main.c

Run

Output

Clear

```c
1  #include <stdio.h>
2  #include <string.h>
3  #include <openssl/aes.h>
4  #include <openssl/rand.h>
5
6  #define BLOCK_SIZE 16
7
8  void pad_data(const unsigned char *input, int
       input_len, unsigned char *output, int
       *padded_len) {
9      int pad_len = BLOCK_SIZE - (input_len %
           BLOCK_SIZE);
10     if (pad_len == 0) pad_len = BLOCK_SIZE;  //
           Always pad
11     memcpy(output, input, input_len);
12     output[input_len] = 0x80;  // 1 bit
13     memset(output + input_len + 1, 0x00,
           pad_len - 1);
```

```
/tmp/91GpcOYXVZ/main.c: In function 'ecb_encrypt':
/tmp/91GpcOYXVZ/main.c:19:5: warning:
    'AES_set_encrypt_key' is deprecated: Since OpenSSL
  3.0 [-Wdeprecated-declarations]
  19 |     AES_set_encrypt_key(key, 128, &aes_key);
     |     ^~~~~~~~~~~~~~~~~~~
In file included from /tmp/91GpcOYXVZ/main.c:3:
/usr/include/openssl/aes.h:51:5: note: declared here
  51 | int AES_set_encrypt_key(const unsigned char
       *userKey, const int bits,
     |     ^~~~~~~~~~~~~~~~~~~
/tmp/91GpcOYXVZ/main.c:21:9: warning:
    'AES_ecb_encrypt' is deprecated: Since OpenSSL 3.0
    [-Wdeprecated-declarations]
  21 |         AES_ecb_encrypt(plaintext + i,
       ciphertext + i, &aes_key, AES_ENCRYPT);
     |         ^~~~~~~~~~~~~~~
/usr/include/openssl/aes.h:63:6: note: declared here
```

main.c   Run   Output   Clear

```c
                     padded_len);
 96    cbc_decrypt(key, iv, ciphertext, padded_len
          , decrypted);
 97    print_hex("CBC Decrypted ", decrypted,
          padded_len);
 98
 99    // CFB
100    cfb_encrypt(key, iv, padded, padded_len,
          ciphertext);
101    print_hex("CFB Ciphertext", ciphertext,
          padded_len);
102    cfb_decrypt(key, iv, ciphertext, padded_len
          , decrypted);
103    print_hex("CFB Decrypted ", decrypted,
          padded_len);
104
105    return 0;
106  }
```

```
/tmp/91GpcOYXVZ/main.c: In function 'ecb_encrypt':
/tmp/91GpcOYXVZ/main.c:19:5: warning:
    'AES_set_encrypt_key' is deprecated: Since OpenSSL
    3.0 [-Wdeprecated-declarations]
   19 |      AES_set_encrypt_key(key, 128, &aes_key);
      |      ^~~~~~~~~~~~~~~~~~~
In file included from /tmp/91GpcOYXVZ/main.c:3:
/usr/include/openssl/aes.h:51:5: note: declared here
   51 | int AES_set_encrypt_key(const unsigned char
        *userKey, const int bits,
      |      ^~~~~~~~~~~~~~~~~~~
/tmp/91GpcOYXVZ/main.c:21:9: warning:
    'AES_ecb_encrypt' is deprecated: Since OpenSSL 3.0
    [-Wdeprecated-declarations]
   21 |        AES_ecb_encrypt(plaintext + i,
        ciphertext + i, &aes_key, AES_ENCRYPT);
      |        ^~~~~~~~~~~~~~~
/usr/include/openssl/aes.h:63:6: note: declared here
```