|  |  |
| --- | --- |
| **Server & Cloud Security**  Diploma in CSF/IT  Oct 2022 | Week 6 |
| Tutorial |
| **Cloud Data Security** | |

1. When a user requests to upload a file and store it as an encrypted object in an S3 bucket, Amazon S3 would request a data key from AWS KMS to use to encrypt the file. Briefly describe how a data key is created and shared with Amazon S3.

|  |
| --- |
| The data key is created in AWS KMS and it is shared when Amazon S3 requests to use the key to encrypt and decrypt data. |

1. Briefly explain TWO challenges of cloud encryption.

|  |
| --- |
| The encrypted data cannot be search or processed.  You do not manage and control the encrytion keys |

1. AWS Key Management Service (AWS KMS) uses Hardware Security Modules (HSMs) to protect users’ keys. Research and explain what is a hardware security module.

|  |
| --- |
| A HSM is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digtial signatures, strong authentication and other cryptographic functions.  HSMs may have features that provide tamper evidence such as visible signs of tampering or logging and alerting, or tamper resistance which makes tampering difficult without making the HSM inoperable, or tamper responsiveness such as deleting keys upon tamper detection.[[4]](https://en.wikipedia.org/wiki/Hardware_security_module#cite_note-4) Each module contains one or more [secure cryptoprocessor](https://en.wikipedia.org/wiki/Secure_cryptoprocessor) chips to prevent tampering and [bus probing](https://en.wikipedia.org/wiki/Bus_analyzer), or a combination of chips in a module that is protected by the tamper evident, tamper resistant, or tamper responsive packaging.  A vast majority of existing HSMs are designed mainly to manage secret keys. Many HSM systems have means to securely back up the keys they handle outside of the HSM. Keys may be backed up in wrapped form and stored on a [computer disk](https://en.wikipedia.org/wiki/Disk_storage) or other media, or externally using a secure portable device like a [smartcard](https://en.wikipedia.org/wiki/Smartcard) or some other [security token](https://en.wikipedia.org/wiki/Security_token).[[5]](https://en.wikipedia.org/wiki/Hardware_security_module#cite_note-5) |

- The End -