Criptografía Práctica para Comunicaciones: Cifrado Simple y Claves Precompartidas

Autor: EA4IPV
Fecha: 23/03/2026
Categoría: Electrónica y Energía
Etiquetas: Sin etiquetas

Criptografía Práctica para Comunicaciones: Cifrado Simple y Claves Precompartidas

Cuando las redes de telefonía móvil colapsan o se interrumpen —algo habitual en desastres naturales como los vividos en la DANA de Valencia de 2024— las comunicaciones por radio, mensajería offline o incluso notas escritas pueden necesitar un nivel básico de confidencialidad. No se trata de ocultar actividades ilícitas, sino de proteger información sensible como ubicaciones de suministros, rutas de evacuación familiares o datos médicos frente a actores oportunistas. La criptografía práctica para preppers no requiere ordenadores ni conocimientos matemáticos avanzados: se basa en técnicas manuales probadas durante siglos, adaptadas al contexto moderno y complementadas con herramientas digitales sencillas cuando hay electricidad disponible. En España, el uso de cifrado en comunicaciones privadas es legal según el artículo 18.3 de la Constitución, que garantiza el secreto de las comunicaciones.

Fundamentos del cifrado con clave precompartida (PSK)

El cifrado con clave precompartida (Pre-Shared Key) es el sistema más práctico para grupos familiares o comunidades pequeñas. Todos los miembros del grupo acuerdan previamente una clave secreta que usarán para cifrar y descifrar mensajes. No requiere infraestructura de certificados ni conexión a Internet.

Principio de funcionamiento: Emisor y receptor comparten la misma clave antes de que ocurra la emergencia. El emisor transforma el mensaje original (texto claro) en texto ilegible (texto cifrado) usando la clave. El receptor aplica la misma clave en sentido inverso para recuperar el mensaje original. Sin la clave, el texto cifrado es ininteligible.

Distribución segura de claves: Las claves deben distribuirse en persona, nunca por teléfono, radio ni Internet. Reúne a tu grupo familiar y entrega a cada miembro una copia física de la tabla de claves. Establece un calendario de rotación (por ejemplo, clave A para enero-marzo, clave B para abril-junio). Cada miembro guarda su copia en la mochila de emergencia dentro de una funda impermeable.

Rotación y compromiso de claves: Si sospechas que una clave ha sido comprometida (alguien ajeno al grupo la ha visto), toda comunicación con esa clave debe considerarse insegura. Establece una señal convenida (una palabra clave en una transmisión de radio, por ejemplo) que indique al grupo que deben pasar a la siguiente clave de la tabla sin mencionarla explícitamente.

Cifrado Vigenère: método manual sin tecnología

El cifrado Vigenère es un sistema polialfabético del siglo XVI que, aunque no es irrompible por criptoanálisis profesional, ofrece un nivel de protección suficiente para comunicaciones tácticas de corto

plazo en emergencias. Su gran ventaja es que solo necesitas lápiz, papel y una tabla.

Paso
Acción
Ejemplo

1
Elegir una clave secreta
Clave: FUEGO

2
Escribir el mensaje en mayúsculas sin espacios ni signos
REUNIONENELPUENTE

3
Repetir la clave debajo del mensaje hasta cubrir todas las letras
FUEGOFUEGOFUEGOF

4
Para cada letra, sumar las posiciones (A=0, B=1... Z=25) y aplicar módulo 26
R+F=W, E+U=Y, U+E=Y, N+G=T, I+O=W...

5
Resultado cifrado
WYYTWSSJKRZYKTJK

Para descifrar, el receptor realiza la operación inversa: resta la posición de la letra de la clave a la letra cifrada. Si el resultado es negativo, suma 26. Con práctica, una persona puede cifrar o descifrar un mensaje de 50 caracteres en menos de 10 minutos.

Consejo: Imprime varias copias de la tabla Vigenère (también llamada Tabula Recta) en papel plastificado e inclúyela en tu kit de emergencia. Puedes encontrar la tabla en cualquier manual de criptografía básica o generarla tú mismo con un procesador de textos.

Códigos de libro: cifrado irrompible con recursos mínimos

El cifrado de libro (Book Cipher) es uno de los sistemas más seguros que existen si se usa correctamente, y solo requiere que emisor y receptor posean el mismo ejemplar de un libro concreto.

Selección del libro: Elige un libro común que no levante sospechas: un diccionario, una novela popular, una guía de campo. Todos los miembros del grupo deben tener la misma edición exacta (editorial, año, ISBN). Diferencias entre ediciones cambiarían la paginación y harían imposible el descifrado.

Método de cifrado: Cada palabra del mensaje se sustituye por una referencia al libro con el formato página-línea-palabra. Por ejemplo, «45-7-3» significa página 45, línea 7, tercera palabra. Para mayor seguridad, usa

una palabra diferente del libro para cada aparición de la misma palabra en el mensaje (nunca repitas la misma referencia).

Ventajas en emergencias: No requiere electricidad ni dispositivos. El «equipo» de cifrado es un libro de bolsillo que pesa 200 gramos. Si el libro es común (un diccionario RAE de bolsillo, por ejemplo), poseerlo no levanta sospechas. Sin conocer qué libro se usa, el cifrado es prácticamente irrompible.

Cifrado digital sencillo cuando hay electricidad disponible

Si dispones de un ordenador o móvil con batería, puedes usar herramientas de cifrado digital que son mucho más robustas que los métodos manuales.

Herramienta
Tipo
Uso en emergencias
Requisitos

Signal
Mensajería cifrada E2E
Mensajes y llamadas cifradas si hay datos móviles o WiFi
Smartphone + conexión de datos

Briar
Mensajería P2P sin Internet
Mensajes cifrados vía Bluetooth, WiFi Direct o Tor
Android + otro dispositivo cercano

GPG4USB / Kleopatra
Cifrado asimétrico de archivos
Cifrar documentos antes de compartirlos por cualquier medio
PC con Windows o Linux, sin conexión

AES Crypt
Cifrado simétrico de archivos
Cifrar un archivo con contraseña compartida
PC o móvil, software portable, sin conexión

VeraCrypt
Volumen cifrado
Crear contenedor cifrado en USB con documentos críticos
PC con Windows o Linux para crear; acceso desde cualquier PC

Sobre comunicaciones por radio: En España, el artículo 197 del Código Penal tipifica la interceptación de comunicaciones. Sin embargo, las comunicaciones por radio en frecuencias abiertas (PMR446, CB 27 MHz) son inherentemente públicas y cualquiera puede escucharlas legalmente. Si transmites por radio, asume

que alguien escucha. El cifrado de voz en bandas de radioaficionado está prohibido por el Cuadro Nacional de Atribución de Frecuencias (CNAF), pero sí puedes usar códigos preacordados con significados no obvios.

Protocolo de comunicaciones cifradas para grupos familiares

Un protocolo práctico para un grupo familiar de 3-6 personas que combine métodos manuales y digitales según la disponibilidad de recursos.

Situación
Método de cifrado
Canal de comunicación
Ejemplo

Hay Internet y smartphones
Signal con grupo preconfigurado
Datos móviles o WiFi
Mensajes de texto y notas de voz cifradas E2E

Hay electricidad pero no Internet
Briar vía Bluetooth
Bluetooth entre dispositivos cercanos (
Mensajes cortos entre personas en el mismo edificio

Hay radio pero no electricidad para cifrado digital
Códigos preacordados + Vigenère
PMR446 o CB 27 MHz
«Tango 3 en Sierra» = familia reunida en punto de encuentro C

No hay electricidad ni radio
Cifrado de libro o Vigenère en papel
Notas escritas entregadas por mensajero
Referencia de libro con ubicación y estado

Evacuación en marcha
Señales visuales convenidas
Marcas en puertas, tiza, cinta
Cruz roja en puerta = casa evacuada, flecha = dirección tomada

Practica estos protocolos al menos dos veces al año con tu grupo familiar, igual que practicarías un simulacro de evacuación. La criptografía más sofisticada es inútil si nadie recuerda cómo usarla bajo presión.

 Advertencia: Esta información es orientativa y educativa. En situaciones de emergencia real, consulte a profesionales cualificados siempre que sea posible. No ponga en riesgo su vida ni la de otros sin la formación adecuada.