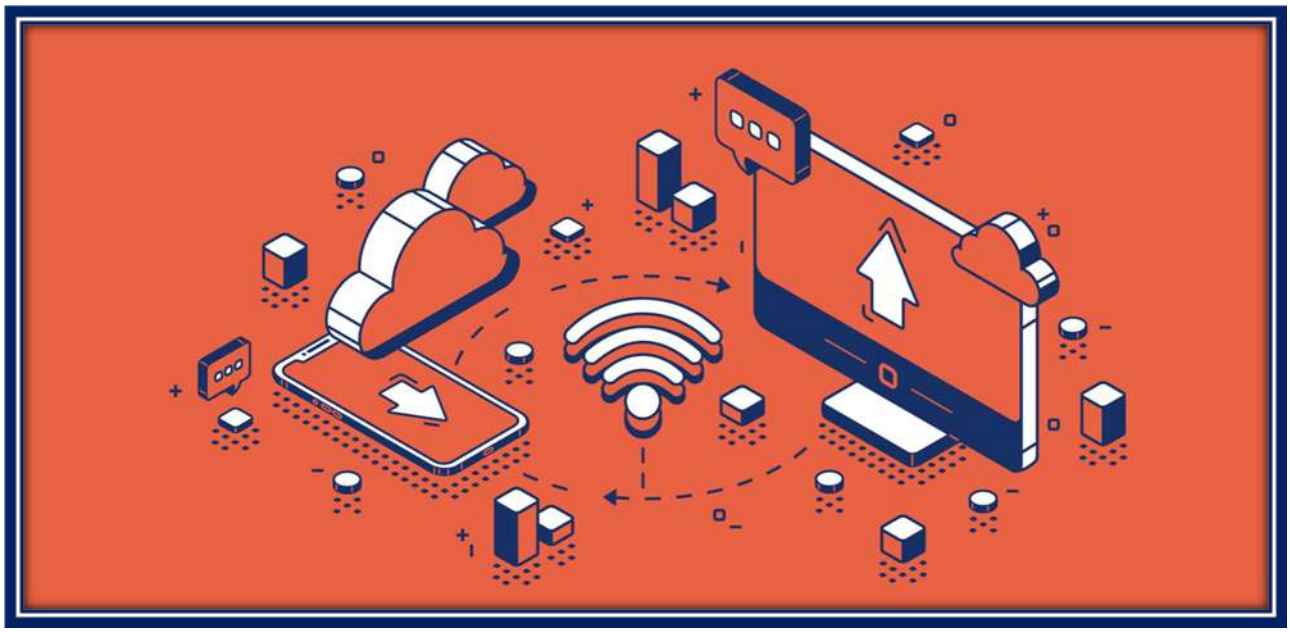
REDES INALÁMBRICAS

WIFI - PROTECTED ACCESS *WPA*



SISTEMAS INFORMÁTICOS 1º DAW

ALEJANDRO PONCE

JAVIER CALLEJÓN

ÍNDICE

1. **PORTADA** P.01
2. **ÍNDICE** P.02
3. **INTRODUCCIÓN** P.03
4. **DESARROLLO** P.04 - 12
5. **BIBLIOGRAFÍA** P.13

INTRODUCCIÓN

En este trabajo abordaremos las Redes inalámbricas ***WIFI***. Vamos a repasar su historia y evolución hasta día de hoy, trataremos los estándares más importantes, los protocolos de integridad y seguridad.

En este documento no se pretende hacer una profundización técnica sobre los canales de transmisión de datos a nivel inalámbrico, ni sus unidades de medida o frecuencia, sino que más bien dar una visión general y comprensible para todo el público general interesado en la temática.

REDES INALÁMBRICAS *WIFI*

WIFI es una abreviación de ***Wi****reless* ***Fi****delity*, y es un medio de proporcionar internet de banda ancha a uno o más dispositivos por medio de transmisores inalámbricos y señales de radio.

HISTORIA Y EVOLUCIÓN

Si nos remontamos al principio de todo, se conoce que la primera transmisión por medios inalámbricos de ondas electromagnéticas la realizo el físico alemán ***Rudolf Hertz*** en el año **1888**.

Hertz utilizó un oscilador como emisor y un resonador como receptor. En medio año este tipo de transmisión ya era usada como medio de comunicación de ondas de radio.

1889, ***Guillermo Marconi*** estableció las primeras comunicaciones inalámbricas a través del canal de la Mancha.

1907, se transmitieron los primeros mensajes completos que cruzaron el Océano Atlántico.

HEDY KIESLER / HEDY LAMARR

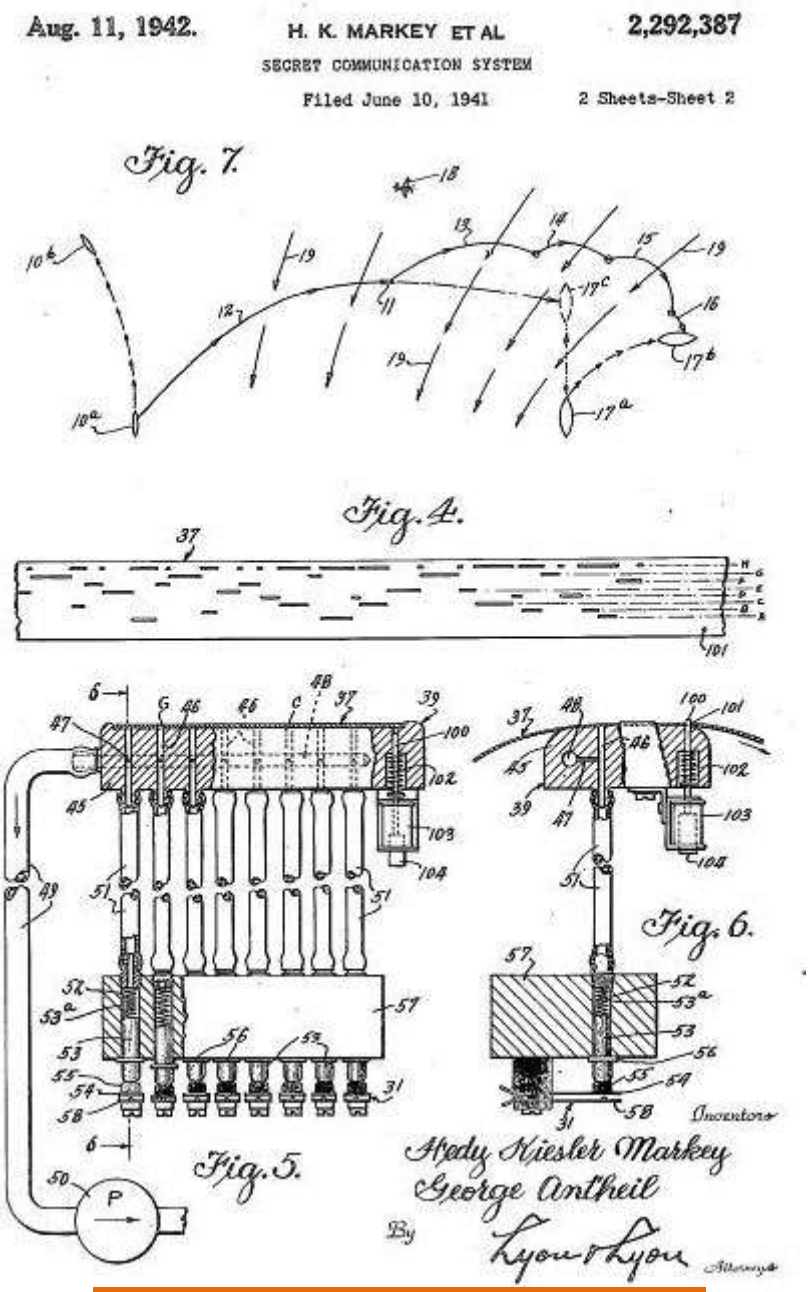
Es imperativo hablar sobre ***Hedy Lamarr*** (9 de septiembre 1914 - 19 de enero 2000).

Hedy Lamarr
Crédito: Pieter Franken

- Fue una estrella de Hollywood que dedicaba las noches a desarrollar un **sistema de salto de frecuencias de comunicación**.
- Fue Inventora del precursor del ***WIFI***, que de día interpretaba a ***Dalila*** bajo la dirección de ***Cecil B. DeMille***.
- Fue la esposa trofeo del judío ***Fritz Mandl*** que vendía armas a Hitler y Mussolini.
- Fue la emigrante que contó a las autoridades de ***EE.UU*** todo lo que sabía sobre el armamento de las **potencias del Eje**.

Y por todo esto es imperativo hablar sobre ella.

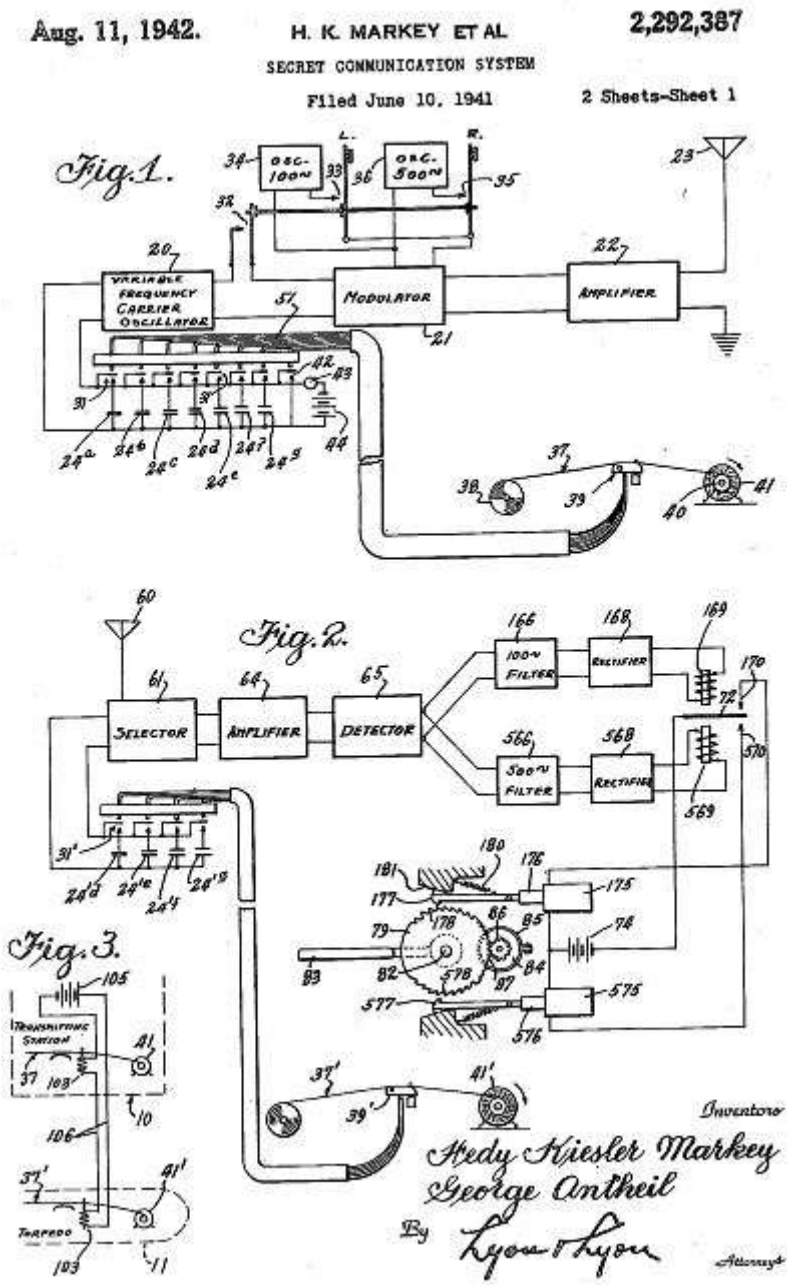
Tras escapar de su marido y emigrar a ***EEUU***, reanudó su carrera en Hollywood con su nuevo nombre ***Hedy Lamarr***, donde conoció a ***George Antheil*** pianista y compositor pionero de la música mecanizada y la sincronización automática. Juntos pensaron en aplicar el principio de la pianola a los torpedos dirigidos por radio; es decir, emplear rollos de papel perforado para que la frecuencia de comunicación fuera saltando entre 88 valores distintos (el número de teclas del piano), según una secuencia que solo podrían conocer quienes poseyeran una clave para impedir que el sistema fuera interceptado.


Aug. 11, 1942. H. K. MARKEY ET AL 2,292,387
SECRET COMMUNICATION SYSTEM
Filed June 10, 1941 2 Sheets-Sheet 2
Fig. 7.
Fig. 4.
Fig. 6.
Fig. 5.
Inventors
Hedy Kiesler Markey
George Antheil
By Lyon & Lyon
Attorneys

Nº patente 2.292.387, publicada el 11 de agosto de 1942
Nombre: Sistema de comunicación secreta

El sistema no se explotó de inmediato supuestamente por dos razones según el escritor de su biografía ***Stephen Michael Shearer*** el cual cito a continuación:

1ª "El gobierno no entendió o no conceptualizó entonces la comunicación inalámbrica"
2ª "Posiblemente el invento fue aparcado porque se consideraba a ***Lamarr*** la chica más guapa del mundo y debemos tener en cuenta que en esa época nadie tomaba en serio a una mujer bella en cuestiones intelectuales"



Nº patente 2.292.387, publicada el 11 de agosto de 1942
Nombre: Sistema de comunicación secreta

Tras **20** años en **1959** con la patente expirada sin producir ni un solo dólar, se utilizó para desarrollar comunicaciones militares inalámbricas para misiles guiados. Esto llevaría juntamente con la invención de los teléfonos móviles, al fundamento de todas las comunicaciones inalámbricas que conocemos a día de hoy como el ***WIFI***.

En **mayo** de **2014** ***EEUU*** incorporó a ***Lamarr*** y ***Antheil*** al ***Inventor Hall of Fame.***

1971, la *Universidad de* ***Hawaii***, concibió el primer sistema de comunicación de paquetes mediante red por radio (***ALOHA***). Fue la primera red inalámbrica y estaba formada por siete ordenadores situados en distintas islas que podían comunicarse con el ordenador central.

En el inicio se generó un gran desorden ya que los fabricantes de tecnologías inalámbricas a principios de los 90, creaban sus propios dispositivos bajo estándares personalizados lo que hacía que los equipos fuesen incompatibles entre diferentes marcas.

Fueron las empresas ***Nokia*** y ***Symbol technologies*** quienes crearon la ***WECA*** (*Wireless Ethernet Compatibility Alliance*), que en **2003** paso a llamarse **Wi-Fi Alliance**, con la finalidad de crear un estándar para que todos los dispositivos fueran compatibles entre sí y poder masificar el uso de la tecnología.

1997, llega a los consumidores finales por primera vez el ***WIFI*** gracias a la creación del comité **802.11**, donde se dio paso a la estandarización **IEEE 802.11**, denominación que hace referencia a la estandarización de comunicación para redes de área local inalámbricas (***WLAN***).

WIFI A / WIFI B

1999, los fabricantes adoptan estos estándares para comercializar ***WIFI*** con ***WIFI B*** se estableció una capa física para usar el espectro de extensión de secuencia directa, o DSSS. Este estándar operaba en la banda de ***2.4GHZ*** mantenida hasta día de hoy, y limitaba la velocidad de envío de datos a ***11Mbps***.

El ***WIFI A*** corría de forma paralela al ***B*** pero las dificultades técnicas en la fabricación de componentes compatibles con la frecuencia que utilizaba de ***5GHZ*** supusieron que le WIFI B se convirtiese en el más popular relegando al ***WIFI A*** a un segundo plano pese a su superioridad en velocidad de transferencia ***54Mbps***, hasta su adhesión al ***WIFI AC*** años mas tarde.

ESTÁNDAR 802.11G

2003, hasta esta fecha la comisión de estándares estuvo realizando la unión de todas las tecnologías desarrolladas hasta el momento para crear este estándar.

Se mejoraron los *router* para que tuvieran más potencia en su señal y pudieran cubrir mayor área. A partir de este punto los *router* comenzaron a competir con los otros tipos de conexiones.

ESTÁNDAR 802.11N

2009, aparece el estándar **802.11N**, el cual fue una revolución en el mercado incorporando los avances logrados y añadiendo nuevos avances:

- Implementación de hasta **4** antenas aumentando rendimiento y permitiendo que cualquiera de las antenas pudiera "*caerse*" y seguir funcionando. **MIMO** (***M****ultiple* ***I****nput* ***M****ultiple* ***O****utput).*

- Aumento de velocidad hasta los ***600Mbps***.

ESTÁNDAR 802.11AC Y 801.11ax

2013, con el estándar **802.11AC** llega el nacimiento de las redes duales y otro gran salto de velocidad soportando velocidades de hasta **7Gbps**.

2018, llega el estándar **801.11AX** y el **MIMO-OFDA** este estándar nace bajo la idea de mejorar el consumo de los dispositivos que hacen uso de él, tales como los teléfonos móviles entre otros. Trae un aumento de velocidad hasta los **8** ***Gbps*** y mediante la tecnología ***MIMO-OFDA*** se dobla la capacidad de enviar transmisiones de **4** a **8** simultáneamente.

ACTUALIDAD *WIFI 6*

2019, la ***WI-FI Alliance*** introduce una nueva denominación para los dispositivos y redes compatibles con cada estándar con el objetivo de facilitar la identificación y diferenciación entre redes ***WIFI*** es por eso que recibe el nombre de ***WIFI 6*** en lugar de estándar **802.11AX**. Es compatible con protocolos anteriores, proporciona más alcance, mejor cobertura incluso en espacios saturados y un aumento de velocidad hasta los ***10Gbps***.

PROTOCOLO WEP (WIRED EQUIVALENT PRIVACY)

Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas.

En **1999**, el sistema de cifrado ***WEP*** fue el protocolo usado para las redes ***Wireless***, y que fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

El protocolo ***WEP*** usa el algoritmo de cifrado ***RC4*** para la confidencialidad (capa **2** del modelo OSI), que se transmite utilizando claves de **64** o de **128** bits.

¿CÓMO FUNCIONA *RC4?*

RC4 funciona expandiendo una semilla (***seed*** en inglés) para generar una secuencia de número *pseudoaleatorios* de mayor tamaño. Esta secuencia de número *pseudoaleatorio* se unifica con el mensaje mediante la operación **XOR** y lo que se obtiene al hacer el **XOR** del mensaje en claro con la secuencia de números *pseudoaleatorios* es el mensaje **cifrado/encriptado**.

El algoritmo de encriptación de ***WEP*** es el siguiente:

1. Se calcula un **CRC** de **32** bits de los datos. Este **CRC-32** es el método que propone ***WEP*** para garantizar la integridad de los mensajes *(**ICV**, Integrity Check Value).*
2. Se concatena la clave secreta a continuación del **vector de inicialización** (**IV**) formado el ***seed***.

3. El ***PRNG*** (*Pseudo-Random Number Generator*) de ***RC4*** genera una secuencia de caracteres *pseudoaleatorios* (***keystream***), a partir del ***seed***, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (***XOR***) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el **IV** (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama ***IEEE 802.11*** (*Familia de normas inalámbricas creada por el Instituto de Ingenieros Eléctricos y Electrónicos*).

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el ***seed*** y con ello podrá generar el ***keystream***. Realizando el ***XOR*** entre los datos recibidos y el ***keystream*** se obtendrá el mensaje sin cifrar (datos y ***CRC-32***). A continuación se comprobara que el ***CRC-32*** es correcto.

TEMPORAL KEY INTEGRITY PROTOCOL - TKIP

TKIP es una solución temporal que resuelve el problema de la reutilización del Vector de Inicialización de la encriptación ***WEP*** mediante mecanismos mejorados con el nuevo estándar ***802.11*** para mejorar la encriptación de datos inalámbricos.

Proporciona variedad de claves por paquete, control de la integridad del mensaje y un mecanismo de reintroducción de claves cada **10.000** paquetes o **10 KB**.

Ventajas.

- Los puntos de acceso basados en ***WEP*** se pueden actualizar a ***TKIP*** a través de los parches de firmware de manera relativamente simple.

EL PROTOCOLO *WPA*

Es un protocolo para proteger redes inalámbricas, creado para corregir las deficiencias del sistema previo ***WEP***.

Mejoras respecto a ***WEP***:

- Soluciona la debilidad de claves mediante la inclusión de vectores de longitud ***48 bits*** frente a los ***24*** de ***WEP***. Estos permiten generar claves de ***2*** elevado a ***48*** combinaciones de claves diferentes.
- Se incluye un nuevo código para la integridad de los mensajes denominado MIC.
- Las claves se generan de forma dinámica y se distribuyen automáticamente por lo que se evita modificarlas manualmente cada cierto tiempo.
- Se sustituye el mecanismo de autentificación así como la posibilidad de verificar las direcciones ***MAC*** de las estaciones.
- Su inconveniente es que requiere mayor infraestructura ya que requiere implementar un servidor ***RADIUS*** (*Remote Authentication Dial-In User Service*) que es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

Modos de funcionamiento:

- ***WPA-Personal***
- ***WPA-Empresarial***

EL PROTOCOLO *WPA-PSK*

Es el sistema más simple de control de acceso tras ***WEP***, a efectos prácticos tiene la misma dificultad de configuración que ***WEP***, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad.

PSK (*PreShared Key*) a efectos del cliente basa su seguridad en una contraseña compartida. ***WPA-PSK*** usa una clave de acceso de una longitud entre ***8*** y ***63*** caracteres, que es la clave compartida. Al igual que ocurría con ***WEP***, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red. Las características de ***WPA-PSK*** lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

REFERENCIAS Y BIBLIOGRAFÍA

- https://www.xataka.com/especiales/que-wifi-6-que-va-a-mejorar-tu-red-wifi-casa-cuando-te-conectes-a-publica
  Fecha consulta: 15/5/2021
- https://www.bbvaopenmind.com/tecnologia/visionarios/hedy-lamarr-la-actriz-que-invento-el-wireless/
  Fecha consulta: 15/5/2021
- https://www.xatakamovil.com/conectividad/11mbps-11gbps-evolucion-estandares-wifi-wifi-802-11ax
  Fecha consulta: 15/5/2021
- https://es.wikipedia.org/wiki/Wifi
  Fecha consulta: 15/5/2021
- https://softwarelab.org/es/que-es-wifi-que-significa-y-para-que-sirve/
  Fecha consulta: 15/5/2021
- Biografía de ***HEDY LAMARR*** citada en este documento y escrita por ***Stephen Michael Shearer.*** ***"Beautiful: The life of Hedy Lamarr"***