos de descifrado e investigación estadística iniciados por el matemático polaco Marian Rejewski[4]. El compartir sus descubrimientos con el bando aliado llevó a estos últimos a

diseñar el denominado programa **"ULTRA"**. Bajo estas siglas se escondió la mayor operación de descifrado en la historia militar hasta esa fecha.

FIGURA 3. MAQUINA ENIGMA.

Con base en *Bletchley Park*, a 80 Km. al norte de Londres se estableció una base de operaciones que, formada por matemáticos, estadísticos, jugadores de bridge, ajedrez, y fanáticos de los crucigramas, se encargaron de dar los pasos necesarios para descifrar las comunicaciones alemanas durante la contienda. Entre los matemáticos que colaboraron de manera activa, estaba Alan Turing[5] como director de la sección *Naval Enigma* de la citada base de operaciones**.**

Los esfuerzos dedicados a esta operación dieron sus frutos junto con la ayuda de indirecta de los propios operadores de radio alemanes, que en algunas ocasiones cometían errores de seguridad importantes realizando pruebas de envíos con sus máquinas Enigma originales: *"…En un caso, a un operador le fue solicitado enviar un mensaje de prueba, por lo que él simplemente tecleó T's repetidamente, y lo enviaron. Un analista británico recibió un mensaje largo sin una sola T en las estaciones de intercepción, e inmediatamente comprendió lo que había pasado. En otros casos, los operadores, usarían constantemente las mismas configuraciones para codificar un mensaje, a menudo su propias iniciales o las de sus novias. Se pusieron analistas a encontrar estos mensajes en el mar de tráfico interceptado todos los días, permitiendo a Bletchley usar las técnicas polacas originales para encontrar las configuraciones iniciales durante el día. Otros operadores alemanes usaron el mismo formulario para los*

informes diarios, en su mayoría para los informes de tiempo, de manera que la misma criba pudo usarse todos los días…".

Este tipo de *"fallos humanos"* en la seguridad aún se siguen cometiendo hoy en día, si bien no con máquinas Enigma, sí con actitudes por parte del usuario como las que propician el enviar datos por Internet sin validar la solicitud de origen de los mismos, por ejemplo.

Así mismo, la captura de barcos o submarinos alemanes que llevaban consigo máquinas de este tipo, ayudó sobremanera a conseguir descifrados sólidos de las transmisiones alemanas.

Finalmente es de destacar el hecho de que hasta los años 60' los aliados no desvelaron que habían conseguido descifrar las transmisiones realizadas con la máquina Enigma durante la Segunda Guerra Mundial. Sólo a partir de esa década se supo lo que había ocurrido realmente en los últimos años de la contienda.

No obstante y para todos aquellos que se preguntan qué utilidad puede tener el conocer antiguos (que no anticuados) métodos de encriptación de datos reproducimos a continuación un ejemplo, en lenguaje de programación C, del código que se ejecutaba mediante hardware con estas peculiares e interesantes máquinas Enigma.

```
#include <stdio.h>
#include <ctype.h>
/*
   Maquina Enigma de 3 rotores.
   Martin Di Luzio, Ivan Rizzo, Taihu Pire
   enigma@kstor.com.ar
   (C) Mayo - 2006

   This program is free software; you can redistribute it and/or
   modify it under the terms of the GNU General Public License
   as published by the Free Software Foundation; either version 2
   of the License, or (at your option) any later version.
*/

//Rotores
char extra [2][26]={
    {"ABCDEFGHIJKLMNOPQRSTUVWXYZ"},
    {"ABCDEFGHIJKLMABCDEFGHIJKLM"},
};
char rotor1 [2][26]={
    {"MNOPQRSTUVWXYZABCDEFGHIJKL"},
    {"ESOVPZJAYQUIRHXLNFTGKDCMWB"},
};
char rotor2 [2][26]={
    {"EFGHIJKLMNOPQRSTUVWXYZABCD"},
    {"BDFHJLCPRTXVZNYEIWGAKMUSQO"},
};
char rotor3 [2][26]={
    {"IJKLMNOPQRSTUVWXYZABCDEFGH"},
    {"AJDKSIRUXBLHWTMCQGZNPYFVOE"},
};

//Gira n veces los rotores
void rotar(char (*rotor)[26],int n)
{
```

```
int i,j;
char temp1,temp2;
for(i=0;i<n;i++){
 temp1=rotor[0][25];
 temp2=rotor[1][25];
 for(j=25;j>=0;j--){
  rotor[0][j]=rotor[0][j-1];
  rotor[1][j]=rotor[1][j-1];
 }
 rotor[0][0]=temp1;
 rotor[1][0]=temp2;
 }
}

//Busca la posicion de un caracter en una lista
int poschar(char (*rotor)[26],char c,int d)
{
 int i;
     for(i=0; i<26 && c!=rotor[d][i] ;i++);
     return (i);
}

int main(int argc,char *argv[])
{
 int i,pos,b1,cont=0;
 char a1,c;

    if (argc!=4){
     printf("\nUso: ./enigma <clave> <archivo> <destino>\n");
     return 0;
     }
    else {

 //Posicion inicial de los rotores
    rotar(rotor1,*argv[1]);
    rotar(rotor2,*++argv[1]);
    rotar(rotor3,*argv[1]);

    printf("\n|||||||||||||< Maquina Enigma de 3 Rotores >|||||||||||||\n\n");

    FILE *en,*sa;
    en = fopen(argv[2],"r");
    sa = fopen(argv[3],"w");

    if (en==NULL){
     printf("Archivo no encontrado\n");
     return 0;
     }

    printf("Se guardo en %s\n",argv[3]);

    while((c=getc(en))!=EOF){

    if (!isalpha(c)) //Se fija si el caracter pertenece al alfabeto.
     continue;
    else {

    c=toupper(c);
    i=poschar(extra,c,0);

    a1=rotor1[0][i];
            b1=poschar(rotor1,a1,1);
            a1=rotor2[0][b1];
            b1=poschar(rotor2,a1,1);
            a1=rotor3[0][b1];
            b1=poschar(rotor3,a1,1);
            a1=extra[1][b1];
```

```
  for(i=0;i<26;i++)
   if ((a1==extra[1][i])&&(i!=b1))
    pos = i;

  a1=rotor3[1][pos];
          b1=poschar(rotor3,a1,0);
          a1=rotor2[1][b1];
          b1=poschar(rotor2,a1,0);
          a1=rotor1[1][b1];
          b1=poschar(rotor1,a1,0);
  a1=extra[0][b1];

          putc(a1,sa); //Guarda en archivo

  //Rotacion
  rotar(rotor1,1);
          cont++;
          if ((cont%26)==0){
           rotar(rotor2,1);
          }
  if ((cont%676)==0){
   rotar(rotor3,1);
  }
  //Fin rotacion

  }

  // Forma 12 bloques de 5 char por linea
  if ((cont%5)==0)
   putc(' ',sa);
  if ((cont%60)==0)
   putc('\n',sa);

 }

fclose(en);
fclose(sa);

 printf("\n");
}

return 0;
}
```

Código de la Máquina Enigma de tres rotores.
Cortesía de Martin Di Luzio, Ivan Rizzo y Taihu Pire.

Se ha mantenido el código fuente original, tal cual lo implementaron sus autores en el 2006, para demostrar que, aunque la técnica en que se basa puede parecer antigua, su utilidad de encriptación y desencriptación sigue vigente hoy en día.

4. La criptografía hoy

La breve reseña histórica que hemos realizado en los apartados anteriores de este artículo nos lleva afrontar la situación de la ciencia criptográfica en la actualidad y sus aplicaciones técnicas.

El mayor avance en las técnicas criptográficas ha venido de la mano del desarrollo de los ordenadores. Esto ha permitido que cada vez sea más importante un análisis algebraico para perfeccionar y desarrollar las técnicas ya

existentes y diseñar nuevos sistemas en función del incremento de potencia computacional motivado por el avance de los nuevos equipos informáticos. Estos nuevos criptosistemas tienen una base común al soporte en el que son desarrollados, es decir, se sustentan en análisis binarios.

El proceso de encriptación se reduce a "transformar" cadenas de caracteres en los ceros y unos que los representan y, a partir de ahí, aplicar los algoritmos necesarios para encriptar la información. El receptor por su parte debe realizar los pasos opuestos para poder leer el mensaje.

Con esto presente podemos clasificar los sistemas criptográficos modernos en dos categorías básicas:

- ***Cifrados secuenciales***: su funcionamiento se centra en generar una sucesión de bits con la misma longitud que el texto cifrado, la "secuencia clave". Para cifrar el mensaje se va a realizar un "**XOR**" (suma exclusiva) entre el mensaje binario original y la citada secuencia clave. El resultado será el mensaje cifrado a transmitir. Para descifrarlo se realizará el proceso inverso.

Para garantizar la seguridad en la transmisión, la palabra clave debería cambiarse cada vez. Si ese cambio se produce en connivencia con el receptor, se denomina cifrado *sincronizado*. Si esta variación se realiza sólo por el emisor que posteriormente lo transmite al receptor en la cabecera del mensaje, se denomina *autosincronizado*. Aunque en teoría este último resulta más seguro, en la práctica es difícil implementar un generador secuencial de estas características.

- ***Cifrados en bloque***: en esencia dividen el texto a transmitir en bloques de bits del mismo tamaño y posteriormente cada uno de ellos se transforma en otro según determine el proceso de cifrado teniendo en cuenta la clave elegida para ello; también mediante un "**XOR**". Valores típicos para las longitudes de los bloques suelen ser 64, 128, o 256 bits por bloque y garantizan una mayor seguridad que los cifrados secuenciales aunque su procesamiento conlleva un mayor tiempo que en los primeros, sobre todo en función del tamaño del bloque utilizado.

No obstante y para que esta mejora en las seguridad sea completa, debería de utilizarse lo que se denomina *vector de inicialización* de esta forma cada mensaje se generará atendiendo a una suma exclusiva del citado vector con el primer bloque de código, éste resultado se suma con el segundo bloque y así sucesivamente, la generación de esta encriptación será más resistente que la citada inicialmente y elimina la posibilidad de repetición de bloques encriptados que se formen a partir de bloques iguales de texto y que sí se pueden producir en el caso general.

No obstante la propia evolución tecnológica ha propiciado la aparición de nuevos sistemas para la rotura o desencriptación de claves. Hoy en día la seguridad de un sistema criptográfico viene en gran medida motivada por la cantidad del tiempo que supone llegar a romperlo. Si este tiempo es lo suficientemente largo el sistema se considerará seguro, pero en ningún caso

podemos llegar a pensar que sea invulnerable; al menos en el momento actual de la técnica.

Un paso más a la hora de incrementar este tiempo de rotura de un sistema criptográfico es el diseño de lo que se ha dado en llamar **Criptografía en clave pública**. En ella cada clave consta a su vez de dos claves, una privada en poder de una única persona y otra pública conocida por todo el mundo. Los mensajes se cifran con la clave pública y serán descifrados con la privada. De esta forma cualquiera puede cifrar mensajes, pero solo aquél que tenga la clave privada podrá descifrarlos.

Este nuevo diseño ha recibido la denominación de *criptografía asimétrica*, en oposición a la criptografía tradicional o *simétrica*; llamada así porque en esta última el emisor y el receptor empleaban la misma clave secreta.

Es precisamente en este contexto dónde surge la figura del tándem *autoridad certificadora-contraseña de usuario*. En él la autoridad certificadora se encargaría del diseño y emisión de una clave pública que, combinada con la contraseña de usuario (su clave privada), garantizaría la seguridad de la transacción de datos y la identidad del emisor y el receptor de los mismos. Ejemplos actuales de este sistema los podemos ver en los certificados de firma electrónica expedidos a través del proyecto CERES desde la Fábrica Nacional de Moneda y Timbre (FNMT.), o en el; ya citado al comienzo de este artículo; DNI electrónico en nuestro país.

5. Conclusiones finales

Con este artículo hemos realizado un breve viaje recorriendo las diferentes iniciativas criptográficas a lo largo de la historia. Sólo nos hemos parado en aquellos sistemas que en un primer momento nos han parecido más representativos en determinados períodos, bien sea por su carácter innovador o por sus curiosas características de funcionamiento. Evidentemente el mundo de la criptografía abarca campos de la ciencia que no hemos tenido tiempo de ver en esta primera aproximación, si bien la matemática, se ha constituido como un pilar consistente en su estructura, no es menos cierto que la lingüística, la psicología, y hoy en día la tecnología, tienen mucho que decir en el desarrollo de este arte.

Lo que se ha evidenciado en cualquier caso es la importancia que tiene el hecho de cifrar o no una información. El ejemplo de Enigma es más que evidente, pero no sólo debemos ceñirnos al ámbito militar. Transacciones habituales como las compras a través de Internet, la extracción de dinero en un cajero automático, la transferencia entre cuentas bancarias, o la emisión y recepción de un correo electrónico con datos sobre algún proyecto empresarial que debe quedar oculto a los ojos de la competencia, son otros ejemplos en los que se aprecia la importancia que la encriptación de datos puede tener en nuestra vida diaria.

A lo largo de los siguientes artículos intentaremos profundizar más en estas cuestiones, conoceremos alguno de los programas informáticos de criptografía que más eco han tenido en las últimas décadas, profundizaremos en sus restricciones y limitaciones; muchas veces motivadas por razones de tipo político amparadas en la denominada “seguridad nacional” , y veremos que ésta a permitido que salieran al mercado sistemas ya obsoletos o muy limitados y que hoy en día todos estamos utilizando sin apenas ser conscientes del peligro para nuestra información que ello supone. Un ejemplo de esto podría ser el limitado protocolo de seguridad de las redes Wi-Fi, algo que afortunadamente ya se está corrigiendo hoy en día.

De la misma forma seguiremos viendo como se pueden implementar en lenguajes de programación como JAVA, C o Pascal, algunos de los algoritmos más habituales de encriptado simétrico. El ejemplo visto en este mismo artículo nos muestra las posibilidades que a nivel software existen hoy día en lo que a criptografía aplicada se refiere.

Pero con independencia de todo ello hay una cosa que nos debe quedar clara desde un principio. Cualquiera que sea el nivel de seguridad de un sistema criptográfico existe una importante vulnerabilidad en su misma fortaleza: su clave. Si no ponemos cuidado en salvaguardar esa clave nos veremos abocados a fracasar en el intento de mantener la integridad y protección de la información que poseemos. Con lo que el factor humano; una vez más; no puede ser sustituido por la tecnología. Es posible que hoy día las máquinas sean capaces de compilar algoritmos complejos y robustos, pero al otro lado del teclado siempre habrá un ser humano, con su psicología, sus virtudes, sus defectos y sus claves y contraseñas muy probablemente anotadas en un papel; o peor aún, en algún archivo de texto dentro de su sistema; y haciendo referencia a lugares, hechos, fechas, momentos, amigos o familiares. Y de la misma forma, al otro lado de otro teclado, en un lugar distinto geográficamente hablando; aunque no necesariamente lejano; habrá otro ser humano que intentará por todos los medios a su alcance descubrir esa clave necesaria para beneficiarse, de una manera deshonesta, de la información que tan confiadamente atesoramos.

6. Notas aclaratorias

1.- ***Cifradores poligráficos***: el cifrado por sustitución es un método de cifrado por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular; las "unidades" pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros. El receptor descifra el texto realizando la sustitución inversa. Cuando un cifrado de estas características opera sobre grupos de letras se denomina, “poligráfico”.

2.- ***Thomas Jefferson*** *(13 de abril de 1743 - 4 de Julio de 1826)*: Fue el tercer Presidente de los Estados Unidos de América, ocupando el cargo de 1801 a 1809. Fue también Vicepresidente entre 1797 y 1801, gobernador de Virginia

(1779-1781), principal autor de la *Declaración de Independencia* de los Estados Unidos y fundador de la Universidad de Virginia.

3.- ***Étienne Bazeries*** *(21 August 1846 - 7 November 1931)*: Militar francés y criptoanalista activo entre 1890 y la Primera Guerra Mundial. Está considerado como un hito en la literatura sobre el criptoanálisis.

4.- ***Marian Rejewski*** *(16 de agosto de 1905 - 13 de febrero de 1980)*: Matemático y criptógrafo polaco que, en 1932, descifró la máquina Enigma, el dispositivo de cifrado principal usado por Alemania en la Segunda Guerra Mundial. El éxito de Rejewski y sus colegas impulsaron a Inglaterra a leer los mensajes de Enigma, lo cual contribuyó, quizás decisivamente, a la derrota de la Alemania Nazi.

5.- ***Alan Mathison Turing*** *(23 de junio de 1912- 7 de junio de 1954)*: Científico, matemático de la informática y la criptografía, y filósofo inglés. Considerado uno de los padres de la computación. Su mayor aportación a la ciencia informática fue su Máquina de Turing, una máquina de estados base de lo que posteriormente sería el desarrollo matemático de los estudios sobre computación e inteligencia artificial.

7. Bibliografía e imágenes

De estás páginas y libros se ha sacado la mayor parte de la información necesaria para escribir este artículo, así como las fotografías que lo ilustran.

-J. Ramió Aguirre. "*Aplicaciones Criptográficas".* Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid. España. 1999.

-E. Garcia, M. A. Lopez, J. J. Ortega. *"Una introducción a la Criptografía".* Departamento de Matemáticas E.S. de Informática de la Universidad de Castilla-La Mancha. 2005.

- http://www.kriptopolis.org

- http://www.wikipedia.org/Enigma_(maquina)

- http://www.kstor.com.ar/

- http://www.lpsi.eui.upm.es/SInformatica/diapositivas.htm

- http://www.cert.fnmt.es/

ENGLISH ZONE

Por: Gloria Murillo Cordero

Coordinadora del Boletín de la rama IEEE – UNED.
E-mail: gmcordero@indra.es

1. Over & Under

El prefijo **"over"** a veces aporta la idea de **"exceso"** como en el caso del verbo "to overwork" que significa "trabajar en exceso" o "trabajar más de la cuenta". Por cierto, no se dice "o vér" sino "ó va".

- Tengo que tener cuidado por ahora, ya que gasté más de la cuenta el mes pasado.
- I have to be careful at the moment as I **overspent** last month.

- Sobreestimó el interés popular en el evento. Fue un fracaso total.
- He completely **overestimated** public interest in the event. It was a complete flop.

- No pegué ojo porque me harté de comer anoche.
- I didn't sleep a wink as I seriously **overate** last night.

- Debes moderarte un poco. Estás trabajando más de la cuenta y eso puede llevar a serios problemas de salud.
- You must cut down a bit. You're **overworking** and that can lead to serious health problems.

- La reunión duró dos horas más de lo previsto.
- The meeting **overran** by more than two hours.

Como es lógico, el prefijo contrario **"under-"** equivale al prefijo **"infra-"** en castellano.

- Lo siento, creo que no cociné lo suficiente la carne.
- I'm sorry but I think I **undercooked** the meat.

- Había subestimado a mi contrincante. Por eso perdí la concentración y acabé perdiendo el partido.
- I had **underestimated** my opponent which is why I lost my concentration and ended up losing the match.

- No estamos vendiendo nuestro producto lo suficientemente caro.

- We're **underpricing** our product.

- Tengo la impresión de que estamos infrautilizando nuestros recursos.
- I get the impression we're **underusing** our resources.

- Cuando llegué a la reunión me di cuenta de que no iba vestido adecuadamente para la ocasión.
- When I got to the meeting I realised I had **underdressed** for the occasion.

2. Key Learning

Cuidado con el verbo irregular "to wake". El pasado es "woke", mientras que el participio es "woken".

If you don't wake up the little girl, I'll wake her up.

3. One expression

The tickets are sold out.

Se han agotado las entradas.

4. One phrasal verb

To stick up for - Dar la cara por / Defender

Nobody ever sticks up for him

Nunca nadie da la cara por él.

5. One adjective

Wee - Pequeñito

Would you like a wee drink before your dinner?

6. Brain Teasers

Con la realización del siguiente ejercicio además de comprender la situación debemos de aplicar la lógica, ya que tenemos una serie de “rompecabezas” en los cuales tenemos que adivinar la solución de las diferentes situaciones que se nos proponen.

THE PHOTOGRAPH

A man is looking at a photograph when someone asks him "Whose picture is that?"

The man replies "I have no brothers or sisters, but this man's father is my father's son"

Whose photo is the man looking at?[4]

THE ACCIDENT

Mr. Jones and his son Alfred are travelling together when therir aeroplane crashes. The father is killed, and Alfred is seriously injured. Arriving at the hospital emergency room, the head surgeon cries "I cannot operate on this patient, he's my son Alfred!"

How can you explain this?[5]

ENGLISH YOLK OR EGG YOLK?

Which of these two phrases is correct?

"The egg's yolk is white" or "the egg yolk is white"[6]

---

[4] THE PHOTOGRAPH

The man in the photograph is the man's own son.

[5] THE ACCIDENT

The head surgeon is the Alfred's mother.

[6] EGG'S YOLK OR EGG YOLK?

Neither. Egg yolks are yellow, not white.

THE ROBBERY

Following a robbery, three suspects, Richard, David and Tommy are taken to the Police station for questioning. Here are the facts that emerged from the investigation.

No one other than these three was implicated in the crime.

Richard never works alone, he always employs at least one accomplice.

Tonny is innocent.

Is David guilty or innocent?[7]

A PROBLEM OF TIME

A train leaves London for Edinburgh. An hour later another train leaves Edinburgh for London. The two trains travel at exactly the same speed. Which of the two will be closest to London when they meet?[8]

HANGED OR DROWNED?

A man has committed a crime punishable by death. The man must make a statement. If the statement is true he will be drowned; if the statement is false he will he hanged. What statement should he issue in order to confuse his executioners?.[9]

---

[7] **THE ROBBERY**

If Richard is innocent and Tommy is innocent, David must be guilty. If Richard is guilty and Tommy is innocent, Richard's only possible accomplice is David. David must therefore be guilty in either case.

[8] **A PROBLEM OF TIME**

Obviously, when they meet, they will both be the same distance from London.

[9] **HANGED OR DROWNED**

All he need say is "I'll be hanged"

7. Links

- http://www.vausys.com/
- http://www.vaughanradio.com/reproductor/player2.htm
- http://www.mansioningles.com/

INFORMACIÓN GENERAL RESUMIDA

La Rama de Estudiantes creada en la Universidad Nacional de Educación a Distancia (UNED) tiene por objetivo principal **la difusión de la ciencia y la tecnología**.

Se consolidó inicialmente con 37 miembros en noviembre del año 2004 y actualmente cuenta ya con 70 miembros en activo.

La información general sobre sus actividades e información de cómo hacerse miembro se puede ver en la página Web:

http:// www.ieec.uned.es/IEEE/

dentro del enlace de la Rama de Estudiantes.

Las actividades principales que las Ramas de España realizan son: charlas, cursos, congresos, concursos, actividades educativas, visitas a empresas y organizaciones, interrelación cultural y multidisciplinar y cualquier actividad que quiera desarrollar cada uno de sus miembros.

Actualmente puede participar cualquier estudiante de las carreras de Informática y de Industriales de la UNED. Para conocer más información sobre el IEEE, las Ramas de España y sus posibilidades se recomienda leer los primeros artículos de éste Boletín y visitar la página Web para ver los boletines previos. De todas formas cualquier información o consulta puede dirigirse a Sergio Martín:

sergio.martin@ieee.org

Esperamos que os haya gustado a todos éste décimo Boletín y agradecer una vez más a todos los autores el haber participado en el mismo haciéndolo posible.

UN SALUDO

Sergio Martín
Presidente de la Rama de Estudiantes IEEE-UNED

RAMA DE ESTUDIANTES IEEE-UNED
1 - SEPTIEMBRE - 2008 (BOLETIN Nº 10)