

Mujeres en informática

Hoy es **8 de marzo**, un día muy especial pues es el día de la mujer. Ojalá un día así no hiciese falta porque fuera obvio que todos tenemos los mismos derechos, pero dado que existe el día y que queda lucha por hacer, vamos a dedicar un momento a seguir los pasos de las mujeres que marcaron historia en informática, como Ada Lovelace, de la que ya hablamos hace tiempo. Comencemos.

Hace tiempo estuvimos hablando de criptografía, y cómo las matemáticas de la criptografía llevan existiendo desde siempre para comunicar mensajes secretos. Durante la 2GM, este era un recurso común, y en este contexto nació la llamada Máquina Enigma, que los alemanes utilizaban para enviar mensajes. Existía todo un despliegue de personal dedicado a descifrarlo en el servicio secreto de Inglaterra, y la mayoría de las llamadas **“codebreakers”** eran mujeres, que trabajaban en un lugar llamado Bletchley Park. Las codebreakers tenían que enfrentarse a un complicado sistema de encriptación, pero finalmente sus aportaciones consiguieron reducir los años de guerra. Echemos un ojo a lo que investigaban...

La máquina enigma es un sistema que juega con **entremezclar letras** para generar un mensaje cifrado. Por ejemplo, si nuestro alfabeto es:

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

Teniendo un alfabeto A, si decimos que nuestro sistema de encriptación es A+1 (es decir, la A es una B, la B es una C y así) nuestro alfabeto sería:

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 A

Y así, un mensaje como **“HOLA”** se convertiría en...

¿En qué se convertiría si nuestro **Alfabeto nuevo = Alfabeto normal + 1**?

Bien, si tenemos esto en cuenta, finalmente sacaremos que $A_{Nuevo} = A_{Normal} + \text{número de vueltas}$, en nuestro caso 1. Pero podríamos darle 2, 3 o todas las vueltas que quisiéramos. Esta es una de las variables que contempla Enigma.

Bien, pero ¿qué ocurriría si además podemos sustituir algunas letras? Veamos. Volvemos a nuestro alfabeto normal:

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

Pero decidimos que la R sea igual a la X. De modo que nuestro alfabeto modificado sería:

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

Y sobre ese, decidimos hacer 2 vueltas como las de antes, es decir, $A = A + 2 \rightarrow A = C$.
Nuestro alfabeto es:

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

Este es el segundo sistema que utilizaba la máquina Enigma. Sin embargo, precisamente lo que hacía esta máquina, era proporcionar una herramienta que pudiera configurarse con varias vueltas y varias sustituciones a cada mensaje, ¡imagina que trabajazo se dieron para “romper” los mensajes ocultos! El equipo de Bletchley Park, tras mucho análisis matemático y trabajo, lo consiguió.

Diseñemos nuestro propio mensaje con Enigma, y escribamos adecuadamente su ecuación. **¿Cómo lo haremos?**

Pensemos primero en las letras a sustituir. Escribe los equivalentes a 4 letras aquí:

| | | | |
|---------|--|---|--|
| Letra 1 | | = | |
| Letra 2 | | = | |
| Letra 3 | | = | |
| Letra 4 | | = | |

Edita este alfabeto con las letras modificadas:

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

Ahora piensa un número del 1 al 5, y ese será el número de vueltas que de nuestro alfabeto.

Alfabeto Nuevo = Alfabeto Normal + []

Escribe el Alfabeto nuevo aquí:

Bien, ya tenemos el Alfabeto listo. Siguiendo las indicaciones creadas, **traduce**:

| | | |
|------|---|--|
| RAFA | = | |
| HOLA | = | |
| | = | |

Además de las mujeres de Bletchley Park, existen otras mujeres que han hecho historia en informática y gracias a ellas conocemos la tecnología tal cual es hoy. Por ejemplo, hablemos del origen de la **WIFI**.

A principios del siglo XX, nació una mujer llamada Hedy Lamarr. Si la buscamos en internet, lo que probablemente nos aparezca sean sus películas, dado que era actriz. Sin embargo esta famosa actriz esconde algo mucho más grande, y es que era una niña superdotada que comenzó a estudiar ingeniería a los 16 años. Desgraciadamente en su juventud, y debido a un matrimonio concertado contra su voluntad, se vio rodeada de un ambiente peligroso, dado que su marido era nazi. Horrorizada por lo que descubrió ofreció su ayuda contra los nazis, y así diseñó lo que posteriormente se conocía como el sistema **WIFI**.



¿Cómo funciona la Wifi?

Conociendo lo que sabes sobre la wifi, ¿Cómo crees que funciona?

Como ya sabrás, la Wifi nos permite conectarnos inalámbricamente a internet. Ahora parece algo muy normal, sin embargo hace no tanto teníamos que andar usando cables ethernet (que aún así se siguen usando) para todo. La wifi funciona a través de ondas, ondas muy parecidas a las de radio, que transmite una antena.

A grosso modo, puede pensarse en la Wifi como una conexión parecida a la radio pero donde ambos nodos transmiten y reciben. El adaptador inalámbrico de un ordenador convierte el contenido de lo que mandamos en datos que se pueden enviar a través de una onda, posteriormente estos datos son recibidos y cifrados en el router, que está físicamente conectado con un cable como el mencionado.

La wifi es un sistema de comunicación inalámbrico muy común, y es por esto que existe un importante sector de seguridad informática dedicada al análisis del tráfico en una red determinada. Para ello por ejemplo se utilizan programas como [Wireshark](#), [Bro](#), y otros complementos.

¿Qué tipo de información crees que puede sacarse de una red?

Siguiendo en la línea que nos concierne hoy, y avanzando un poco más en la historia, durante los años 80 y 90 hubo un gran movimiento de personas jóvenes (generalmente de instituto) interesadas en la informática y que tenían grandes capacidades. Algunos de estos grupos aprovechaban sus capacidades para delinquir, otros para aprender y enseñar. Aún se conservan [algunos tomos de revistas online](#) que escribían estos individuos. En cualquier caso, entre ellos, destacaban también algunas chicas, que se dedicaban a utilizar lo ya mencionado para analizar redes, descubrir errores de seguridad, y similar. Entre ellas estaba Natasha Grigory.



Sus habilidades con seguridad informática, permitieron hacer grandes avances en investigaciones policiales. Vamos a ponernos en su piel por un momento.

Imaginemos que, usando uno de los programas mencionados anteriormente, y bajo el mando del equipo de Natasha, hemos conseguido la siguiente información:

Leyendo datos de la red...

Comunicación 1:

La ip

94.23.40.150

se ha conectado a la página https://comprodrogas_facil.net y ha enviado un paquete encriptado

.....

La página https://comprodrogas_facil.net ha respondido con un paquete encriptado

....

La ip

94.23.40.150

se ha conectado a la página http://comprodrogas_facil_registro.net y ha enviado un paquete

¿Qué conclusiones podemos sacar de aquí? Sigamos una guía:

- ¿De dónde es la ip que hemos localizado?
- ¿A dónde se conectaba?
- ¿Recuerdas la diferencia entre HTTP y HTTPS?
- Con los datos que hemos conseguido ¿Podríamos pillarle?

En el mundo real, los análisis de este tipo son mucho más complejos, la mayoría de las conexiones están encriptadas y las IP van cambiando, sin tener que coincidir necesariamente con el país al que apuntan.

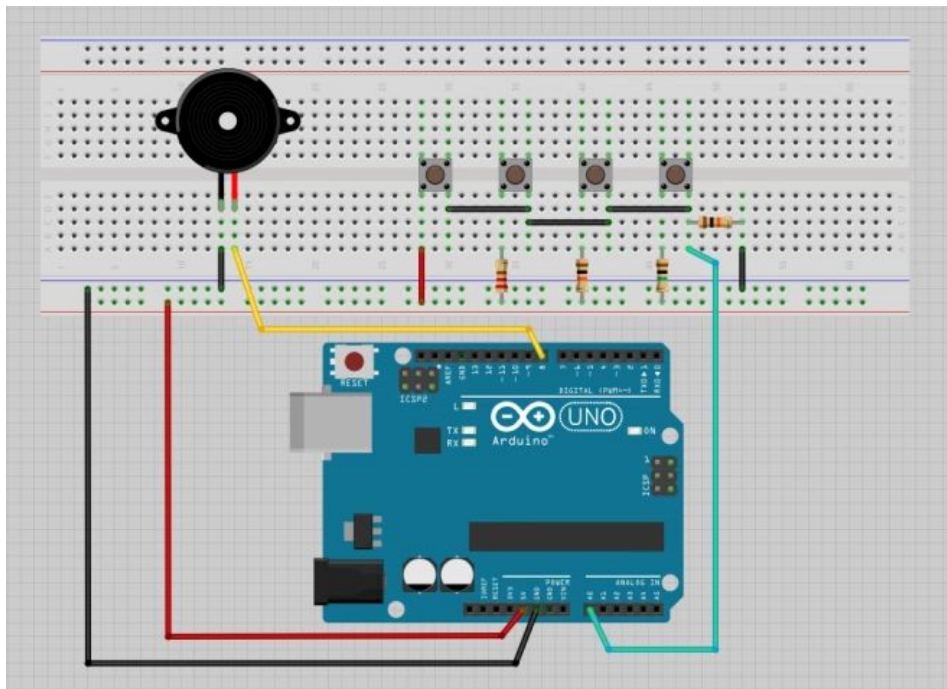
Día tras día, montones de profesionales, y entre ellos, varias mujeres, se dedican a investigar casos de esta índole, y en informática en general.

Ahora, arreglemos lo anterior

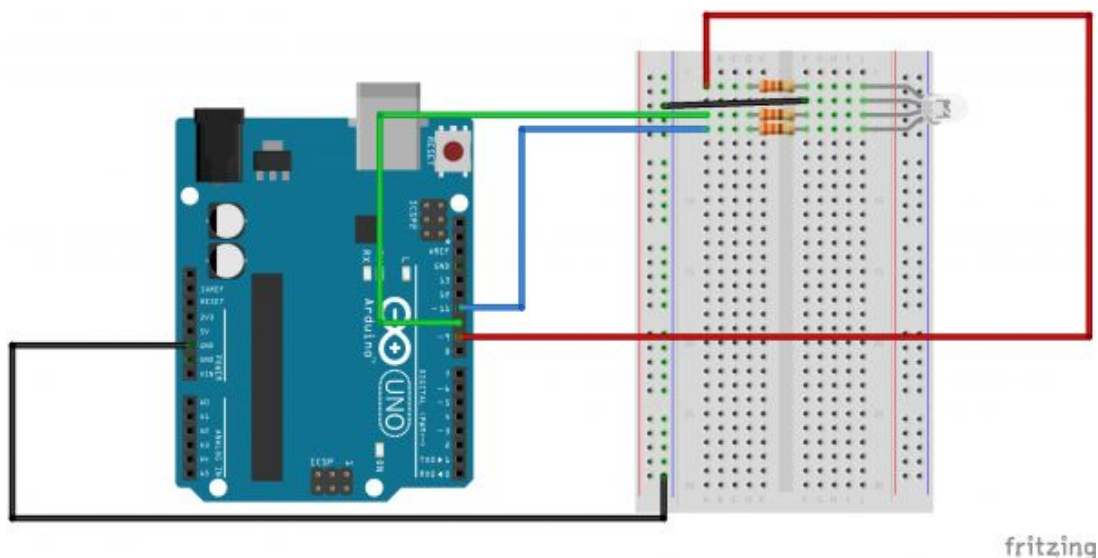
El día pasado estuvimos trabajando en un teclado con el piezo. Como este no funcionaba, probemos a sustituir el piezo por un led RGB.

¿Recuerdas cómo funciona un led **RGB**?

Para sustituirlo, tenemos que hacer cambios tanto en el hardware como en el software.
¡Pero tranquilo! no tenemos que cambiarlo todo. Observa el circuito físico del día pasado.



El piezo, realmente solo ocupa un pin digital y GND. Eliminemos sólo esa parte, y el piezo, claro está. Ahora vamos a incluir nuestro LED rgb. El led rgb es el siguiente:



Como ves, a parte de ocupar GND, también ocupa 3 pines digitales (Red, Green y Blue) convenientemente indicados con cables de colores en la imagen. Añadámoslo a nuestro circuito que ya tiene el teclado.

Si todo está correcto, ahora nos toca incluir el software.

```
int buttons[6];
int buttons[0] = 2;
```

```
//QUITAMOS int notes[] = {262,294,330,349};
int RED_PIN = 9;
int GREEN_PIN = 10;
int BLUE_PIN = 11;

void setup(){

    Serial.begin(9600);
    pinMode(RED_PIN, OUTPUT);
    pinMode(GREEN_PIN, OUTPUT);
    pinMode(BLUE_PIN, OUTPUT);

}
void loop(){

    int keyVal = analogRead(A0);
    Serial.println(keyVal);

    if(keyVal >= 990 && keyVal <= 1010){
        digitalWrite(RED_PIN, LOW);;
    }
    else if(keyVal >= 505 && keyVal <= 515){
        digitalWrite(GREEN_PIN, LOW);
    }
    else(keyVal >= 5 && keyVal <= 10){
        digitalWrite(BLUE_PIN, LOW);;
    }

}

}
```

Si sigue sin funcionar:

- Observemos el Serial Monitor, y sus rangos de keyVal. Corrijamos sobre la marcha.