[User Story would like to know the encryption/decryption process in AWS 1jc](https://github.com/kdanedesigns/kdpcapstone-AD440-2023-EasilySendDataSecurely/issues/24) issue #24

[**https://aws.amazon.com/blogs/security/how-to-protect-sensitive-data-for-its-entire-lifecycle-in-aws/**](https://aws.amazon.com/blogs/security/how-to-protect-sensitive-data-for-its-entire-lifecycle-in-aws/)

## Field-level encryption process

### Step 1 – RSA key generation and inclusion in Lambda@Edge

You need to extract the RSA public key from AWS KMS so you can include it in the [AWS Lambda deployment package](https://docs.aws.amazon.com/lambda/latest/dg/python-package.html). You can do this from the [AWS Management Console](http://aws.amazon.com/console), through the [AWS KMS SDK](https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html), or by using the [get-public-key](https://docs.aws.amazon.com/cli/latest/reference/kms/get-public-key.html) command in the [AWS Command Line Interface (AWS CLI)](http://aws.amazon.com/cli). Figure 5 shows **Copy** and **Download** options for a public key in the **Public key** tab of the AWS KMS console.

### Step 2 – HTTP API request handling by CloudFront

### Step 3 – Lambda@Edge processing

### Step 4 – Lambda@Edge response

### Step 5 – Forward the request to the origin server

## Field-level decryption process

### Step 1 – Application retrieves the field-level encrypted data

### Step 2 – Application invokes the decryption Lambda function

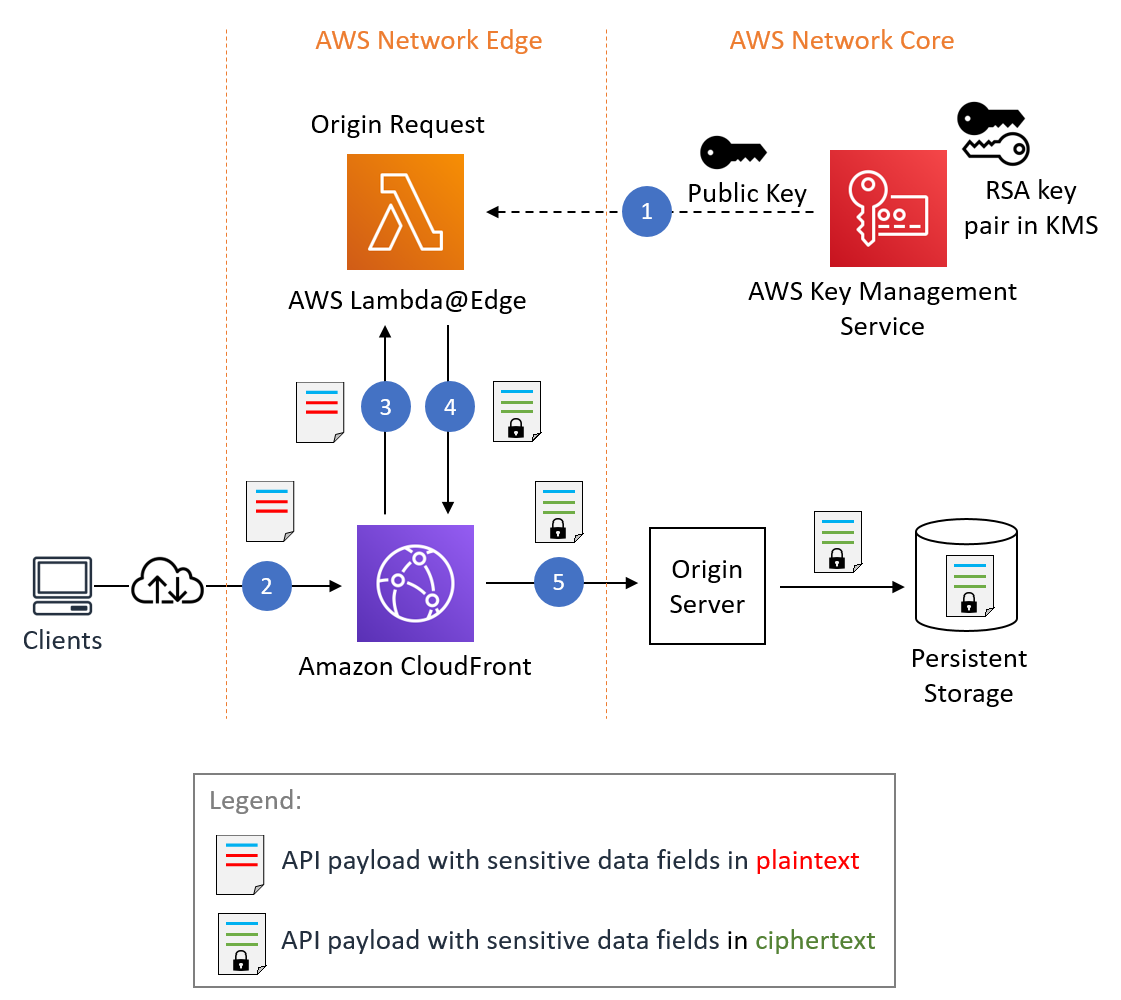
### Step 3 – Lambda calls the AWS KMS decryption API

### Step 4 – AWS KMS decrypts ciphertext and returns plaintext

### Step 5 – Lambda returns decrypted data body

## Field-level encryption process

Let’s discuss the individual steps involved in the encryption process as shown in Figure 2.



**Field-level decryption process**

An application that’s authorized to access sensitive data for a business function can decrypt that data. An example decryption process is shown in Figure 6. The figure shows a Lambda function as an example compute environment for invoking AWS KMS for decryption. This functionality isn’t dependent on Lambda and can be performed in any compute environment that has access to AWS KMS.

