An example Crypto API   (OpenSSL)

```
void AES_cbc_encrypt(
          const unsigned char *in,
          unsigned char *out,
          size_t length,
          const AES_KEY *key,
          unsigned char *ivec,          ←   user supplies IV
          AES_ENCRYPT or AES_DECRYPT);
```

otherwise, no
CPA security

When nonce is non random need to encrypt it before use