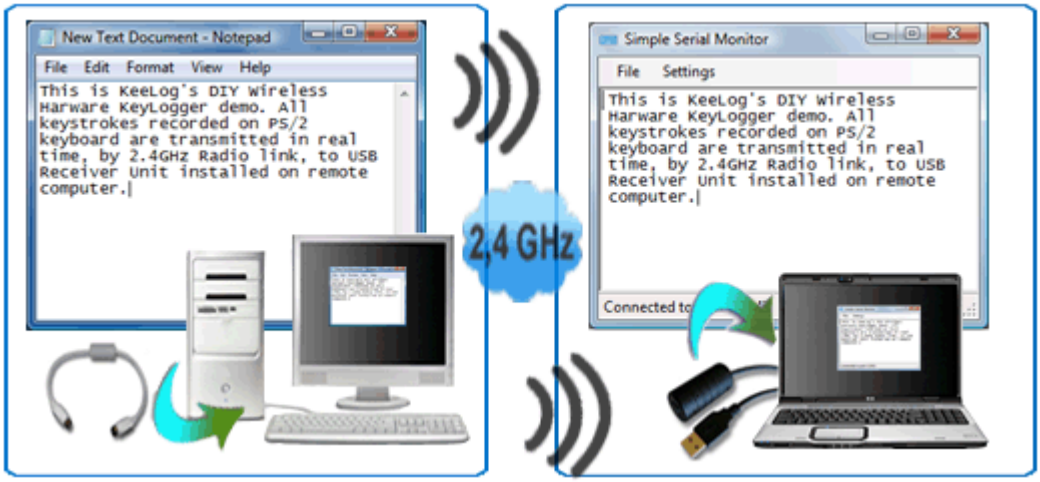
Keylogger Inalámbrico

¡Hazlo tú mismo!



Introducción

¿Conoces la noción de keylogger por hardware? El keylogger por hardware es una solución perfecta que sirve para seguir la actividad del usuario de ordenador con escaso riesgo de su detección. El keylogger por hardware es un dispositivo en un 100% electrónico así que no requiere acceso al sistema operativo, no deja ningunas huellas y los programas no son capaces de detectar este tipo de dispositivo. El concepto del keylogger por hardware tiene un defecto: para recuperar los datos intercaptados es necesario el acceso físico al dispositivo. Este problema, por fin, ha encontrado una solución: Keylogger Inalámbrico.

KeeLog en el pasado ya publicó un proyecto de keylogger por hardware PS/2 tipo Open Source. Ahora lo hacemos otra vez con el proyecto de Keylogger Inalámbrico, destinado para montar individualmente. Este proyecto se puede utilizar tanto con fines privados como comerciales con las siguientes limitaciones:

1. Todos los materiales incluidos en esta página web constituyen propiedad intelectual de la empresa KeeLog y su uso significa aceptación de las condiciones expuestas a continuación y del Contrato de Usuario General.
2. Este proyecto de Keylogger Inalámbrico ha sido publicado "así como es" con todos los defectos y sin ninguna garantía.

El Keylogger Inalámbrico no podrá ser utilizado para la captación no autorizada de datos, en particular contraseñas, datos bancarios, correspondencia confidencial, etc. En la mayoría de los países lo antedicho se considera un delito.

El Keylogger Inalámbrico esta compuesto de dos partes principales: emisor y receptor. El registro real de las teclas tiene lugar el en emisor el cual en realidad es un keylogger por hardware PS/2 con un módulo de radio 2.4 GHz incorporado. Los datos intercaptados del teclado no se archivan en la memoria sino se transmiten en tiempo real por la conexión por radio. El receptor, en el otro extremo, es un dispositivo inalámbrico de comisión con interfaz USB. Todos los datos recibidos del emisor se envían al ordenador por USB. Desde el punto de vista de programa estos datos son accesibles por el puerto virtual COM, lo que permite su visualización por cualquier cliente de la terminal.

Keylogger Inalámbrico - esquema de bloque

Todo el sistema funciona en tiempo real así que el texto escrito en ordenador remoto se ve inmediatamente en el lado del receptor. El sistema tiene un alcance máximo de aprox. 50 metros. Esto corresponde a un alcance eficaz de aprox. 20 metros por 2-4 paredes, en función de su grosor.

Keylogger Inalámbrico - emisor

Keylogger Inalámbrico - receptor

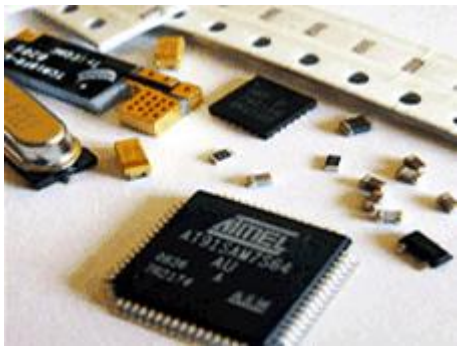
Tanto el emisor como el receptor están basados en el mismo esquema eléctrico y circuito impreso. Los dos tienen los mismos tamaños y están destinados a fijarlos en alargadores cortes PS/2 y USB. Se recomienda utilizar cajas de filtros tipo EMC, lo que provocará que el dispositivo entero parezca un adaptador o alargador.

Subconjuntos

Este artículo describe el proceso completo de montaje del Keylogger Inalámbrico. En función de los conocimientos puedes decidir y crear tu propio Keylogger Inalámbrico desde principio o pedir los subconjuntos a nosotros. Nosotros podemos suministrar el juego de subconjuntos con los microcontroladores programados y cajas estándares (presentadas en la foto) o un juego completo de dispositivos montado y probado. Pasa a la sección conjuntos para conseguir más detalles.

Si has decidido de crear tu propio Keylogger Inalámbrico debes tener una experiencia básica en electrónica y en soldadura, lo mejor en la tecnología de montaje superficial (SMT). La opción más fácil es pedir el juego completo de los subconjuntos a nosotros y hacer la soldadura, cables y montaje final individualmente. Para hacerlo es necesario tener una máquina para soldar con regulación de temperatura y bastante buenos conocimientos de soldadura. Si has decidido de diseñar y realizar los circuitos impresos por tu cuenta, esto requerirá mucha experiencia y unos equipos adecuados.

La tabla de abajo presenta la lista de subconjuntos (BOM), necesarios para hacer una unidad de emisor o receptor. El alargador adicional PS/2 se requiere para el emisor y un cable USB con conector tipo A se requiere para el receptor.



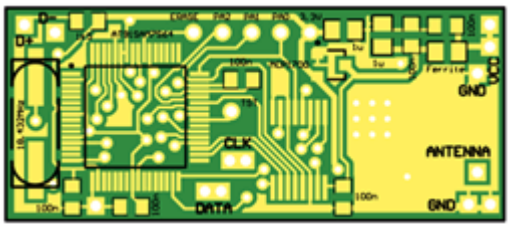
Juego de subconjuntos electrónicos

Cables, caja y circuitos impresos

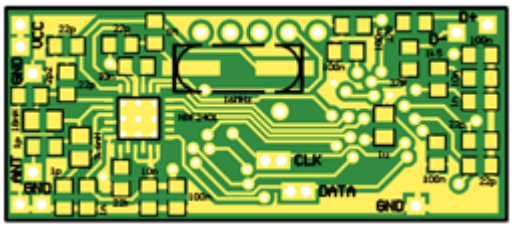
Marca	Descripción	Caja	Cantidad
U1	Microcontrolador AT91SAM7S64	TQFP64	1
U2	Transceiver nRF2401	QFN24	1
U3	Estabilizador MCP1700T-330	SOT-23	1
Q1	Cuarzo 18.432 MHz	HC-49 SMD	1
Q2	Cuarzo 16 MHz	HC-49 SMD	1
R1, R2	Resistor 1.5 kΩ	0805	2
R3, R4	Resistor 27 Ω	0805	2
R5	Resistor 1 MΩ	0805	1
R6	Resistor 22 kΩ	0805	1
C1, C27	Condensador 10 nF	0805	2
C2, C28	Condensador 1 nF	0805	2
C3, C4, C6, C7, C8	Condensador 22 pF	0805	5
C5	Condensador 33 nF	0805	1
C9	Condensador 2.2 pF	0805	1
C10, C11	Condensador 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Condensador 100 nF	0805	11
C21, C31, C41	Condensador 1 µF	0805	3
L1	Bobina de choque	0805	1
L2	Bobina 3.6 nH	0805	1
L3	Bobina 18 nH	0805	1

Keylogger Inalámbrico - lista de subconjuntos

Tanto el emisor como el receptor utilizan el mismo circuito impreso y el mismo juego de subconjuntos (se diferencian por cableado y firmware). El microcontrolador Atmel AT91SAM7S64 y el transceiver de radio nRF2401 son subconjuntos claves del circuito electrónico. Los dos requieren osciladores de cuarzo para su correcto funcionamiento. Aparte del estabilizador MCP1700, todos los demás subconjuntos son pasivos (resistores, condensadores y varias bobinas). Un trozo normal de alambre es recomendado como antena dipolar. El circuito impreso de doble cara y doble capa está presentado en los dibujos de abajo.

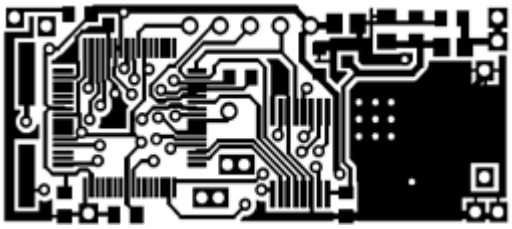


Distribución del circuito impreso - lado superior

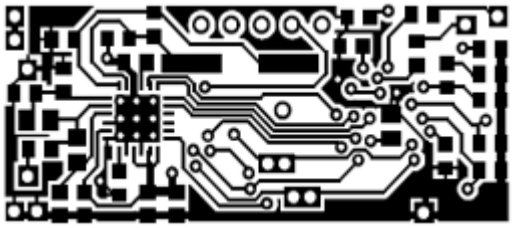


Distribución del circuito impreso - lado inferior

Si tienes conocimientos suficientes para hacer los circuitos impresos por tu cuenta puedes utilizar el juego de máscaras en la escala 1:1 presentadas abajo. El proyecto de referencia utiliza un laminado tipo FR4 de 1 mm de grosor.



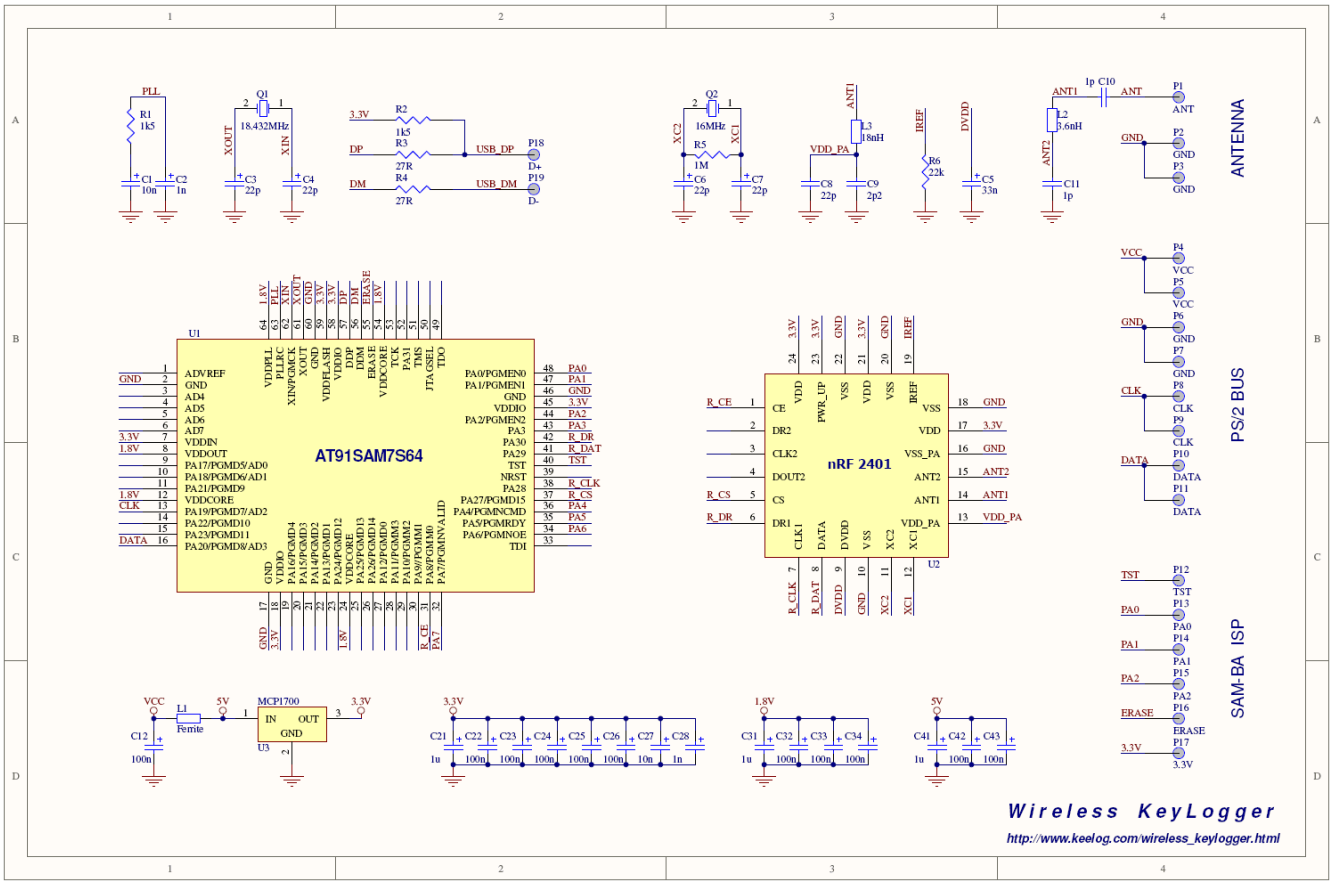
Máscara del circuito impreso - lado superior



Máscara del circuito impreso - lado inferior

Montaje

El circuito del Keylogger Inalámbrico está compuesto de dos componentes principales: microcontrolador AT91SAM7S64 y transceiver nRF2401. Los elementos pasivos que les acompañan son, principalmente, el oscilador y los circuitos de alta frecuencia RF. Todo el circuito está alimentado por 3.3V, generados por el estabilizador MCP1700 y filtrados por el juego de condensadores. La alimentación de entrada se coge directamente de la arteria de comunicación PS/2 (emisor), o USB (receptor). Si ya posees los circuitos impresos montados, pasa a la sección cableado. Si has decidido de montarlo individualmente te serán útiles las indicaciones y el esquema eléctrico presentados a continuación.



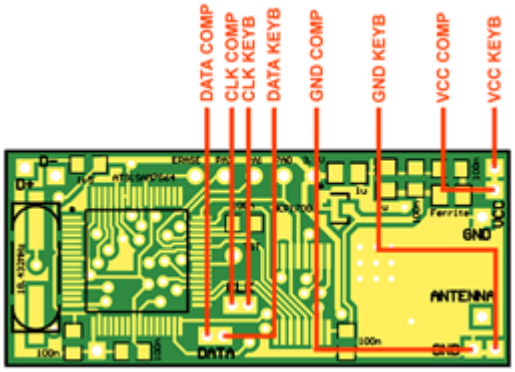
Keylogger Inalámbrico - esquema eléctrico

Para soldar utiliza una soldadura con pico fino (normalmente inferior a 0.5 mm) y una pasta de soldar (por ejemplo RMA7). Recuerda que los elementos no se calienten demasiado a la hora de soldarlos. Empieza por el montaje del transceiver nRF2401 por el motivo de la complejidad del tipo de la caja. A continuación pasa al microcontrolador AT91SAM7S64 y al estabilizador MCP1700. Recuerda que el pin número 1 en la caja coincida con el primer pin en el circuito impreso. Al final suelda todos los circuitos adicionales: cuarzos, resistores, condensadores y bobinas. Deja la antena al final. Puedes utilizar una antena dedicada para la banda ISM 2.4 GHz, o hacer una simple antena de una cuarta onda dipolar de un trozo de alambre. Una longitud óptima son 3.125 cm (1.23"). Los circuitos impresos montados deben parecerse a los presentados en las fotos.

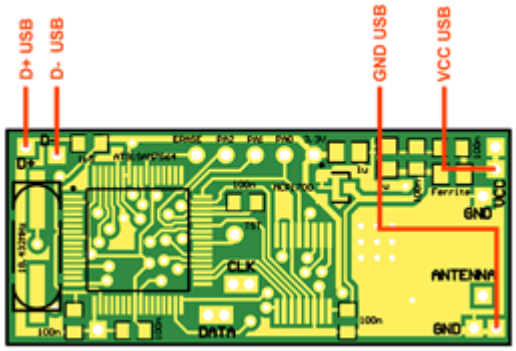
Circuito impreso montado - lado superior con microcontrolador

Circuito impreso montado - lado inferior con transceiver

Una vez montados los circuitos impresos es necesario hacer el cableado. Aparte del firmware es un punto en el que el emisor se diferencia del receptor. El emisor debe estar acoplado paralelamente con la central de distribución PS/2. El circuito impreso del emisor tienes pads que permiten soldar los cables que llegan tanto al ordenador como al teclado. El receptor debe de tener una conexión estándar al puerto USB. Las fotos de abajo enseñan cómo realizar todas las conexiones.



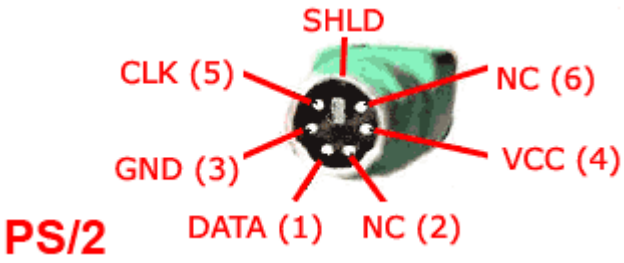
Esquema de cableado PS/2 para el emisor



Esquema de cableado PS/2 para el receptor

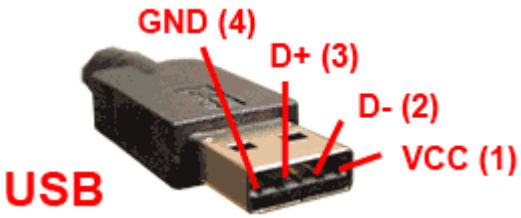
Utiliza los alargadores PS/2 y USB, córtalos y aísla las líneas de señales. Una cosa que puede provocar problemas es adjudicar los cables a las señales concretas. Algunos de los cables PS/2 y USB tienen colores estandarizados pero confiar en ellos es muy peligroso. La solución que se recomienda es utilizar una unidad de medida de cortocircuitos u ohmímetro para saber cuál cable corresponde a qué línea de señales. Los esquemas presentados abajo deben ser útiles.

Señal	Descripción	Pin PS/2	Comentarios
VCC	Alimentación de +5V	4	tienen que estar conectados al módulo
GND	Masa de alimentación	3	
CLK	Reloj	5	
DATA	Datos	1	
NC	Líneas no utilizadas	2, 6	no utilizadas por el módulo, si existen dejar en el estado original
SHLD	Apantallado	-	



Empalme PS/2 (emisor)

Señal	Descripción	Pin USB	Comentarios
VCC	Alimentación de +5V	1	tienen que estar conectados al módulo
D-	Datos	2	
D+	Datos	3	
GND	Masa de alimentación	4	
SHLD	Apantallado	-	no utilizadas por el módulo, si existen dejar en el estado original



Empalme USB (receptor)

Si los microcontroladores que estás utilizando aún no han sido programados ahora es un buen momento para cargar el firmware utilizando la tecnología ISP (In-System Programming). Lee la sección firmware para conseguir más detalles. Una vez hecho este paso, los dispositivos montados deben tener el aspecto presentado en las fotos.

Emisor con cableado PS/2

Receptor con cableado USB

Antes de montar la caja recomendamos realizarla última prueba. Utiliza la unidad de medida de cortocircuitos u ohmímetro para medir la resistencia entre la alimentación (VCC) y la masa (GND) tanto en el empalme USB, como en PS/2. Cortocircuito significa que hay que comprobar todo el circuito, en otro caso el ordenador se podrá dañar. Si todo está bien, cierra las cajas utilizando cola y ha llegado el tiempo para la primera conexión.

Puesta en marcha

Una vez montado el circuito emisor-receptor es necesario hacer la primera prueba. Es recomendable utilizar un sólo ordenador para probar los dos. Al principio apaga el ordenador y conecta el emisor entre el teclado PS/2 y el puerto PS/2.

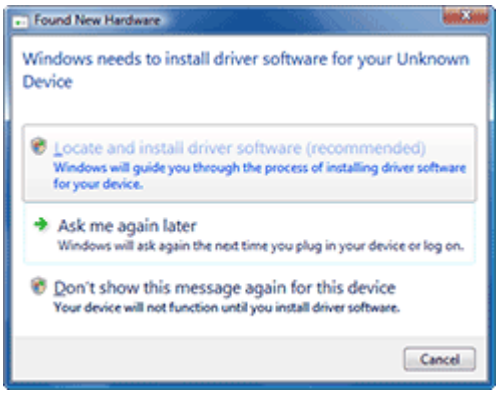
Conecta el emisor al puerto PS/2

Conecta el teclado PS/2 al emisor

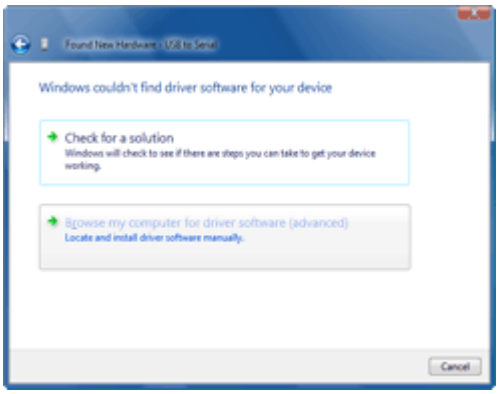
Después enciende el ordenador y asegúrate de que el teclado PS/2 funciona (no se debe de notar ninguna influencia del keylogger). A continuación probamos el receptor. Antes es necesario descargar el archivo del driver KeeLog. Descomprímelo y guárdalo en el disco local del ordenador. A continuación, conecta el receptor al puerto USB libre (no se requiere encender el ordenador antes). Asegúrate de que la posición del receptor permite recibir la transmisión de radio del emisor.

Conecta el receptor al puerto USB libre

Cuando el emisor está conectado por primera vez aparecerá una ventana de instalación del driver. Es decir, se utilizarán los drivers del puerto virtual COM suministrados con la mayoría de los sistemas operativos como Windows. Pero el archivo adecuado de la descripción INF tiene que seleccionarse manualmente. Cuando el sistema pregunte por los drivers pasa a la pista donde están guardados archivos de los drivers. Los dibujos de abajo presentan el proceso entero.

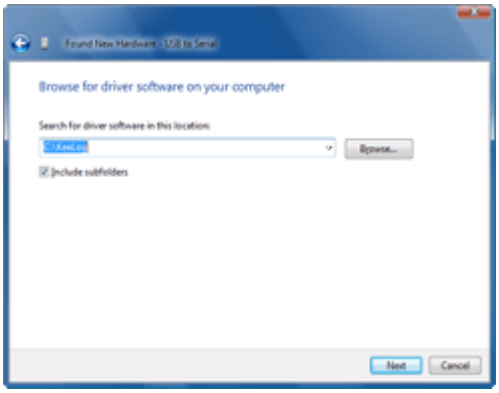


Selecciona la localización y la instalación del software



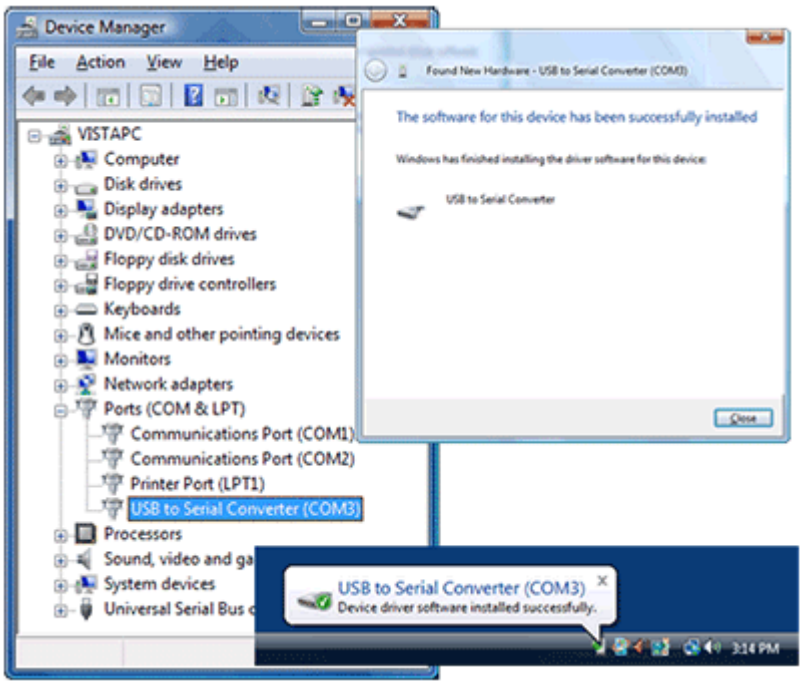
Selecciona la localización del driver

Selecciona para presentar la opción de la localización



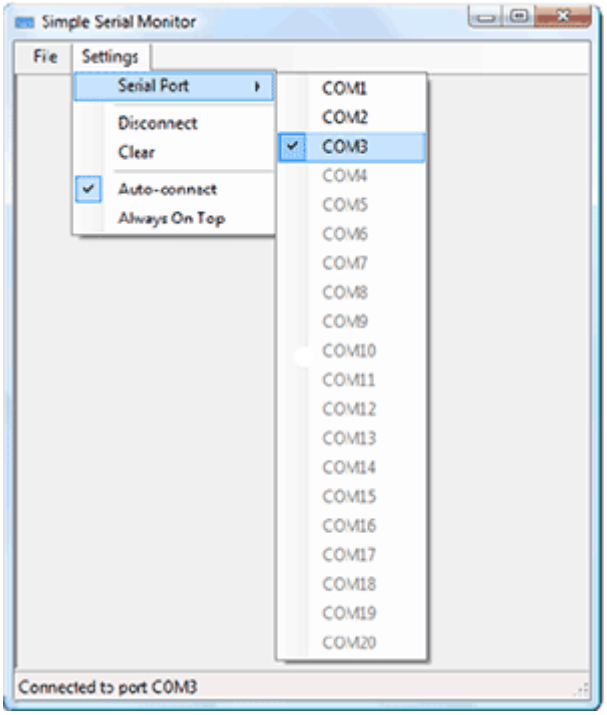
Indica la situación de los archivos del driver

Cuando el proceso de instalación termina con éxito el receptor debe estar visible como convertidor de USB al puerto en serie. Abre Administrar Dispositivos en el sistema Windows para verificar cuál puerto en serie ha sido adjudicado al receptor.



Receptor visible en Administrar Dispositivos

Para empezar a recibir los datos del teclado del emisor se puede utilizar cualquier cliente de la terminal, como, por ejemplo, Hyperterminal. Recomendamos utilizar nuestra aplicación gratuita Simple Serial Monitor por su comodidad y facilidad de uso.



Simple Serial Monitor (cliente gratuito de la terminal suministrado por KeeLog)

Una vez arrancado Simple Serial Monitor (o una aplicación alternativa) recuerda seleccionar el puerto adecuado COM. Si todo ha ido bien, el receptor empezará de inmediata presentar el haz de teclas presionadas en el teclado PS/2.

Ordenador remoto con emisor PS/2 *Ordenador local con receptor USB*

El siguiente paso será probar lo mismo en dos ordenadores diferentes. Asegúrate de que están en el alcance de la transmisión. Si el texto aparece en la ventana de la terminal tu Keylogger Inalámbrico está listo para su primera misión real. Recuerda utilizar este dispositivo conforme con la ley!

Descarga

Firmware para el microcontrolador que permite programar el emisor y el receptor
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

El driver que permite instalación del receptor como puerto virtual COM
http://www.keelog.com/files/UsbToSerial.zip

Programas gratuitos que permiten recepción de los datos intercaptados por el puerto virtual COM (equivalente de la aplicación Hyperterminal). Requiere plataforma Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Programas que permiten programar firmware utilizando SAM-BA
http://www.keelog.com/files/At91Isp.zip

Guía cómo programar firmware para el microcontrolador por bootloader incorporado sin utilizar programador adicional
http://www.keelog.com/files/SambaUserGuide.pdf

Listado de subconjuntos utilizados para el montaje de Keylogger Inalámbrico (emisor y receptor)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Esquema de cableado para el Keylogger Inalámbrico (emisor y receptor)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Esquema eléctrico del Keylogger Inalámbrico (emisor y receptor)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Lado superior del circuito impreso (emisor y receptor)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Lado inferior del circuito impreso (emisor y receptor)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Máscara para el lado superior del circuito impreso (emisor y receptor), escala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Máscara para el lado inferior del circuito impreso (emisor y receptor), escala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

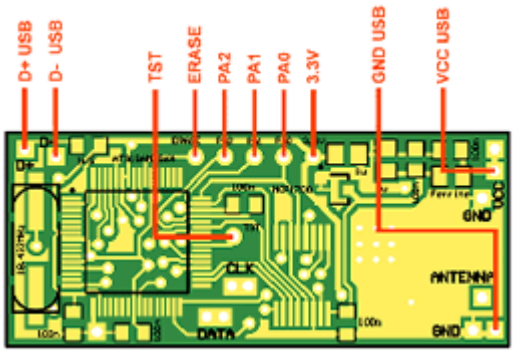
Firmware

Lee este capítulo sólo si necesitas programar el microcontrolador AT91SAM7S64 por tu cuenta. Si nos has comprado el juego a nosotros, ya hemos hecho este paso por ti.

Los microcontroladores contemporáneos, como Atmel AT91SAM7S64 tienen cajas muy ocupadas lo que provoca problemas a la hora de buscar un programador tradicional que trabaja con el tipo concreto de microcontrolador. Por este motivo la programación en el sistema ISP (In-System Programming) en los últimos años se está desarrollando muy rápidamente. ISP permite primero el montaje del circuito entero y a continuación programación del firmware, muchas veces utilizando herramientas simples. El microcontrolador AT91SAM7S64 tiene una solución muy cómoda ISP, en base al módulo USB incorporado. Se llama SAM-BA (SAM Boot Assistant), y sólo requiere un cable USB y varias armaduras simples. Para poner en marcha SAM-BA en el Keylogger Inalámbrico, descarga primero el programa AT91 ISP. A continuación pasas los siguientes pasos para cargar firmware al módulo del emisor y del receptor.

Paso 1: Referente sólo al emisor. Prepara el cable USB con la conexión tipo A en un lado y con cables desaislados en el otro lado. Suelda las líneas USB: VCC, GND, D+, y D- a los puntos correspondientes en el circuito impreso. Este paso es imprescindible para el receptor porque éste ya tiene preparada la conexión USB.

Paso 2: Prepara varios alambres para cerrar los pines SAM-BA: TST, ERASE, PA2, PA1, PA0, 3.3V. Suelda un extremo de cada hilo al punto de soldadura correspondiente SAM-BA en las dos placas. Alternativamente puedes preparar armaduras especiales como presentado en los dibujos de abajo.



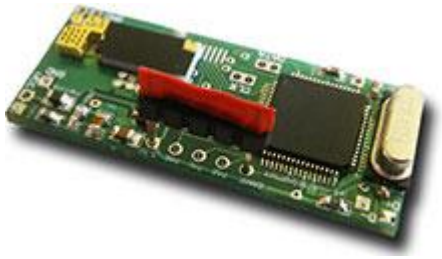
Esquema de cableado SAM-BA

Paso 3: Instala el paquete de programas AT91 ISP.

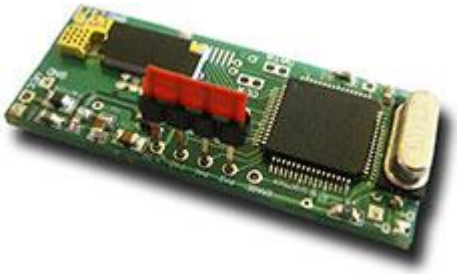
Paso 4: Conecta el dispositivo al puerto USB libre. El comunicado Dispositivo desconocido en esta etapa es normal.

Paso 5: Conecta ERASE a 3.3V para un corto momento. Esto provocara que se borre la memoria flash del microcontrolador.

El cable USB y las armaduras para bootloader SAM-BA



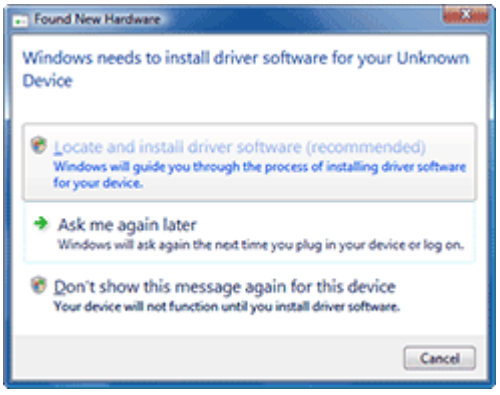
Limpieza de memoria (ERASE conectado a 3.3V)



Activación del bootloader (PA0, PA1, PA2 y TST conectados a 3.3V)

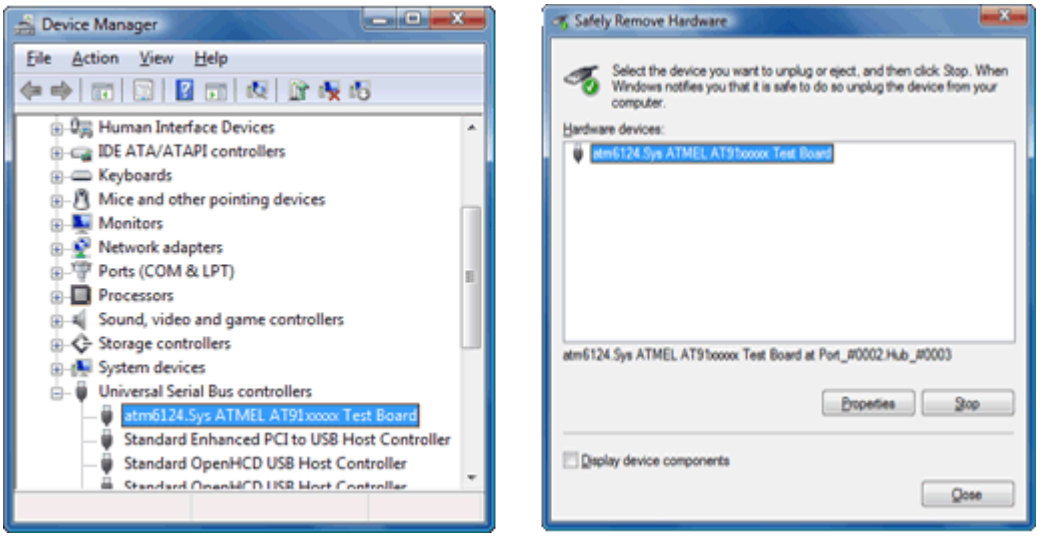
Paso 6: Desconecta el dispositivo del puerto USB. Asegúrate de que la conexión ERASE ya no está conectada a 3.3V. A continuación, conecta el conjunto de conectores PA0, PA1, PA2 y TST a 3.3V. Conecta otra vez el dispositivo al puerto USB (Dispositivo desconocido puede aparecer otra vez). Deja el dispositivo conectado durante unos 10 segundos, a continuación desconéctalo del puerto USB. Esta operación debe activar el bootloader interno SAM-BA.

Paso 7: Quita todas las armaduras o conectores y conecta el dispositivo al puerto USB. Debe aparecer el comunicado Nuevo dispositivo encontrado. Haz el procedimiento de instalación estándar y deja al sistema buscar los drivers sólo.



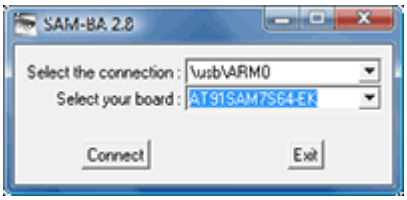
Diálogo Nuevo dispositivo encontrado

Paso 8: Abre Administrar Dispositivos para asegurarse de que el bootloader SAM-BA está activo.



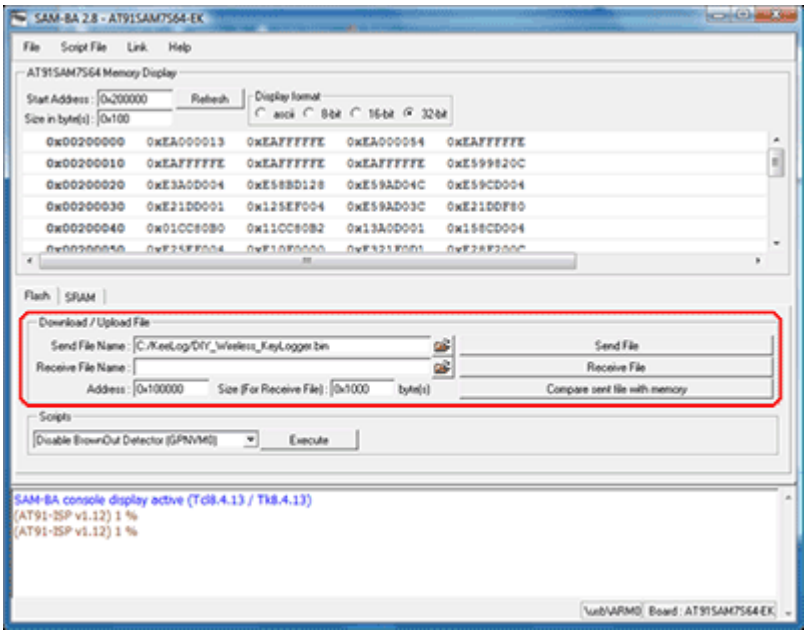
Administrar Dispositivos con el equipo Atmel AT91

Paso 9: Arranca la aplicación SAM-BA del paquete de programas AT91 ISP y selecciona la plataforma de dispositivos de destino AT91SAM7S64-EK.



Selección de la plataforma de dispositivos

Paso 10: Una vez conectado a la plataforma de dispositivos, pasa a la pestaña Flash, selecciona el correspondiente firmware para el emisor/ receptor, a continuación pincha Send File. Cuando la aplicación pregunte si desbloquear y bloquear los campos correspondientes de la memoria flash, es necesario seleccionar Yes. Si este paso ha terminado con éxito éso significa que el firmware ha sido cargado correctamente a la memoria flash del microcontrolador.



Aplicación SAM-BA

Recuerda repetir el procedimiento SAM-BA tanto para el emisor como para el receptor. Una vez terminado el procedimiento los dos dispositivos están listos para trabajar.