# Data encryption management

Even today, quite a high percentage of satellite traffic is unencrypted and therefore vulnerable to eavesdroppig and spoofing. CCSDS documentation strongly recommends implementing means to ensure the confidentiality of data. It is important to ensure the confidentiality of uplink commands as well as downlink channels transferring images
and other valuable and sensitive data. Also, it is important to encrypt data stored
in ground-station storages as well as payload data on satellites.

## How data encryption help:

In today's interconnected world, data confidentiality is vital in order to protect intellectual property and maintain technological superiority. For resilient data encryption, it is important to choose the right encryption algorithms for the right tasks.
For instance, different cryptographic methods are used for maintaining the confidentiality of data while other methods are suitable for ensuring integrity and authenticity.

## How it works:

CORAC KeyMaster API endpoints contain the capability to generate symmetric and asymmetric encryption keys as well as directly encrypt data anywhere on the ground station. Examples of encryption/decryption endpoints are as follows:

```
POST /encrypt/aes256
POST /decrypt/aes256
```

CORAC EPU, as a satellite HW crypto payload, completes CORAC KeyMaster in encrypting and decrypting protected data when received on a satellite