KY-57 (VINSON)

Voice encryption unit

The KY-57 was a wide-band voice encryption unit that was developed in the USA during the 1970s as a replacement of the NESTOR cryptographic products, such as the KY-38. It was suitable for use with a wide range of military radios and telehone lines. As part of the VINSON family of devices, it was the main crypto 'workhorse' of the US Army during the 1980s. Even today, many radios and voice encryption devices are still backwards compatible with the KY-57, that is also known as the **TSEC/KY-57**. The airborne version of the KY-57 is called the KY-58.

The KY-57 uses the GCHQ/NSA-developed Type-1 SAVILLE cryptographic algorithm. When used in combination with a radio transceiver, such as the SINCGARS non-ICOM RT-1439/VRC, the KY-57 allows signal fades or losses for up to 12 seconds without losing synchronization.

The KY-57 was eventually superceeded by the KY-99 that offered newer - more advanced - cryptographic algorithms, but that was still backwards compatible with the KY-57. Later SINCGARS ICOM radios, such as the RT-1523, had built-in KY-57 (VINSON) compatibility.

Both voice and data can be encrypted with the KY-57. Voice data is digitized using *Continuous Variable Slope Delta* modulation (CVSD), similar to other voice crypto systems of the same era, such as the Philips Spendex-10 , the Spendex 50 and the Telsy TS-500. Data from the CVSD modulator is mixed with data from a key stream generator that is seeded by a Traffic Encryption Key (TEK). The resulting digital data stream of 16 kbps requires a wide-band radio channel, making it unsuitable for use on HF radio frequencies. Rather than the standard 5 kHz (voice only) channel spacing, the KY-57 requires a 25 kHz channel, which is why it is VHF/UHF only.

The KY-57 was interoperable with the British BID/250 (Lamberton), that also uses the SAVILLE crypto algorithm. It was sometimes used in combination with HAVE QUICK frequency hopping. The KY-57 was produced until 1993, when it was replaced by more advanced encryption units such as the KY-99 and radios with integrated COMSEC [1] such as the modern SINCGARS radios.

Cryptographic Keys

The KY-57 has room for 6 front panel selected cryptographic keys. Keys 1 to 5 are the Traffic Encryption Keys (TEK). They are either loaded manually, using a key fill device such as the KYK-13 and the KOI-18, or by means of *Over The Air Rekeying* (OTAR). Key number 6 must always be loaded manually as it is the Key Encryption Key (KEK) that is used for OTAR.

When loading the keys manually, the MODE selector (S2) should be placed in the **LD**-position. When updating keys 1 to 5 remotely, S2 should be set to **RV** (Remote Variable).

Connections and controls

All controls of the KY-57 are on the front panel. The three major connectors are on the front panel as well. The only other connector is the power socket which is located at the rear panel. A detailed description of all connectors can be found on Brooke Clarke's website. A detailed description of the U-229 AUDIO/FILL sockets can be found here.

The following controls are available:

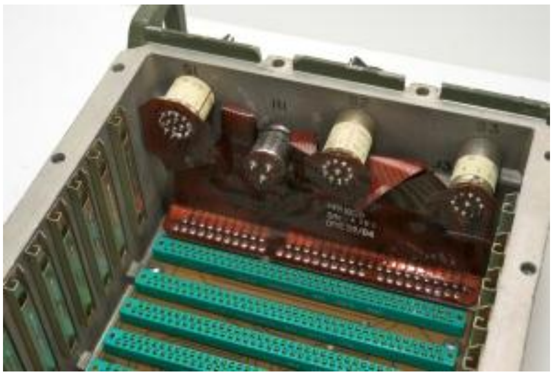
- **S1** - Operation (right)
  OFF: Power OFF
  ON: Power ON
  TD: Power ON with Time Delay enabled (needed for satellite use)
- **S2** - MODE (center)
  P: Plain voice (pull out knob first)
  C: Crypto
  LD: Load keys manually
  RV: Remote key loading (Remote Variable, OTAR)
- **S3** - Key (left)
  Z 1-5: ZEROIZE keys 1 to 5 (pull out the knob first)
  1-5: Selection of the Traffic Encryption Key (TEK)
  6: Select the Key Encryption Key (KEK) for OTAR-use
  Z ALL: ZEROIZE ALL keys (pull out the knob first)
- **R1** - Volume
  This is an analog control (potentiometer) that is used for controlling the audio volume of the unit. Turn right to raise the volume.

Connectors:

- **J1** - AUDIO (right)
  Standard U-229 6-pin socket for the connection of audio equipment such as a headset and/or microphone.
- **J2** - FILL (center)
  Standard U-229 6-pin socket for the connection of a US military DS-102 compatible key fill device such as the KYK-13.
- **J3** - RAD (left)
  19-pin connection to a suitable radio set, such as the PRC-77 UHF FM rig.
- **J4** - POWER (rear)
  Standard US military power connector. Used for the connection of a battery box or an external power adapter.

Demilitarized version

Although the KY-57 is a relatively old device, it is still very difficult - if not impossible - to find a complete and working unit. This is mainly due to the fact that some KY-57 units might still be in operation with the US military or their Allies. Furthermore, later cryptographic devices, such as the KY-99 and some SINCGARS radios, are often backwards compatible with the KY-57.



In the late 2000s however, demilitarized versions of the KY-57 sometimes showed up on auction sites such as Ebay. Although the internal electronics have all been removed from these devices, they are still cosmetically complete and do look nice in any cryptographic collection.

The image on the right shows an example of such a demilitarized KY-57 unit. All PCBs have been removed from their sockets and the flex wiring has been cut at various places. With some effort, it would be possible to convert the unit into a demonstrable *dummy*.