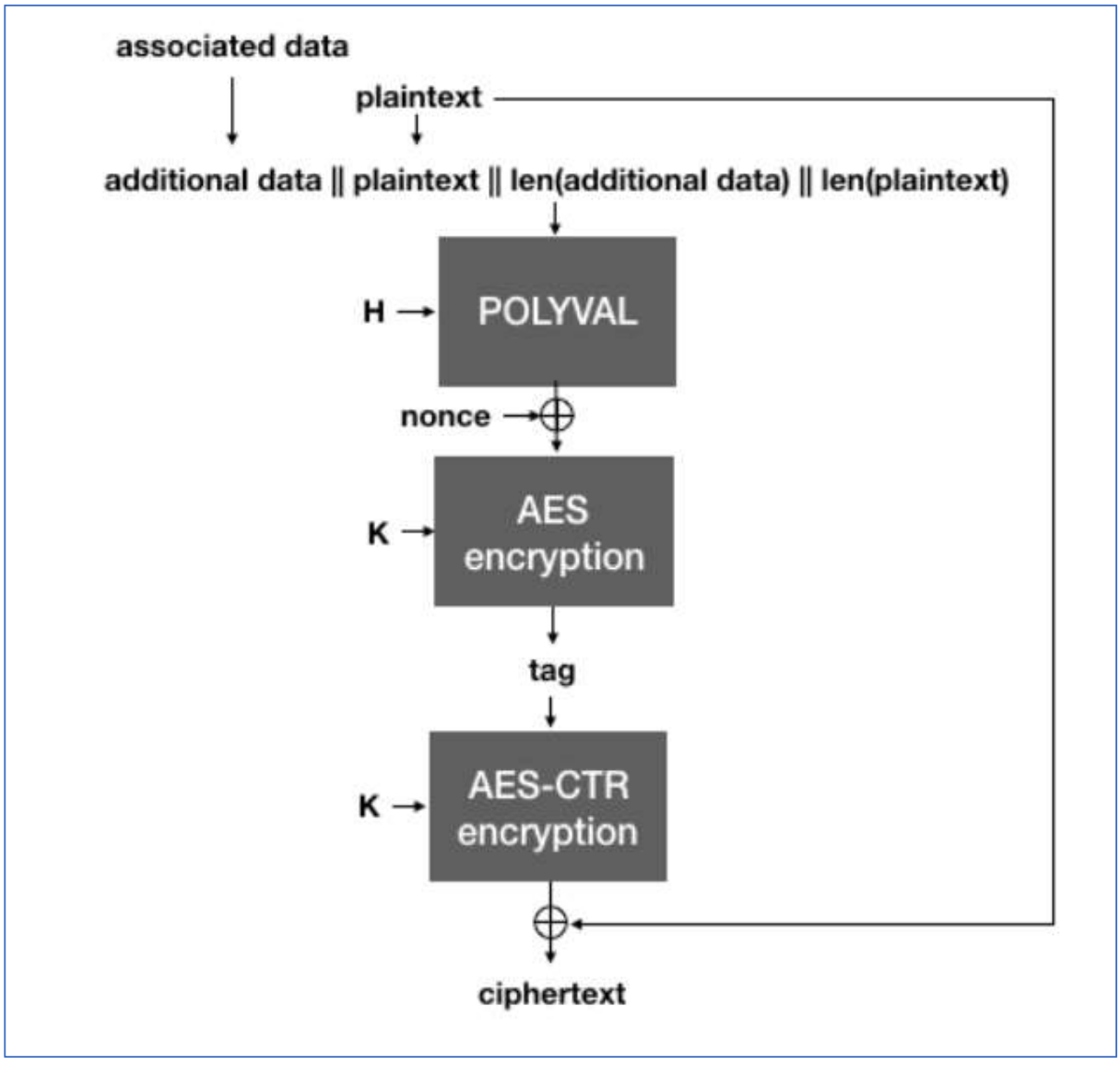
Answer the following questions in your e-portfolio:

- Why did you select the algorithm you chose?

  AES provides authenticated encryption (confidentiality and authentication) and can verify the integrity and authentication of additional authenticated data(AAD)sent in the clear. There are four inputs for authenticated encryption: the secret key, nonce(initialisation vector), plain text to be encrypted, and tag(additional authentication data for integrity check). AES-256 provides data protection for both data at rest and data in transit. It has the mathematical equivalent of 2^{256} keys possibilities.



- Would it meet the GDPR regulations? Justify your answer

Although the Regulation does not mandate or explicitly call for data security encryption**,** organisations must enforce the best security measures and safeguards. The Regulation recognises the risk exposure concerning the processing of personal data, and so it places the responsibility on the controller and the processor in Article. 32(1) to implement appropriate technical measures to secure personal data. The GDPR Regulation repeatedly mentions encryption and pseudonymisation as proper technical and organisational measures for GDPR data security.AES-256 ensures privacy by encrypting data and transforming it into ciphertext. The ciphertext hides the actual data from unauthorised access. The other functionality AES-256 provides is verifying the integrity of the secured data using a tag to authenticate the secured data.