Communications Security (COMSEC) | **Student Companion Guide** fortunefavorsthepreprared.com

COMPANION GUIDE TO ONLINE TRAINING

Requires Patreon subscription — use alongside the online lessons at fortunefavorsthepreprared.com/com-03-landing/

COM-03: COMMUNICATIONS SECURITY (COMSEC) STUDENT COMPANION GUIDE

The Operator's Field Reference

Physical Security, Key Management, Cryptographic Fundamentals, and Authentication
Four Domains · Key Custody Log · Authentication Rotation Log · COMSEC Posture Worksheet

Edition v1.0 · 2026

Semper Paratus, Semper Gumby
https://fortunefavorsthepreprared.com/
Nick Meacher

COM-03: COMMUNICATIONS SECURITY (COMSEC) — STUDENT COMPANION GUIDE

Companion Guide to Online Training

Published by Fortune Favors the Prepared
Thomasville, Pennsylvania
fortunefavorsthepreparedcom

Edition v1.0 | 2026

This companion guide requires an active Patreon subscription. It is designed to be used alongside the COM-03 Communications Security online training series at fortunefavorstheprepared.com/com-03-landing/. The online lessons are the instruction. This guide contains reference tables, worksheets, and the COMSEC Posture Worksheet template only — it does not contain the instructional content. It cannot be used as a standalone document.

ONLINE TRAINING ACCESS

The five online lessons are available to Patreon subscribers at the Operator tier or above:
patreon.com/fortunefavorsthepreparedcom

INSTRUCTOR-LED GROUP TRAINING

Group sessions and facilitated training are available. Contact:
fortunefavorstheprepared@protonmail.com

How to Use This Companion Guide

THIS GUIDE IS A COMPANION TO PATREON-GATED ONLINE TRAINING

This companion guide requires an active Patreon subscription. It is designed to be used alongside the COM-03 Communications Security online training series — the online lessons are the instruction. This guide contains reference tables, worksheets, and a COMSEC posture template only. It is not a standalone document.

Subscribe for online training access:

patreon.com/fortunefavorsthepreprepared

Online curriculum:

fortunefavorsthepreprepared.com/com-03-landing/

What this guide contains

For each of the five online lessons: a condensed reference summary covering only the key terms, tables, and standards — not the instruction. The Four-Domains checklist, the key-management best practices, and the U.S. regulatory table are included as working references. The COMSEC Posture Worksheet is in Part III. The instruction is delivered online — this guide is what you use in the field and when documenting your group's plan.

Required workflow — online lessons BEFORE using this guide

ORDER MATTERS

Do not open any section of this guide until the corresponding online lesson has been completed. The condensed summaries here are reference material, not instruction. The sequence below is required, not suggested.

Step 1 — Subscribe at patreon.com/fortunefavorsthepreprepared (Operator tier or above)

Step 2 — Access the online lessons at fortunefavorsthepreprepared.com/com-03-landing/

Step 3 — Complete all five lessons including knowledge checks

Step 4 — Use this guide in the field as a reference and to complete your group's COMSEC Posture Worksheet

THIS GUIDE IS NOT STANDALONE

The instruction for each lesson is delivered through the online training series. This guide contains condensed reference tables and a blank worksheet only. If you have not completed the online lessons, this guide will not teach you the material — it will give you tables whose meaning you do not yet understand.

Guide Map — What to Reference When

When you need…	Turn to…
What COMSEC protects and the four domains	Part I, Chapter 1
Physical security and key management best practices	Part I, Chapter 2
Cryptographic security fundamentals and the Enigma lesson	Part I, Chapter 3
How Signal, Session, Telegram, WhatsApp, Zello, and PoC radios stack up on COMSEC	Part I, Chapter 3
Authentication methods, isograms, DRYAD sheets, brevity codes	Part I, Chapter 4
U.S. radio regulations and what encryption is actually legal on your radios	Part I, Chapter 5
A one-page checklist to sanity-check your group's COMSEC posture	Part II, Chapter 6
A blank Key Custody Log to fill in	Part III — Key Custody Log Worksheet
A blank Authentication / Brevity Code Rotation Log	Part III — Rotation Log Worksheet
The blank COMSEC Posture Worksheet (the course capstone exercise)	Part III — COMSEC Posture Worksheet
How COMSEC relates to OPSEC, RTSA, PREP-CON, and COMCON	Part IV, Chapter 7
Doctrinal sources behind the method	Part IV, Chapter 8

PART I — REFERENCE TABLES

Chapter 1: What COMSEC Protects

COMSEC — Communications Security — is the discipline of preventing an adversary from intercepting, exploiting, or deriving intelligence value from your communications, while still getting the message to the people who need it, on time. It is a layered system of procedures, equipment, discipline, and awareness — not a single tool or product.

Three things COMSEC protects

Protects	Meaning
Content	What is actually said — protected by encryption, brevity codes, and operator discipline about what goes out over the air.
Context	Who is communicating, how often, and when — metadata that can reveal information even when content is unreadable.
Continuity	Your ability to keep communicating under degraded or hostile conditions.

The four domains of COMSEC

Domain	Covers	Where covered in depth
Transmission Security (TRANSEC)	Reducing the chance a transmission is detected, intercepted, or jammed — power discipline, directional antennas, short/irregular transmissions.	COM-04, EMCON
Emissions Security (EMSEC)	Denying intelligence from unintended electromagnetic emissions.	COM-04, EMCON
Cryptographic Security (CRYPTOSEC)	Proper selection, use, rotation, and destruction of cryptographic systems and keys.	This course (Ch. 3); COM-09 for the full dedicated course; COM-07 for One-Time Pads
Physical Security of COMSEC Material	Protecting radios, codebooks, keys, and authentication material from loss, theft, or compromise.	This course (Ch. 2)

ONE WEAK DOMAIN COMPROMISES THE WHOLE SYSTEM

A perfectly encrypted message is worthless if the key was stolen because it was left in an unlocked vehicle. COMSEC fails at its weakest domain, not its strongest.

The modern threat picture

Modern monitoring capability includes automated spectrum scanning, AI-assisted pattern recognition, and networked direction-finding. COMSEC failures are now detected faster, more broadly, and more quietly than in the era of a single human intercept operator. This raises the value of consistent procedural discipline — it does not make COMSEC hopeless for a preparedness group.

Encrypted content still leaks context

On most digital radio systems, including trunked and DMR systems, the radio ID and talkgroup ID are not encrypted even when the voice content is. A scanner capable of decoding the system's control channel can see which radio IDs are transmitting on which talkgroups in real time, whether or not it can hear a word of the actual conversation — enough to build a traffic-pattern picture without ever breaking the encryption. A sharp increase in activity on a talkgroup known to be assigned to a SWAT team is a reasonable basis to hypothesize an operation is underway, purely from who is talking to whom and how often. System assignments and talkgroup labels for a given radio system are frequently documented by hobbyists at radioreference.com — worth knowing both as a monitoring resource and as a reminder that your own group's talkgroup structure may already be mapped somewhere if it resembles a public system.

Encryption protects content. It does not protect who is talking, how often, or to which group. A fully encrypted talkgroup can still be pattern-analyzed from the outside using nothing but ID and traffic-volume data.

Not everyone can fight. Everyone benefits from secure communications.

Why This Matters in a Disaster

It is easy to treat COMSEC as an abstract discipline until you picture the actual moments where it matters. Two of the most common are worth walking through directly, because neither one requires an adversary with sophisticated equipment -- just someone listening.

Situation reports can be a target list

SALUTE reports and similar structured situation reports -- covering Size, Activity, Location, Unit, Time, and Equipment -- are a normal, useful part of disaster response. They are also, read a different way, a list of which structures are damaged, unoccupied, or unsecured, and where casualties or fatalities are located. A group broadcasting an unencrypted, unauthenticated situation report over an open channel is potentially broadcasting a target list to anyone with a scanner who wants to know which houses are empty and unguarded.

The practical alternative: put it on a bicycle instead of on the air. If a SALUTE report is sensitive enough that broadcasting it worries you, the simplest fix is often to not broadcast it at all -- a written report hand-carried by courier never has to touch a radio. This is a genuinely good task for older kids in a family or group: a bicycle courier run is well within a capable pre-teen or teenager's ability, gives them a concrete job during a stressful event, and is worth practicing before you need it.

Family bike rides around the neighborhood in ordinary times double as reconnaissance -- a young courier who already knows every street and cut-through from routine rides will move faster and more confidently under real pressure.

The full doctrine on this method is its own course, COM-08, Dead Drop and Courier Protocols. SALUTE and SPOT reporting itself is covered in depth in INT-03, SALUTE and SPOT Report Training.

Casualty and fatality information deserves the same discipline

Passing information about the deceased or seriously injured over an open channel, where literally anyone with a receiver can hear it, is simply not good practice — independent of any tactical concern. Family members may be monitoring the same frequency and could learn of a loss secondhand before anyone has the chance to notify them properly. Treat casualty and fatality reporting with the same discipline you would want applied if it were your own family being discussed.

The earpiece is the most overlooked COMSEC control you own

Every tool in this course protects the transmission. None of them protect what happens after the audio comes out of a speaker. If a radio is set to loud speaker output, anyone standing near the operator hears the traffic just as clearly as the intended recipient does — fully encrypted or not. A basic, no-cost precaution is to default to an earpiece or headset rather than a speaker mic, especially any time sensitive information might be passed.

A real-world illustration: many law enforcement agencies run fully encrypted radio systems, yet officers commonly carry a speaker mic instead of an earpiece. The encryption does its job on the air — but anyone standing near the officer hears everything the radio receives, in the clear, the moment it comes out of that speaker.

During a search, this can tell a hiding suspect exactly where the officer is. It gets worse if a dispatcher radios that a subject has an active warrant while that subject is standing next to the officer -- the suspect hears it before the officer has a chance to react, gaining a head start to flee or a reason to attack first. The encryption did not fail. The acoustic environment around the radio did.

Chapter 2: Physical Security and Key Management

Physical security is often the weakest link in an otherwise sound COMSEC system — it does not require breaking any code, only gaining access.

Protected material includes

- Radios and accessories capable of secure operation
- Encryption keys and key-loading devices
- Codebooks, one-time pads, and authentication sheets
- Written procedures, cheat sheets, and net rosters

Four best practices

Rule	In practice
Restrict on need-to-know	Fewer hands touching key material means a smaller compromise surface if something goes wrong.
Never leave material unattended	Even a locked vehicle does not count as attended. Unattended means unattended, even for a few minutes.
Assume lost equals compromised	Do not wait to see if lost material turns up. Rotate immediately once anything cannot be accounted for.
Destroy expired/used material immediately	A used pad page or expired table sitting in a drawer is a liability with no upside.

THE RULE MOST GROUPS SKIP

"Assume lost equals compromised" is tempting to delay, especially when replacing key material is inconvenient. That hesitation is exactly the gap an adversary needs.

Secure key exchange — in order of preference

Method	Notes
Hand-carry	The gold standard. A trusted person physically delivers the material — no transmission, no interception risk in transit.
Encrypted channel + out-of-band password	Acceptable secondary option. The password travels through a different channel than the file, so intercepting one channel alone does not expose the key.
Electronic transmission of the key itself	Avoid whenever possible. Multiplies the points where interception could occur.

Chapter 3: Cryptographic Security Fundamentals

This chapter covers CRYPTOSEC at the level every operator should know. A full course dedicated to cryptographic security in depth — COM-09, Cryptographic Security (CRYPTOSEC) — covers this domain the way COM-06 covers Authentication and COM-07 covers One-Time Pads: as a dedicated deep dive on a domain this course only introduces.

Cryptanalysis exploits human and procedural failures far more often than mathematical weaknesses in an algorithm.

Three core principles

- The longer a key is used, the more vulnerable it becomes.
- Poor implementation defeats strong algorithms.
- Reuse is catastrophic in manual systems.

The Enigma lesson: two procedural failures, not a math break

German Enigma keys changed daily and were, mathematically, very difficult to break through cryptanalysis alone. What actually enabled sustained exploitation was a pair of human and procedural failures, not a mathematical shortcut.

Predictable message keys (“cillies”): each message opened with a three-letter key that was supposed to be random. Operators under time pressure sometimes took shortcuts — keyboard patterns, or personal initials — instead. Bletchley Park came to call these predictable keys “cillies,” reportedly after an operator was found repeatedly using his girlfriend's initials instead of a random letter group. Once analysts learned an operator's habit, that day's key was a high-confidence guess, not a secret.

Predictable content (“cribs”): German traffic was formulaic enough to guess fragments of plaintext in advance. Routine weather reports used standard wording at predictable times, and many messages closed with the same sign-off, “Heil Hitler.” Knowing a specific word almost certainly appeared somewhere in a message let codebreakers work backward from a known plaintext-ciphertext pairing, sharply narrowing the settings the Bombe had to search.

This history is dramatized in the 2014 film The Imitation Game. The film takes real dramatic license with several plot details, but the underlying cryptographic facts here -- cillies and weather/sign-off cribs -- are genuine, documented weaknesses Bletchley Park exploited.

FURTHER READING

For the fuller institutional history behind Bletchley Park -- how the Government Code & Cypher School fit into the founding of MI5 and MI6, the Special Operations Executive, and the wartime spy network that later seeded the American intelligence community -- see "MI5, MI6, Bletchley Park & Camp X," Part 1 of the Architecture of Intelligence series at fortunefavorstheprepared.com/mi5-mi6/.

THE LESSON

Crypto is only as strong as its procedures. A message key is only random if it is actually random -- not convenient, not memorable, not personal. If your group ever adopts a keyed cryptosystem, the operator who picks “easy to remember” keys is doing exactly what the Enigma operator did with his girlfriend's initials.

Modern voice encryption

Modern secure voice systems generally rely on AES. AES is described in Federal Information Processing Standard (FIPS) 197, and FIPS 140-2 governs how AES is applied to cryptographic modules in radio systems -- the algorithm and its implementation are governed by two separate standards. AES became effective as a federal standard on May 26, 2002, after NIST found it compliant with FIPS requirements and the Secretary of Commerce approved it.

AES replaced DES, and the timeline matters: DES, developed in 1977, was first cracked by the Electronic Frontier Foundation in 1997 in 84 days, then cracked again faster in 1998 and twice more in 1999. NIST withdrew its endorsement of DES for secure federal communications after May 2005, and AES became required for all federal agency communications systems beyond May 2007. FIPS 140-2 requires all federal agencies to use AES, and under the Cybersecurity Enhancement Act of 2014, any state or local agency wanting to interoperate on a federal LMR system must also have AES on their subscriber units.

Many agencies have transitioned from DES-based to P25 AES-based systems, leaving a surplus of legacy encrypted radios and key loaders on secondary markets — these require dedicated encryption modules, licensing, and programming software, and remain line-of-sight limited without repeaters. Improper key handling or a programming error can silently break interoperability.

Key rotation in practice

The baseline agency policy across most government users is to rotate keys every 30 days, with some agencies rotating more frequently. Historically, the practical obstacle was physical -- every radio had to be connected to a key loader by hand. Over-The-Air Rekeying (OTAR) pushes new keys to every subscriber radio remotely; Over-The-Air Programming (OTAP) does the same for full reprogramming. Together they remove the physical bottleneck that used to make frequent rotation impractical at scale.

FURTHER READING -- CISA/SAFECOM ENCRYPTION GUIDANCE

CISA, through the Federal Partnership for Interoperable Communications (FPIC) and SAFECOM/NCSWIC, publishes the standing reference set on LMR encryption for public safety. Foundational/overview: The Who, What, When, Where, How, and Why of Encryption in P25 Public Safety Land Mobile Radio Systems (May 2023); Considerations for Encryption in Public Safety Radio Systems and its companion fact sheet, Determining the Need for Encryption in Public Safety Radios; Guidelines for Encryption in Land Mobile Radio Systems: Determining What Encryption Method to Use for Public Safety Radios. Key management: Operational Best Practices for Encryption Key Management (Aug 2020), referencing FIPS PUB-197 and TIA-102.AAAD-B; the Encryption Key Management Fact Sheet (2020). Algorithm transition: The Transition to Advanced Encryption Standard White Paper. Link-layer security: Link Layer Authentication (LLA) and Link Layer Encryption (LLE): Are You Really Secure? (2022). Cybersecurity/risk context: Cyber Risks to

Land Mobile Radio -- First Edition (2022); Communications Security -- Protecting Critical Information, Personnel, and Operations.

Nick Meacher, the author of this course, was directly involved in drafting two of the documents referenced above: Considerations for Encryption in Public Safety Radio Systems and Guidelines for Encryption in Land Mobile Radio Systems: Determining What Encryption Method to Use for Public Safety Radios.

Where OTP, book ciphers, and steganography fit

Method	Core idea	Where it fits
One-Time Pad (OTP)	Provably unbreakable when used correctly — truly random keys, key length ≥ message length, never reused, destroyed immediately. Violating any rule collapses the security.	Full course: COM-07
Book ciphers	Two identical books plus pre-agreed indexing rules. Plausible deniability, but vulnerable to computational analysis and known-plaintext attacks.	Low-threat, covert-in-plain-sight use only
Steganography	Hides a message inside ordinary media rather than encrypting it. Best used after encryption, not instead of it.	Covert digital delivery only

Field reference: the same Brevity Cards for OTP set used for brevity codes in Chapter 4 also includes a bonus checkerboard, encryption/decryption instructions, and an OTP conversion grid for pairing with the full One-Time Pad course, COM-07 (fortunefavorstheprepared.com/product/brevity-carsd-for-one-time-pads/).

Commercial Messaging Apps and Cellular PTT in a COMSEC Context

Most groups already use a phone-based app for day-to-day coordination alongside radio. Every one of these tools sits entirely on the CRYPTOSEC side of the four domains from Chapter 1 — none of them provide TRANSEC, EMSEC, or continuity when cellular and internet infrastructure are down. Evaluate each honestly rather than trusting a marketing claim of “encrypted.”

Platform	Content encryption	Metadata / context exposure	COMSEC notes
Signal	True end-to-end by default (Signal Protocol, open-source, audited) for all messages, calls, groups	Minimal — Sealed Sender hides sender identity from Signal's own servers	Best-in-class CRYPTOSEC here. Requires a phone number to register; both parties must be on Signal
Session	True end-to-end (Signal-derived protocol)	Best of this group — no phone/email, onion-routed, no central log of who talks to whom	Public ‘Communities’ are not end-to-end. Smaller audit history than Signal
Telegram	Not end-to-end by default (Cloud Chats). True E2E only in opt-in Secret Chats (1:1 only)	Weak — retains IP, device details, phone number	Treat default chats as readable by the provider
WhatsApp	True end-to-end for content (Signal Protocol) by default	Weak — Meta collects contact/timing/frequency metadata outside the encryption guarantee	Protects content, not who is talking to whom. Cloud backups need separate opt-in
Zello	Depends on tier — free open channels are not encrypted at all; paid Zello Work channels are encrypted	Weak on open channels, public by design	A free-tier open channel is a public broadcast. Know your tier and settings
PoC radios (e.g. Motorola WAVE, ESChat, Kodiak)	AES-256 common, sometimes FIPS-referenced	Weak — many devices include built-in GPS tracking, plus vendor cloud logs	Encryption is hop-to-hop through the vendor's cloud server, not end-to-end. Proprietary ecosystems rarely interoperate without a gateway

PoC (Push-to-Talk over Cellular) turns a phone or purpose-built device into a walkie-talkie using cellular data instead of RF spectrum. Carrier-based versions (AT&T Enhanced PTT, Verizon PTT Plus) tie to one provider; over-the-top versions (Motorola WAVE PTX, ESChat) run on any carrier's data network. Both depend entirely on commercial cellular coverage. The basic path every transmission takes is Radio -> Cellular Network -> PoC Server -> Cellular Network -> Radio -- that PoC Server is exactly the point where a vendor's cloud infrastructure has a technical opportunity to decrypt and process the call.

THE RECURRING PATTERN

Content encryption is common; metadata protection is rare; infrastructure independence is nearly nonexistent. Signal and Session are the only two here with strong metadata protection, and none of the six work at all without cellular or internet service. In a PACE plan, every tool on this table belongs in the Primary or Alternate tier — never Contingency or Emergency.

Further reading on how PoC radios actually work, their range, and where they fit in a layered communications plan: “Radio over LTE (cellular),” fortunefavorstheprepared.com/preparedness-book-of-knowledge-2/communications/communications-radio-over-lte/.

Chapter 4: Authentication and Message Verification

Authentication answers two questions: who actually sent this message, and are they transmitting freely or under duress. Voice recognition alone answers neither reliably.

Two authentication methods

Method	How it works
Challenge and reply	Requires two-way communication. The called party always issues the first challenge — never the caller. Only the responding station is verified; a challenge is never accepted as authentication by itself. Challenge and correct reply are never sent in the same transmission.
Transmission authentication	Used when two-way exchange is impossible or impractical (e.g. a one-way broadcast). A pre-arranged authentication table provides a verification code without a live exchange.

A full course on formal challenge/reply protocol and duress signaling — COM-06, Authentication and Challenge/Reply — covers this subject in much greater depth.

Isograms for rapid authentication

An isogram is a word with no repeating letters. Each letter is assigned a digit, letting a pre-briefed pair of stations authenticate quickly without transmitting the full word.

A	F	T	E	R	S	H	O	C	K
1	2	3	4	5	6	7	8	9	0

Strengths: fast, low-tech. Limitations: must rotate frequently; never transmit the full word.

DRYAD sheets

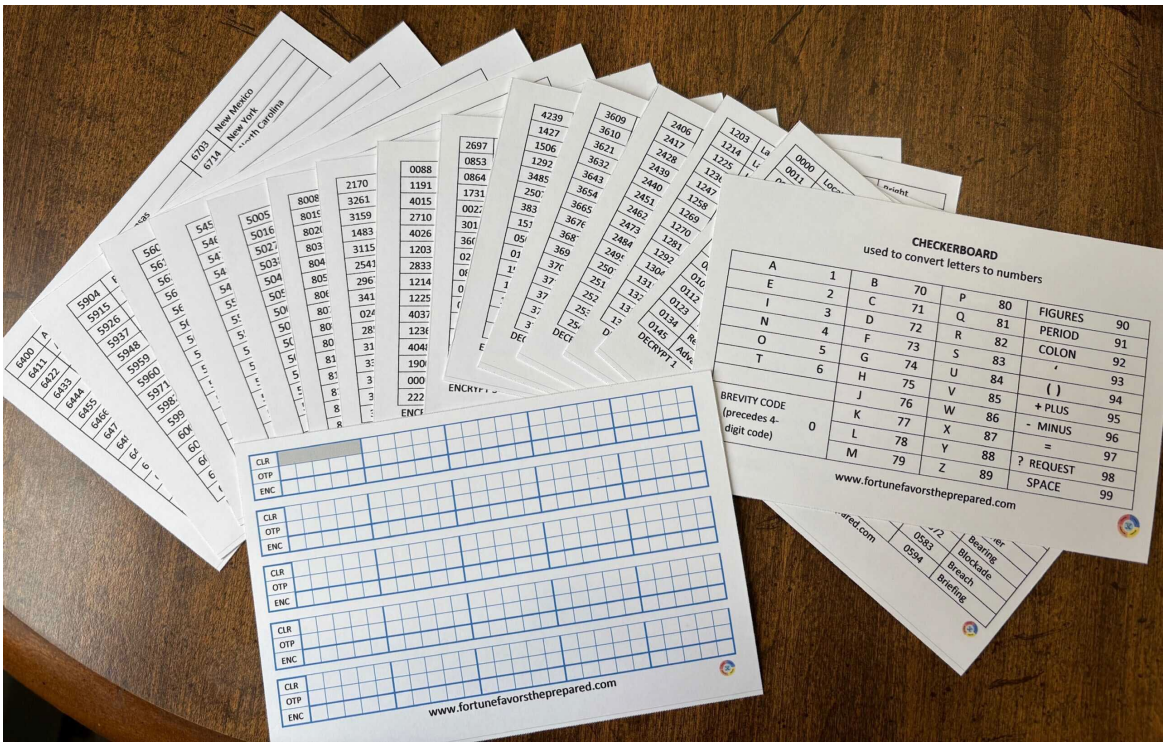
Manual authentication and numeric-encryption aids designed for speed and field use, typically on crypto periods of six hours or less. Easy to destroy, resistant to traffic analysis when rotated properly. Used for authentication, numeric encryption of frequencies/coordinates, and one-way broadcast authentication.

DRYAD sheets are procedurally secure, not mathematically strong — discipline is essential.

Code words and brevity codes

Replace a long message with a single prearranged word — shortens transmission time and obscures meaning even if intercepted in the clear. Rotate frequently, never reuse a word for a different meaning, and maintain one controlled master list.

Encrypting letter-by-letter is slow and error-prone — a 10-letter word can take up to 20 encrypted digits, and a phrase like ‘emergency shelters established’ can run to 50. A brevity code collapses either to a single 4-digit code (preceded by a zero marking it as a brevity code).
The Brevity Cards for OTP set (fortunefavorsthepreparedcom/product/brevity-carsd-for-one-time-pads/) is a ready-made controlled master list: 16 double-sided cards with 450+ common SITREP/LP-OP/disaster words organized numerically and alphabetically, 60 prebuilt phrases, and blank slots for your own entries. Codes use the Verhoeff algorithm, which includes a check digit specifically to catch transposition errors.



The Brevity Cards for OTP set. Word/phrase cards are numbered for lookup in both directions; the checkerboard card (right) converts letters to numbers for OTP encryption, with codes 90-99 reserved for figures and punctuation; the blank grid cards (front) are worksheets for building the clear text, pad, and encrypted lines of an OTP message.

Chapter 5: U.S. Radio Regulations and Encryption

Know what is actually legal on the frequencies your group uses — this determines which tools in this guide are usable for licensed operation. Each service blocks encryption through a different legal mechanism; the details matter.

Amateur Radio (Part 97)

The core rule is §97.113(a)(4), which prohibits amateur stations from transmitting messages encoded for the purpose of obscuring their meaning, except as otherwise provided in the rules.

Not all encoding is banned. The FCC has confirmed the rule targets obscuring meaning specifically — authentication or password schemes used on digital networks have not been found to violate §97.113(a)(4), because their purpose is verification, not concealment. This is why the authentication tools in Chapter 4 remain legal on Amateur frequencies while content encryption does not.

WHY YOUR RADIO'S MENU HAS AN ENCRYPTION OPTION IT IS ILLEGAL TO USE

Popular DMR radios such as the AnyTone AT-D878UV / AT-D578UV — and most DMR radios like them — ship with an encryption menu even though using it on Amateur frequencies violates §97.113(a)(4). The reason is manufacturing economics, not a loophole.

The DMR standard, as defined by ETSI, includes encryption as an optional feature for the commercial and public-safety dispatch systems it was actually built to serve — business security, utility crews, private fleets, and similar Part 90 users where privacy is a legitimate operational need.

Manufacturers build one hardware/firmware platform and sell it across every market the chipset supports: Part 90 commercial licensees, GMRS and equivalent services abroad, and Amateur operators, who receive the identical physical radio. Building a stripped-down amateur-only version without the encryption menu would cost more than it is worth, so the feature ships present in firmware and the licensing framework — not the hardware — governs whether using it is legal.

The menu option existing on your radio is not FCC guidance about what your license permits; it is a byproduct of the radio being built for a bigger market than amateur radio alone.

What's actually in the menu: AES-256 versus ‘ARC’ encryption

A note on why this is included: the model and feature details below are provided for awareness and completeness — so you can recognize what you are looking at if you see these options in a radio's menu, and understand why they are there. Nothing here is an endorsement or encouragement to enable encryption on Amateur or Part 95 frequencies. As covered throughout this chapter, doing so is not legal on those services regardless of which option a radio offers or how strong it is.

Several current AnyTone DMR models advertise AES-256 encryption as a built-in feature, including the AT-D878UV, AT-D878UVII Plus, AT-D168UV, AT-D890UV, AT-D578UV, and the AT-268. Manufacturer listings for the AT-D168UV specifically mention both AES-256 encryption and “ARC Encryption” as separate options, and the AT-D890UV listing includes AES-256 digital encryption alongside its other DMR features. These two options are not remotely equivalent.

‘ARC’ (also written ARC4) refers to the RC4 stream cipher as implemented for DMR — sometimes called ‘Alleged RC4’ because the original algorithm was proprietary and was reverse-engineered and published anonymously rather than officially released. In DMR programming software it commonly shows up labeled ‘Basic Encryption’ or ‘Common/Extended Encryption’ rather than by the ARC4 name directly. It is weak by modern standards — well-documented cryptographic weaknesses, considered obsolete and broken, crackable with widely available tools. It deters a casual scanner listener; it is not a real security measure, and should never be confused with the AES-256 option in the same menu.

Neither option is legal to use on Amateur or Part 95 frequencies — regardless of strength. Cryptographic strength and legal permission are two separate questions. A weak cipher is not ‘probably fine’ because it is easy to crack, and a strong cipher is not legitimized because the manufacturer built it in. If your license is Amateur or Part 95, both options in that menu are off-limits for on-air use.

Why DMR encryption mostly deters casual listeners, not analysts

Most hobbyist scanners cannot decode DMR out of the box — it typically requires a separate add-on module most casual owners never buy. Amateur Radio's 1.25-meter band is similarly absent from most consumer scanners entirely. The result is a kind of security through obscurity: a transmission on Amateur DMR or the 1.25-meter band is already outside what the average scanner hobbyist can hear, encrypted or not. That is a real, if limited, protection against casual listeners — but not against a dedicated analyst with the right equipment, and not a legal basis for running actual encryption.

Personal Radio Services (Part 95: GMRS, FRS, MURS, CB)

There is no single blanket clause across all of Part 95 the way §97.113(a)(4) works for Amateur. Encryption is locked out through two different mechanisms:

Mechanism	How it works
Equipment certification bar (all four services)	The FCC will not issue an equipment certification grant for any transmitter incorporating voice scrambling or other voice-obscuring features, for any Personal Radio Service providing voice communications on shared channels — applies to applications filed on or after December 27, 2017. A certified radio on these services cannot ship with scrambling capability at all.
GMRS-specific operating rule	§95.1733(a)(3) additionally bars GMRS stations from sending coded messages or messages with hidden meanings. Ordinary ‘10-codes’ are specifically excepted. FRS, MURS, and CB have no equivalent dedicated rule — they rely on the general Subpart A prohibitions (§95.333) plus the certification bar above.

Business and Industrial Pool (Part 90)

Encryption is permitted. Proprietary encryption is common, typically weaker than AES but adequate against casual interception. Programming-based keys remain vulnerable if a radio is physically captured.

THE PRACTICAL IMPLICATION

If your group's primary radios are Amateur, GMRS, FRS, MURS, or CB — the large majority of family and MAG setups — encryption is not a legal option during routine, licensed operation, whether through a direct operating rule (Amateur, GMRS) or because no certified radio on that service can legally ship with the capability (FRS, MURS, CB). Your COMSEC posture on those services is built from authentication, brevity codes, physical security, and operational discipline. That is not a limitation of COMSEC — it is most of what COMSEC actually is for the average group.

Source: ARRL comments on RM-11699, discussing FCC guidance on §97.113(a)(4) and permitted authentication schemes.

PART II — QUICK-REFERENCE TOOLS

Chapter 6: Four-Domains Sanity Check

Run through this before considering your group's COMSEC posture complete. A “no” on any line is a gap, not a formality.

Domain	Sanity-check question	Y / N
TRANSEC / EMSEC	Does your group have a documented transmission discipline (see COM-04, EMCON)?	
CRYPTOSEC	Is encryption actually legal on the radios you plan to use it on (Ch. 5)?	
Physical Security	Is every item of key/authentication material on a written, need-to-know access list (Ch. 2)?	
Authentication	Does your group have a rotating authentication method that does not depend on voice recognition alone (Ch. 4)?	

PART III — BLANK WORKSHEETS

Complete each worksheet and keep it with your group's other planning documents. Use a separate copy per item or per session as noted. Write “N/A” rather than leaving a line blank.

Key Custody Log Worksheet

Item description:

Assigned to (need-to-know):

Date issued:

Rotation / expiration date:

Date destroyed / returned:

Confirmed by:

Authentication / Brevity Code Rotation Log

Item (isogram / DRYAD set / brevity word)	Effective date	Rotation date	Destroyed?

COMSEC Posture Worksheet

THIS IS THE COURSE CAPSTONE

Complete this after finishing Lesson 5 online. This worksheet, filled in and kept with your other group planning documents, is a working COMSEC posture.

1. Protected material list (every radio, codebook, sheet, and procedure your group has):

2. Access assignments (who needs access to each item, in writing):

3. Rotation schedule (interval for codes, authentication sets, and any key material):

4. Lost-material procedure (exact steps the moment anything cannot be accounted for):

5. Legal footing (FCC service for each radio; confirm no reliance on illegal encryption):

PART IV — CURRICULUM CONTEXT AND SOURCES

Chapter 7: How COM-03 Relates to the Rest of the Curriculum

COMSEC does not stand alone. It is one discipline among several that overlap in a group's overall security and readiness posture.

Course	Relationship to COM-03
COM-09, Cryptographic Security (CRYPTOSEC)	The full dedicated deep dive on the CRYPTOSEC domain this course introduces in Chapter 3 -- covers cryptographic security in depth the way COM-06 covers Authentication and COM-07 covers One-Time Pads.
SEC-02, OPSEC	OPSEC is the broader discipline of protecting all critical information about a group, not just communications. COMSEC (this course) is the communications-specific application of that same need-to-know, compartmentalization thinking — see Chapters 1 and 2.
INT-02, Radio Traffic Situational Awareness (RTSA)	RTSA teaches how to read a net's health and condition from traffic patterns alone — exactly the capability the Modern Threat Picture in Chapter 1 warns that adversaries now have. Understanding RTSA means understanding what your own group's traffic reveals to someone monitoring it.
PLN-04, PREP-CON (Readiness Conditions)	PREP-CON defines your group's overall readiness condition level. COMCON (below) nests underneath it, and by extension so does your COMSEC posture.
PLN-05, COMCON (Communications Conditions)	COMCON defines escalating condition levels specifically for communications infrastructure. As COMCON tightens, the COMSEC Posture Worksheet in Part III should be reviewed and tightened alongside it — shorter rotation intervals, stricter access, more disciplined content.

Chapter 8: Doctrinal Sources

Source	Publisher	Relevance
MCRP 3-40.3B: Radio Operator's Handbook	United States Marine Corps	TRANSEC, EMSEC, CRYPTOSEC and physical security definitions; authentication doctrine (challenge/reply and transmission authentication) referenced in Chapter 4.
FM 6-99: Army Report and Message Formats	Department of the Army, 2013	Message authentication line conventions referenced across standard report formats.
47 CFR Part 97 (Amateur Radio Service)	Federal Communications Commission	§97.113(a)(4) obscuring-meaning prohibition and permitted authentication practices referenced in Chapter 5.
47 CFR Part 95 (Personal Radio Services)	Federal Communications Commission	Equipment certification bar on voice-obscuring features and the GMRS-specific coded-message rule (§95.1733(a)(3)) referenced in Chapter 5.
47 CFR Part 90 (Private Land Mobile Radio)	Federal Communications Commission	Permitted encryption in the business/industrial pool referenced in Chapter 5.

Communications discipline is a force multiplier. Without it, coordination fails and security degrades quickly, regardless of how good any single piece of equipment is. Like every other skill in this curriculum, COMSEC has to be practiced under realistic conditions — not just studied.

COM-03 Student Companion Guide · fortunefavorstheprepared.com