# Decryption and Download

CHINMAY GIREESH G S
TCR17CS022

# Receiving parameters from getfile.php

1.Filename

2.corresponding key

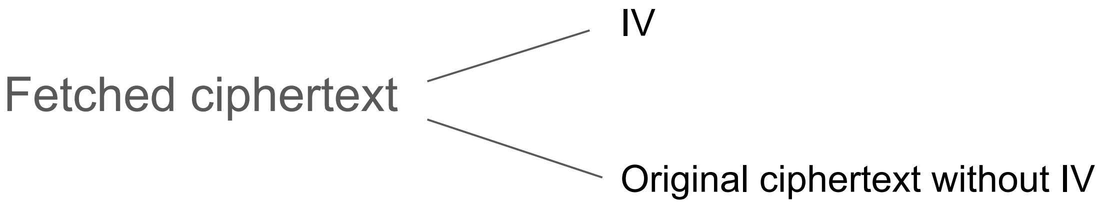
## Code part

```
$key=$_POST['key'];
$filename2="encrypted/".$_POST['file'];
```

# Ciphertext formating

1.Fetching corresponding ciphertext of given file name

2.



Fetched ciphertext

IV

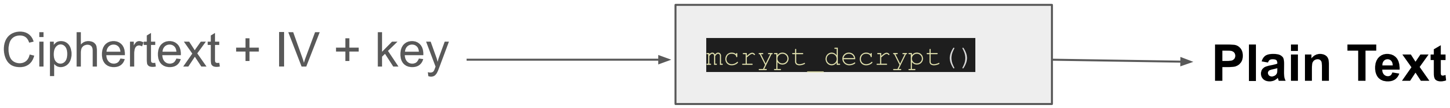
Original ciphertext without IV

Code part

```
# retrieves the IV, iv_size should be created using mcrypt_get_iv_size()
  $iv_dec = substr($ciphertext_dec, 0, $iv_size);

  # retrieves the cipher text (everything except the $iv_size in the front)
  $ciphertext_dec = substr($ciphertext_dec, $iv_size);
```

# Decryption



Ciphertext + IV + key

`mcrypt_decrypt()`

**Plain Text**

## Code part

```
 $plaintext_dec = mcrypt_decrypt(MCRYPT_RIJNDAEL_128, $key,
 $ciphertext_dec, MCRYPT_MODE_CBC, $iv_dec);
```

# Final step

1.Decrypted file is saved in corresponding file name

2.Saved file is ready for download

## Code part

```
$myFile = "decrypted/$filename";
$fh = fopen($myFile, 'w') or die("can't open file");
fwrite($fh, $plaintext_dec );
fclose($fh);
```

# Features to be implemented

1.Detailed Database

2.Third party access request and permission granting for file Access