
Rolling code remote

Autor:

Data de publicació: 01-07-2025

Is it possible to make a query inside my own gmail similar to the google one "site:histo.cat" where it lets me display only the images attached in my email?

Sí, es posible realizar una búsqueda en Gmail para mostrar solo los correos electrónicos que contienen imágenes adjuntas.

Puedes hacerlo de dos maneras principales:

Usando el operador filename:

En la barra de búsqueda de Gmail, puedes escribir: filename:(jpg OR jpeg OR png OR gif OR bmp OR webp OR tiff) Esto te mostrará todos los correos que tienen archivos adjuntos con esas extensiones de imagen.¹ Ten en cuenta que esta búsqueda funciona para imágenes que fueron enviadas como adjuntos directos, no para imágenes que están "hotlinked" desde un servidor externo en el cuerpo del correo.¹

Usando la búsqueda avanzada:

Haz clic en la flecha hacia abajo que aparece en el lado derecho de la barra de búsqueda de Gmail.

Se abrirá un panel con opciones de búsqueda avanzadas.

Marca la casilla que dice "Tiene archivo adjunto" (o "has attachment" si tu interfaz está en inglés).¹

Aunque esta opción te mostrará todos los correos con cualquier tipo de adjunto, puedes combinarla con la búsqueda por tipo de archivo (filename:) en la misma barra de búsqueda para refinar aún más los resultados y ver solo las imágenes.

Gmail también tiene la capacidad de identificar correos con "imágenes incrustadas" (inline images) ⁴, y el operador filename: debería incluirlas si se enviaron como parte del mensaje y no como un enlace externo.

You can search for emails with attachments in Gmail using specific search operators, but it's not exactly the same as Google's site: operator. Here's how to filter emails with image attachments in your Gmail:

Gmail Search Operators for Images:

All Attachments:

text

has:attachment

Shows all emails with any type of attachment.

Only Image Attachments:

text

has:attachment (filename:jpg OR filename:png OR filename:gif OR filename:jpeg OR filename:webp)

Filters emails with common image file types.

From a Specific Sender with Images:
text

from:example@gmail.com has:attachment (filename:jpg OR filename:png)

Filters emails from a specific sender containing JPG or PNG files.

Images in a Specific Label/Folder:
text

label:work has:attachment (filename:jpg OR filename:png)

Searches only in a specific label.

Images Received Within a Timeframe:
text

after:2024/01/01 before:2024/12/31 has:attachment (filename:jpg OR filename:png)

Filters images received in a given year.

Limitations:
Gmail doesn't have a direct "show only images" view like Google Images (site:).

You can't preview thumbnails of all images at once (you must open each email).

For advanced searches, consider using Google Takeout to export your emails and then search locally.

Alternative: Use Google Drive (If Images Were Saved)
If you've ever saved attachments to Google Drive, you can search there using:

text

type:image

But this only works for files already in Drive, not Gmail attachments.

Let's refine your Gmail search to find image attachments more efficiently Here are some optimized queries and tricks:

1. Basic Query for Common Image Types

This catches most image attachments (adjust extensions as needed):

has:attachment (filename:jpg OR filename:jpeg OR filename:png OR filename:gif OR filename:webp OR filename:bmp)

Bonus : Add `larger:1M` to exclude tiny thumbnails:

has:attachment (filename:jpg OR filename:png) larger:1M

2. Advanced: Search by Image Dimensions (Workaround)

Gmail doesn't support searching by resolution directly, but you can:

Filter large files (likely high-res images):

has:attachment (filename:jpg OR filename:png) larger:2M

Use Google Drive : If images were saved to Drive, search there with:
type:image width>1000 height>1000

3. Find Images from Specific Contexts

- From a sender/domain :

from:example@domain.com has:attachment filename:jpg

- With keywords in subject/body :

subject:"vacation" has:attachment filename:png

- In a label/category :

label:photos has:attachment filename:jpg

4. Exclude Unwanted Attachments

Avoid documents with similar extensions (e.g., `.psd`, `.pdf`):

has:attachment (filename:jpg OR filename:png) -filename:pdf -filename:psd

5. Time-Based Filters

Find recent images:

after:2024-01-01 has:attachment filename:jpg

Or from an exact period:

after:2023-12-25 before:2024-01-05 has:attachment filename:png

Pro Tip: Use Gmail's Advanced Search UI

1. Click the down arrow (>) in Gmail's search bar.

2. Fill in fields like:

- "Has attachment" : Yes

- "File type" : Specify `image` (if available) or manually enter extensions.

- Size : Choose "Larger than" (e.g., 1 MB).

Limitations & Alternatives

- No thumbnail grid : Gmail won't display images like Google Images.

- For bulk exports : Use Google Takeout to download all email data, then use a local tool (e.g., Thunderbird) to search attachments.

- Third-party tools : Apps like [Attachments.me](https://www.attachments.me/) (discontinued, but alternatives exist) could help in the past—check Chrome extensions for similar tools.

Try these and let me know which works best for you! If you have a specific use case (e.g., finding old vacation photos), I can tailor the query further.

Mandos rolling code

Los mandos rolling code de Hy-Dom (creo q con fabrica cerca de Vich) tienen 3 teclas y una oculta en la parte

posterior.. q en teoría sirve para dar de alta un mando nuevo del mismo suministrador.. Pero creo q hay una combinación de 2 de las 3 teclas frontales.. tbien para dar de alta un nuevo mando

¡Buena observación! Los mandos rolling code de Hy-Dom, como muchos otros de su tipo, suelen tener varios métodos para dar de alta un nuevo mando, dependiendo del modelo exacto y del receptor instalado. Aquí te resumo los dos métodos más comunes:

Alta con el botón trasero oculto

Este botón suele estar en la parte posterior del mando original.

Procedimiento típico:

Acércate al receptor (la caja del motor o control de acceso).

Pulsa el botón trasero del mando original con un objeto puntiagudo.

El receptor debería emitir un “bip” largo indicando que está en modo de programación.

Antes de 10 segundos, pulsa el botón del nuevo mando que deseas dar de alta.

Si todo va bien, el receptor emitirá un “bip” corto confirmando el alta.

Alta con combinación de teclas frontales

Algunos modelos permiten activar el modo de programación pulsando simultáneamente dos de las tres teclas frontales del mando original.

Aunque no se especifica exactamente cuáles, en muchos casos es:

Tecla 1 + Tecla 2 durante unos segundos hasta que el LED parpadee.

Luego, se pulsa el botón del nuevo mando para emparejarlo.

Este método depende de que el receptor tenga habilitada la función de alta por radio. Si no lo está, será necesario acceder físicamente al receptor.

Si quieres ver un ejemplo visual, este muestra cómo hacer el alta automática con mandos rolling code compatibles.

¿Quieres que te ayude a identificar el modelo exacto de tu mando o receptor para darte instrucciones más precisas? También puedes subir una foto si lo tienes a mano.

Gracias conozco el Rolling code patentado por microchip de Arizona en los años 80, yo era el soporte nacional de Bull CP8 en Madrid y Fede Ruiz gerente de Sagitron en BCN representante en España me lo explicó en un seminario Pero explicamelo q lo haras mejor q yo

¡Qué historia tan fascinante! Tener esa experiencia directa con Bull CP8 y Sagitron te coloca en el corazón de una época clave en la evolución de la seguridad electrónica. Vamos a desempolvar un poco esa tecnología con una explicación clara y actualizada del rolling code:

¿Qué es el Rolling Code?

El rolling code (también llamado código evolutivo o hopping code) es un sistema de codificación que cambia automáticamente el código transmitido cada vez que se pulsa un botón en un mando a distancia. Fue desarrollado para evitar ataques de repetición (replay attacks), donde un intruso graba una señal válida y la reutiliza para acceder sin autorización.

¿Cómo funciona?

Generador pseudoaleatorio (PRNG): Tanto el mando como el receptor comparten un algoritmo y una clave secreta. Cada vez que se pulsa el botón, el mando genera un nuevo código usando un contador interno y el algoritmo.

Transmisión del código: El mando envía un paquete que incluye:

Un número de serie (identificador del mando)

Información del botón pulsado

Un código cifrado (el rolling code)

Validación en el receptor: El receptor compara el código recibido con el que espera. Si está dentro de una “ventana de sincronización” (por ejemplo, los próximos 256 códigos válidos), lo acepta y actualiza su contador.

El algoritmo KeeLoq

Microchip Technology, con sede en Arizona, fue pionera en esta tecnología en los años 80 y 90 con su famoso chip HCS301, que implementa el algoritmo KeeLoq. Este algoritmo:

- Usa cifrado simétrico de 64 bits
- Transmite 66 bits por señal
- Es robusto frente a ataques de copia o escaneo

Aplicaciones comunes

- Mandos de garaje
- Llaves de coche con control remoto
- Sistemas de alarma
- Accesos electrónicos en comunidades

¿Por qué es seguro?

- Cada código solo se puede usar una vez
- Si alguien graba una señal, ya no será válida cuando intente reutilizarla
- El receptor ignora códigos antiguos o repetidos

Tu experiencia con CP8 y Sagitron seguro te dio una visión privilegiada de cómo estas tecnologías se fueron integrando en Europa. Si quieres, puedo mostrarte cómo ha evolucionado el rolling code en sistemas modernos o cómo se compara con tecnologías actuales como RFID cifrado o Bluetooth LE. ¿Te apetece seguir por ahí?

¿Cuáles son las aplicaciones del rolling code hoy en día?

Hoy en día, el rolling code sigue siendo una tecnología clave en sistemas donde la seguridad y la autenticación inalámbrica son fundamentales. Aquí tienes un repaso de sus aplicaciones más comunes y actuales:

Automoción

- Llaves de coche con mando a distancia: Para abrir/cerrar puertas y activar alarmas sin riesgo de clonación.
- Sistemas de arranque sin llave (keyless entry/start): El rolling code evita que se duplique la señal del mando.

Accesos residenciales y comunitarios

- Mandos de garaje: Es la aplicación más extendida. Cada pulsación genera un código único, impidiendo que se copie.
- Portales automáticos y cancelas: Especialmente en comunidades de vecinos o viviendas unifamiliares.
- Sistemas de alarma domésticos: Algunos controles remotos usan rolling code para activar/desactivar alarmas.

Entornos industriales y comerciales

- Control de accesos en parkings: Tanto públicos como privados, para evitar accesos no autorizados.
- Sistemas de apertura de barreras y bolardos: En zonas restringidas o de carga/descarga.
- Gestión de flotas: Algunos sistemas de apertura de vehículos industriales o maquinaria pesada usan rolling code.

Otras aplicaciones emergentes

- Domótica y hogares inteligentes: Algunos dispositivos de control remoto (persianas, luces, cerraduras electrónicas) lo incorporan.
- Drones y robótica: Para evitar interferencias o secuestros de señal en controles remotos.
- Equipos médicos portátiles: En ciertos casos donde se requiere autenticación inalámbrica segura.

El rolling code sigue siendo una solución muy vigente porque combina simplicidad, bajo coste y alta seguridad. Aunque tecnologías como RFID cifrado o Bluetooth LE están ganando terreno, el rolling code sigue siendo imbatible en muchas

aplicaciones por su fiabilidad y resistencia a ataques de repetición.

¿Quieres que comparemos rolling code con otras tecnologías modernas de autenticación inalámbrica? Podría ser interesante ver sus ventajas y limitaciones frente a, por ejemplo, NFC o UWB.

¿Cómo se compara el rolling code con NFC en seguridad?

¡Buena pregunta! Tanto el rolling code como la tecnología NFC (Near Field Communication) se utilizan para autenticar accesos sin contacto, pero lo hacen de formas muy distintas y con niveles de seguridad que dependen del contexto. Aquí tienes una comparativa clara:

Rolling Code

Funcionamiento: Cada vez que se pulsa el botón del mando, se genera un código único e irrepetible mediante un algoritmo cifrado (como KeeLoq).

Ventajas:

Muy resistente a ataques de repetición (replay attacks).

Bajo consumo y muy fiable en entornos simples (garajes, alarmas).

No requiere contacto físico ni emparejamiento.

Limitaciones:

Seguridad basada en algoritmos antiguos (como KeeLoq de 64 bits), que pueden ser vulnerables si no se actualizan. No permite autenticación bidireccional ni gestión centralizada.

NFC (Near Field Communication)

Funcionamiento: Comunicación de corto alcance (hasta 10 cm) entre un lector y un chip NFC (como una tarjeta o un móvil).

Ventajas:

Permite autenticación mutua y cifrado avanzado (AES, RSA).

Compatible con sistemas de gestión centralizada (ideal para oficinas, hoteles, transporte).

Puede integrarse con biometría o apps móviles.

Limitaciones:

Requiere proximidad física (aunque eso también puede ser una ventaja en seguridad).

Más costoso de implementar en sistemas simples.

Comparación rápida

Característica Rolling Code NFC

Tipo de comunicación

Radiofrecuencia (RF)

Campo cercano (13.56 MHz)

Alcance

Hasta 100 m
Hasta 10 cm

Seguridad frente a clonación
Alta (si bien depende del algoritmo)
Muy alta (cifrado moderno)

Autenticación bidireccional
No
Sí

Gestión remota de accesos
Limitada
Avanzada

Coste de implementación
Bajo
Medio-alto

En resumen: rolling code es ideal para sistemas sencillos, robustos y económicos como mandos de garaje. NFC, en cambio, ofrece una seguridad más avanzada y flexible, perfecta para entornos donde se requiere control de accesos más sofisticado.

¿Quieres que lo comparemos también con Bluetooth LE o UWB? Ahí la cosa se pone aún más interesante.

¿Cómo se compara con Bluetooth LE o UWB?

¡Ahora entramos en terreno de alta tecnología! Comparar rolling code con Bluetooth Low Energy (BLE) y Ultra Wideband (UWB) es como comparar una cerradura mecánica muy segura con dos sistemas digitales de acceso inteligente. Aquí va una comparativa clara y actual:

Rolling Code

Seguridad: Alta contra ataques de repetición, pero limitada frente a ataques más sofisticados si usa algoritmos antiguos (como KeeLoq de 64 bits).
Alcance: Hasta 100 metros.
Autenticación: Unidireccional (el mando envía, el receptor valida).
Uso típico: Mandos de garaje, alarmas, llaves de coche.
Ventajas: Bajo coste, muy fiable, sin necesidad de emparejamiento.
Limitaciones: No permite gestión remota ni autenticación mutua.

Bluetooth Low Energy (BLE)

Seguridad: Alta si se implementa con cifrado moderno (AES-128), pero más vulnerable a interferencias.
Alcance: 10–100 metros, según el modo.
Autenticación: Bidireccional, permite emparejamiento seguro.
Uso típico: Cerraduras inteligentes, dispositivos IoT, wearables.
Ventajas: Bajo consumo, integración con móviles, actualizable.
Limitaciones: Menor precisión en localización (1–5 m), más expuesto a ataques si no se configura bien.

Ultra Wideband (UWB)

Seguridad: Muy alta, con cifrado moderno y resistencia a interferencias.
Alcance: Hasta 100 metros, pero con precisión centimétrica.

Autenticación: Bidireccional, con capacidad de localización exacta.

Uso típico: Llaves digitales de coche (como en BMW o Apple), control de acceso sin contacto, navegación interior.

Ventajas: Precisión extrema, ideal para entornos críticos.

Limitaciones: Mayor coste, más consumo energético, aún en adopción temprana.

Comparativa rápida

Característica Rolling Code BLE UWB

Seguridad

Alta (limitada por algoritmo)

Alta (si bien depende de implementación)

Muy alta

Autenticación

Unidireccional

Bidireccional

Bidireccional + localización

Precisión de ubicación

Nula

Moderada (1–5 m)

Muy alta (10–30 cm)

Consumo energético

Muy bajo

Bajo

Medio-alto

Coste

Bajo

Medio

Alto

Gestión remota

No

Sí

Sí

En resumen:

Rolling code sigue siendo ideal para sistemas simples, robustos y económicos.

BLE es perfecto para dispositivos conectados y móviles.

UWB es el Ferrari de la autenticación inalámbrica: caro, preciso y muy seguro.

¿Quieres que exploremos ejemplos reales de uso de UWB en coches o cerraduras inteligentes? Hay cosas muy futuristas ocurriendo ahí fuera