# Cryptography of Tetra

TETRA uses air as a medium of communication. The air interface is the RF (Radio Frequency) link between the MS and the BS. It uses TETRA Encryption Algorithm (TEA) is for encryption. The encryption provides confidentiality (protect against eavesdropping) as well as protection of signaling.

The encryption algorithms used in TETRA are TEA1 (TETRA encryption algorithm 1), TEA2 (TETRA encryption algorithm 2), TEA3 (TETRA encryption algorithm 3) and TEA4 (TETRA encryption algorithm 4).

1. TEA1: TEA1 is a symmetric encryption algorithm (128-bit key) used in the early TETRA system. It is intended for commercial use and restricted export. It is the default and mandatory encryption algorithm for TETRA Encryption mode 1(E1). In E1, all voice and data traffic are encrypted using TEA1, and users cannot disable encryption. TEA1 is a proprietary encryption algorithm, and the details of its operation are typically not publicly disclosed to enhance security. While TEA1 provides a reasonable level of security, it is considered less secure than the subsequent TEA versions.
2. TEA2: TEA2 is an enhanced version of the encryption algorithm designed to provide a higher level of security compared to TEA1 and it is used in national emergency services within Europe. It uses a 256-bit key for encryption. TEA2 is typically employed in TETRA Encryption Mode 2 (E2). In E2, encryption is optional, and users or user groups can choose whether to enable encryption or not.
3. TEA3: TEA3 is another version of the TETRA encryption algorithm, introduced to provide even stronger security. It is used in Extra European Emergency Services. TEA3 uses a 256-bit key for encryption, like TEA2, but may have improved security features. TEA3 is also used in Encryption Mode 2 (E2), making encryption optional for users.
4. TEA4: TEA4 represents the latest version of the TETRA encryption algorithm, developed to further enhance security. It is used in Commercial use and restricted exports as that of TEA1. Like TEA2 and TEA3, TEA4 uses a 256-bit key for encryption. As with the other TEA versions, TEA4 is typically used in Encryption Mode 2 (E2), where encryption remains optional.

The choice of which TEA version to use (TEA1, TEA2, TEA3, or TEA4) depends on network operators' security requirements and the specific regulations in place in each jurisdiction. While TEA1 may still be used in some legacy TETRA systems, there is a trend towards adopting stronger encryption methods like TEA2, TEA3, or TEA4 to ensure a higher level of security for TETRA communication, especially in critical applications like public safety and emergency services.

TETRA allows for two modes of air interface encryption.

1. Encryption Mode 1 (E1): In this mode, encryption is mandatory, meaning that all voice and data traffic is encrypted using TEA1. Users have no option to disable encryption, ensuring a basic level of security.
2. Encryption Mode 2 (E2): In this mode encryption is optional which means users can choose to enable or disable it. If the user disables encryption mode E2, then voice and data traffic will be sent on clear. If encryption mode E2 is enabled, then voice and data traffic is encrypted using TEA2 which provides enhanced security compared to TEA1.

Encryption keys are used to encrypt and decrypt voice and data transmissions, ensuring that unauthorized parties cannot eavesdrop on or tamper with the content of messages. The Key Management Facility (KMF) is the centralized entity responsible for generating, distributing and managing encryption keys. Encryption keys involved in TETRA communication are:

1. Traffic Encryption Keys (TEKs): TEKs are used for encrypting voice and data traffic over the air interface. Each individual or group of TETRA users has their own unique TEK. These keys are periodically rotated or changed to enhance security.
2. Key Encryption Keys (KEKs): KEKs are used to encrypt the TEKs themselves. This adds an extra layer of security. If an attacker needs to crack TEKs they would still need the KEKs to decrypt them. KEKs are typically stored securely within the TETRA devices.
3. Network Management Keys (NMKs): NMKs are used for secure communication between the TETRA devices and the Key Management Facility (KMF). They ensure the confidentiality of key management processes and key exchange.

TETRA uses authentication to ensure that only authorized users can access the network and participate in secure communications. Users must have valid authentication keys (usually stored in their radios) to establish a connection with the TETRA network.

TETRA also uses a technique called frequency hopping to further enhance security. Frequency hopping involves changing the frequency of the radio signal rapidly and randomly during transmission. This makes it difficult for an attacker to intercept and decode the signal, as they would need to know the exact frequency at each moment in time.

In addition to encryption, and frequency hopping, TETRA also supports access control. Access Control Mechanism is used to ensure that users only have access to the resources they are authorized to use while restricting others. These combined security measures make TETRA a robust choice for organizations that require secure and reliable communication systems, especially in critical situations where the confidentiality and integrity of data are paramount.