

Criptografía Aplicada a Comunicaciones por Radio

Autor: EA4IPV

Fecha: 22/03/2026

Categoría: DMR y Modos Digitales

Etiquetas: Sin etiquetas

Marco Legal: Lo que Puedes y No Puedes Hacer

En radioafición, el cifrado está prohibido por regulación internacional (UIT-RR Artículo 25.2A) y nacional (en España, el Cuadro Nacional de Atribución de Frecuencias). Las transmisiones deben poder ser decodificadas por cualquier estación. Sin embargo, existen métodos legítimos para proteger la información operacional sin cifrar las comunicaciones.

Códigos Operacionales

Los códigos preestablecidos dentro de un grupo NO son cifrado. Son abreviaciones operacionales, una práctica común en servicios de emergencia y militar:

CódigoSignificado realTipo

Vamos al mercadoReagruparse en punto de encuentroFrase clave

Paquete azulSituación bajo controlPalabra código

Tengo 3 manzanas3 personas en el grupoSustitución

La tienda cierra a las 5Movimiento a las 17:00Horario encubierto

Diseño de Códigos Efectivos

Memorizables: Máximo 20-30 códigos por persona. Más es inmanejable bajo estrés

Naturales: Las frases deben sonar como conversación normal

Inequívocos: Cada código debe tener un único significado posible

Renovables: Cambiar códigos periódicamente. Si sospechas que están comprometidos, activar el set alternativo

Esteganografía por Radio

La esteganografía oculta la existencia misma del mensaje. Técnicas aplicables a radio:

Spread Spectrum: Técnicas de espectro ensanchado (FHSS, DSSS) dispersan la señal por debajo del ruido.

Difícil de detectar pero requiere equipamiento especializado

Burst transmission: Mensajes pregrabados transmitidos en ráfagas de alta velocidad (duración <1 segundo).
Difícil de interceptar y localizar

Frecuencia variable: Cambiar de frecuencia según patrón preacordado (frequency hopping manual)

Comunicaciones en Bandas No Vigiladas

En un escenario de crisis, reducir la probabilidad de interceptación:

Potencia mínima: Solo la necesaria para el contacto. Menos potencia = menor huella de RF

Transmisiones cortas: Mensajes preparados antes de transmitir. PTT solo lo imprescindible

Frecuencias inusuales: Evitar frecuencias de llamada y de emergencia obvias

Antenas directivas: Yagi o moxon apuntando al destino reducen la radiación lateral

Horarios variables: No transmitir a la misma hora cada día

Protocolos Digitales y Ofuscación

Algunos modos digitales ofrecen cierta protección inherente:

JS8Call: El texto es legible pero requiere software específico para decodificar. No es cifrado pero añade una barrera técnica

VARA: Protocolo propietario que requiere software específico

DMR: La voz digital no se entiende sin decodificador DMR. El cifrado básico (BP) y mejorado (EP) están disponibles pero su uso en bandas de radioaficionado es ilegal

Bandas PMR y Licencia Libre

En bandas PMR446 (sin licencia), la regulación es diferente. No hay prohibición explícita de códigos en PMR446, aunque el cifrado integrado de algunos radios PMR tiene zonas grises legales. En la práctica, para comunicaciones de grupo cortas en PMR446, los códigos operacionales son la mejor opción.