

FAQ - TactoCRYPT High-Grade Secure Files & Messages Encryption BlackBOX

What is TactoCRYPT in one sentence?

TactoCRYPT is a hardware device that adds an independent encryption layer to communications, designed to protect sensitive exchanges even if a **smartphone or network is compromised**.

How is this different from Signal, WhatsApp, or Telegram?

Signal, WhatsApp, and similar apps provide "strong encryption inside the smartphone".

TactoCRYPT addresses a different problem:

> What happens when the smartphone itself cannot be trusted?

TactoCRYPT moves cryptographic operations **outside the phone**, so even if the phone is infected with spyware, it only ever sees **already-encrypted data**.

It is **not a replacement** for secure messaging apps — it is **an additional layer**.

Can governments break TactoCRYPT?

There is **no evidence** that governments can "break" the cryptography used by **TactoCRYPT** when it is implemented correctly and used as designed.

TactoCRYPT relies on widely accepted cryptographic primitives:

- * X25519 (elliptic-curve Diffie–Hellman)
- * HKDF-SHA256
- * HMAC-SHA256
- * Hardware-based random number generation

However, like all security systems:

- * It does **not claim to be unbreakable**
- * It does **not defeat all forms of surveillance**

TactoCRYPT is designed to drastically reduce attack surface, not promise absolute immunity.

Can TactoCRYPT be hacked?

No security device can claim to be impossible to hack.

TactoCRYPT is designed to:

- * minimize software complexity
- * avoid cloud dependencies
- * avoid long-term keys
- * use ephemeral sessions and per-file encryption

Its threat model assumes:

- * hostile networks
- * compromised smartphones

It does **not** claim protection against:

- * physical coercion
- * device seizure
- * user error

Is TactoCRYPT legal?

In most jurisdictions, **using encryption is legal.**

TactoCRYPT:

- * does not exploit vulnerabilities
- * does not bypass networks
- * does not provide anonymity services
- * does not hide metadata such as file size or timing

It is **a defensive security tool**, similar in nature to encrypted storage or secure communication devices.

Users are responsible for complying with local laws.

Is this “military-grade encryption”?

TactoCRYPT **does not use marketing labels like “military-grade.”**

Instead, it uses:

- * modern, publicly reviewed cryptographic primitives
- * open, well-understood algorithms
- * conservative security design choices

Security comes from architecture and correct implementation, not slogans.

Does TactoCRYPT provide anonymity?

No.

TactoCRYPT:

- * protects the **content** of communications
- * does not hide who is communicating
- * does not hide timing, size, or traffic patterns

It is about **confidentiality and integrity**, not anonymity.

Can it protect against spyware like Pegasus?

TactoCRYPT is designed to address a known limitation of messaging apps:

> If spyware controls the smartphone, it can observe **data before encryption or after decryption**.

By moving encryption into **external hardware**, **TactoCRYPT** prevents spyware from seeing unencrypted content that the user chooses to hide.

However:

- * It cannot remove spyware from a phone
- * It cannot protect against screen recording or physical surveillance

However, **TactoCRYPT** significantly **increases the cost and complexity** of surveillance, and with proper application of standard Counterintelligence techniques, **it can largely render it completely ineffective**.

Why is hardware important here?

Modern smartphones are:

- * extremely complex
- * constantly connected
- * frequent targets for zero-click exploits

Hardware separation allows:

- * simpler, auditable code
- * isolated key material
- * reduced trust in the phone's operating system

This is the same reason hardware security modules (HSMs) are used in banking and infrastructure.

Who is TactoCRYPT designed for?

TactoCRYPT is intended for:

- * investigative journalists
- * sources and whistle-blowers
- * activists and civil-society organizations
- * companies and organization for their "at risk" communication
- * anyone operating in high-risk digital environments

It is not aimed at mass consumer messaging.

Does TactoCRYPT hide metadata?

No.

TactoCRYPT does **not** claim to hide:

- * file size
- * communication timing
- * network endpoints

It focuses on protecting **content**, not traffic analysis resistance.

Can TactoCRYPT be misused?

Like any encryption technology, it can be used by anyone.

TactoCRYPT is designed and presented as:

- * a defensive tool
- * focused on protecting free speech and journalistic work
- * people and corporate for security and anti-spying of documents exchange.
- * transparent about its limitations

It does not include features specifically designed to evade law enforcement or enable criminal activity.

Is TactoCRYPT open source?

The code is disclosed on demand for audit by security reviewers under NDA.

TactoCRYPT is built on open, publicly reviewed cryptographic standards. Some implementation details may be published to facilitate analysis by partners.

Why should journalists care?

Because history has shown that:

- * smartphones can be compromised silently
- * encrypted apps cannot protect data once the device is infected
- * journalists and sources are frequent targets

TactoCRYPT is about **reducing dependency on fragile software ecosystems** and restoring a measure of control.

What does TactoCRYPT not promise?

TactoCRYPT does not promise:

- * anonymity
- * invisibility
- * immunity from surveillance
- * protection against physical threats

It promises strong confidentiality for documents and short messages in hostile digital environments, nothing more — and nothing less.