

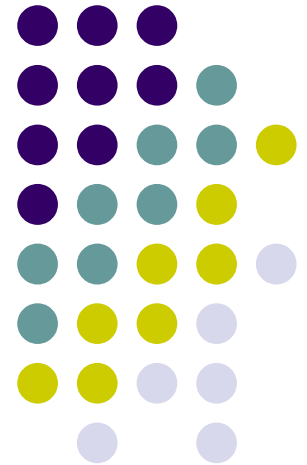
# Crypto libraries

## OpenSSL (cont.)

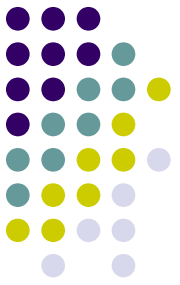
---

**Milan Brož**  
xbroz@fi.muni.cz

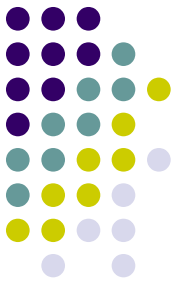
PV181, FI MUNI, Brno



# OpenSSL – [www.openssl.org](http://www.openssl.org)



- opensource cryptography toolkit
- Apache-style license
- hash, symmetric/asymmetric encryption, PKI, CA, ...
- ASN.1, PKCS-5,7,8,12, X509, OCSP, PEM
- SSL and TLS
- command line tool
- C/C++ library bindings (+many other library wrappers)
  - on Linux compile with **-lcrypto -lssl**
  - `#include <openssl/...>`

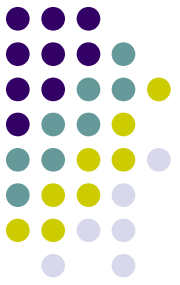


# Today's goals

- **Symmetric encryption**
- **Encryption modes**  
ECB, CBC, CTR, XTS  
IV – initialization vector, tweak
- **Authenticated encryption**  
AEAD – authenticated encryption with associated data  
GCM example
- **Demonstration of failures/mistakes**  
ECB use, CBC mangled IV, CBC mangled ciphertext,  
CTR reuse, XTS patterns, AEAD auth tag and AD

# Example 4:

# Symmetric encryption



## OpenSSL (1.1.x)

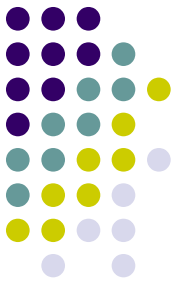
Encryption with EVP interface. Cipher mode is for example **EVP\_aes\_256\_cbc()**.

```
EVP_CIPHER_CTX_new()  
EVP_EncryptInit_ex(context, EVP_cipher_mode,  
                    NULL/*engine*/, key, iv)  
EVP_EncryptUpdate(context, ciphertext, &clen, plaintext, plen)  
EVP_EncryptFinal_ex(context, ciphertext + clen, &len)  
EVP_CIPHER_CTX_free(context)
```

See *4\_encryption\_openssl* directory.

# Example 5:

## Symmetric encryption (AEAD)



### OpenSSL (3.0.x)

(Authenticated) encryption with EVP interface. Cipher mode is for example **"AES-256-GCM"**.

```
EVP_CIPHER_fetch(NULL/*lib*/, "AES-256-GCM", NULL/*props*/)
EVP_CIPHER_CTX_new()
EVP_EncryptInit_ex2(context, EVP_cipher, key, iv, PARAMS[])
EVP_EncryptUpdate(context, ciphertext, &clen, plaintext, plen)
EVP_EncryptFinal_ex(context, ciphertext + clen, &len)

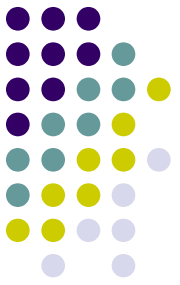
/* OSSL_CIPHER_PARAM_AEAD_TAG access */
EVP_CIPHER_CTX_get/set_params(ctx, PARAMS[]))

EVP_CIPHER_CTX_free(context)
EVP_CIPHER_free(EVP_cipher)
```

See *[4\\_encryption\\_aead\\_openssl3](#)* directory.

# Encryption modes

## common mistakes or failures

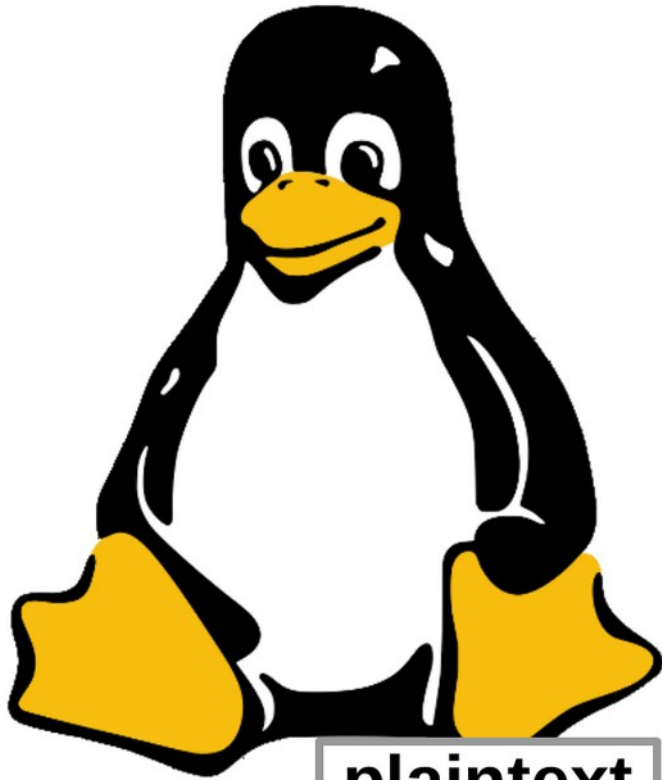
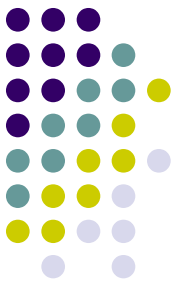


See `6_encryption_fails_openssl` example in git.

Comment out various sections a play with demos.

- Example 1: **ECB patterns**
- Example 2a: **CBC IV bit flips**
- Example 2b: **CBC bit flips in a consecutive block**
- Example 3: **XTS constant IV block patterns**
- Example 4: **CTR key stream recovery from a plain/ciphertext pair**
- Example 5: **GCM authenticated encryption and auth.tags**

# Symmetric encryption: ciphertext



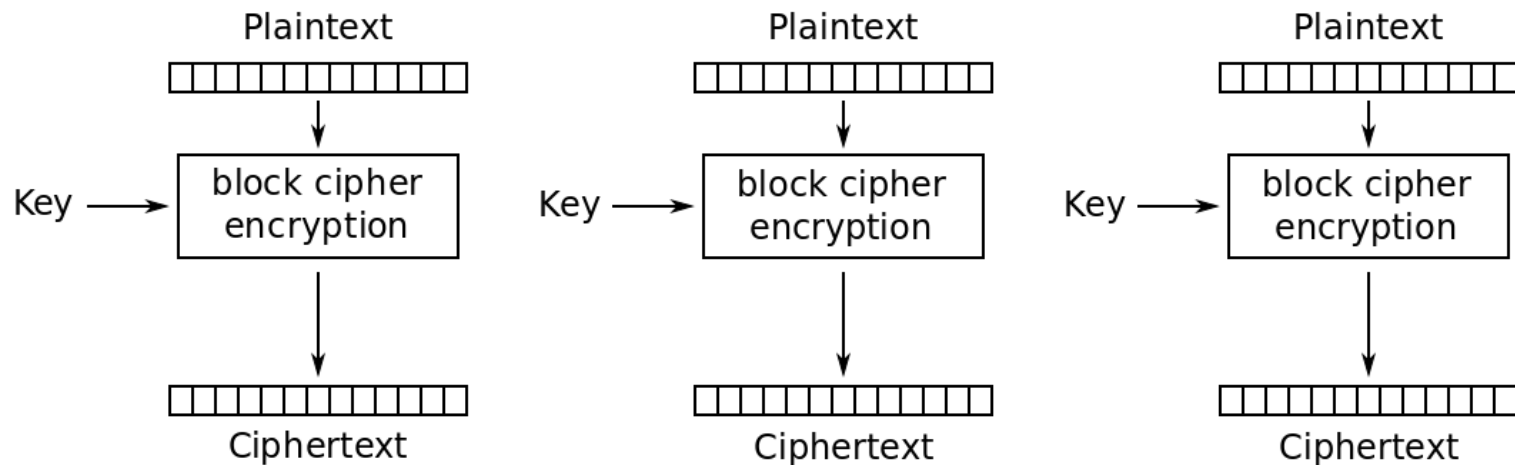
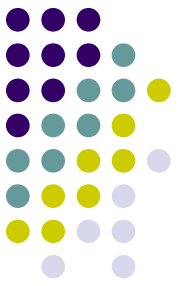
plaintext



ciphertext

# ECB mode

## ...should be never used



Electronic Codebook (ECB) mode encryption

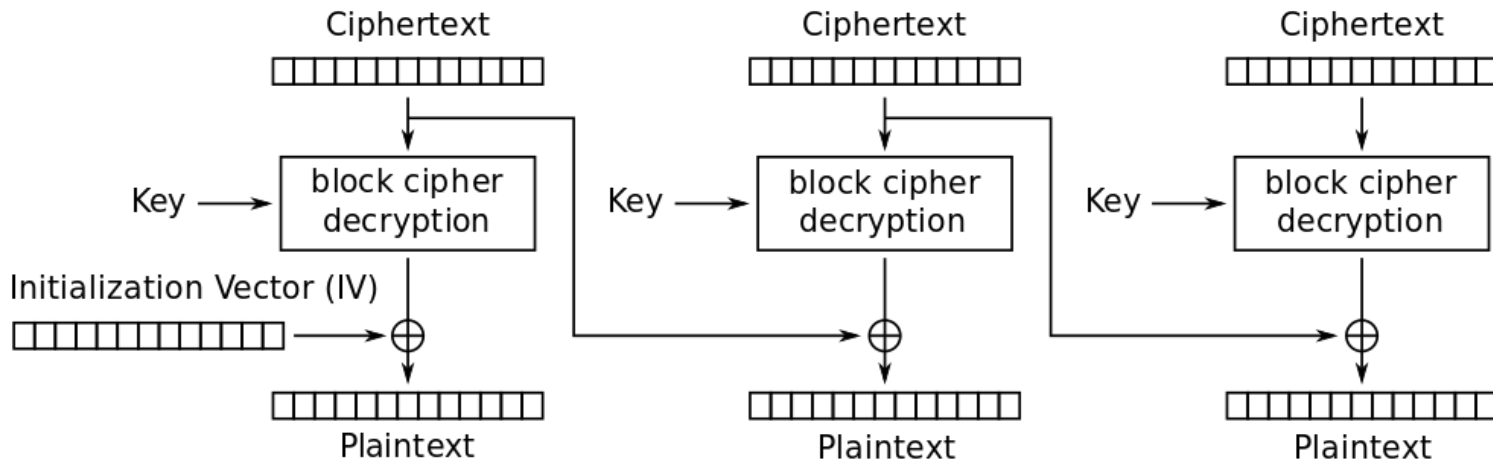
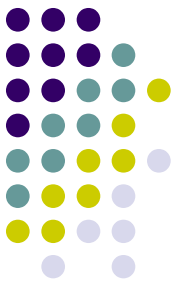
*Wrong use demo: ciphertext patterns, block relocation.*

*See **6\_encryption\_fails\_openssl** directory.*

*picture: Wikipedia*



# CBC mode

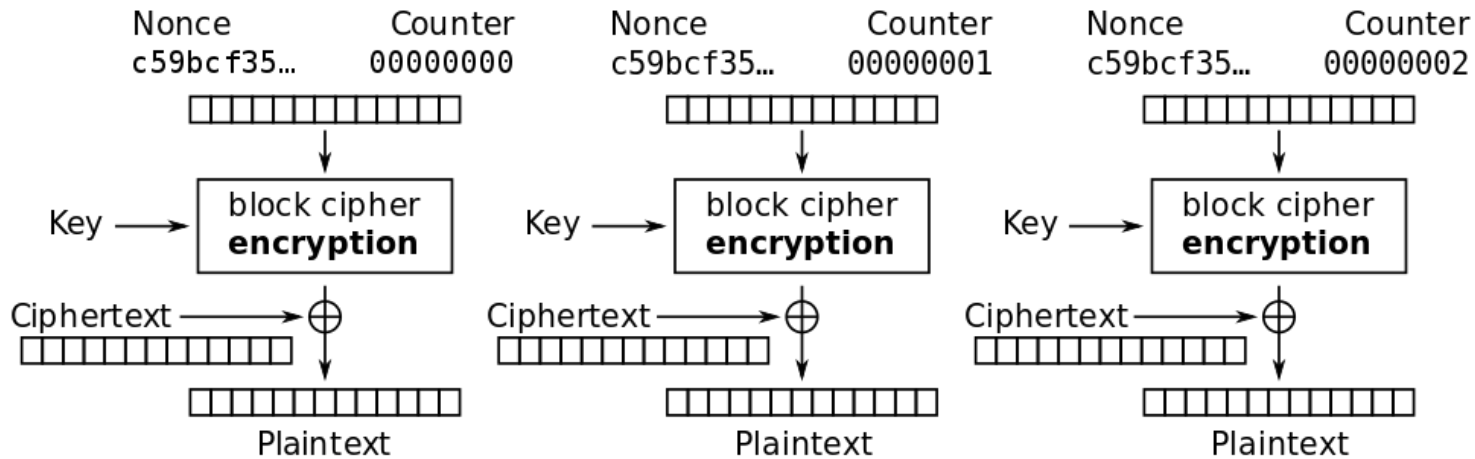
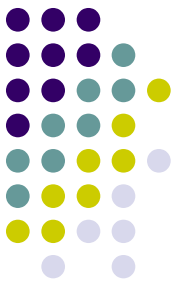


Cipher Block Chaining (CBC) mode decryption

*Wrong use demo: first block bit flips (IV) and consecutive block change.  
See [6\\_encryption\\_fails\\_openssl](#) directory.*

*picture: Wikipedia*

# CTR mode (counter mode)



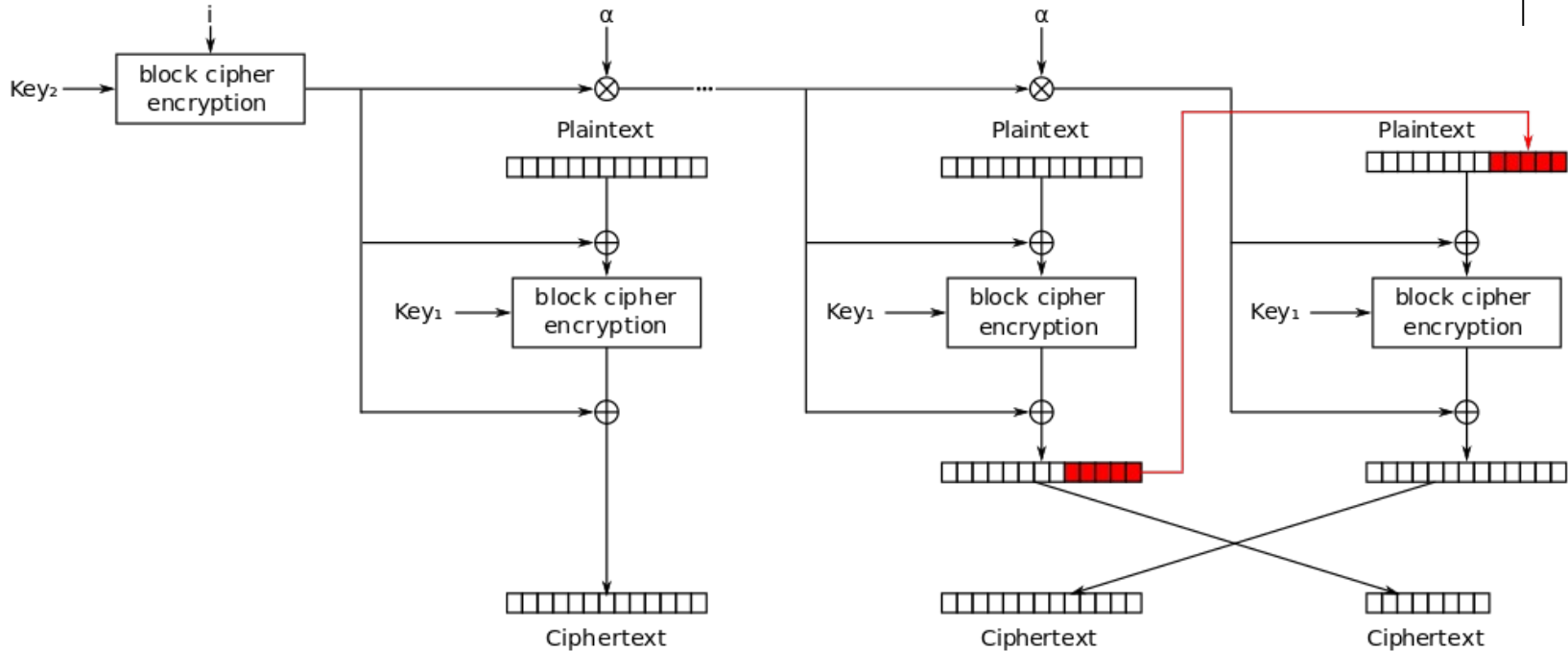
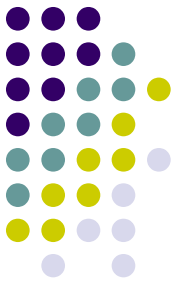
Counter (CTR) mode decryption

*Wrong use demo: re-use key from known ciphertext/plaintext pair.*

*See **6\_encryption\_fails\_openssl** directory.*

*picture: Wikipedia*

# XTS mode storage (file, disk) encryption



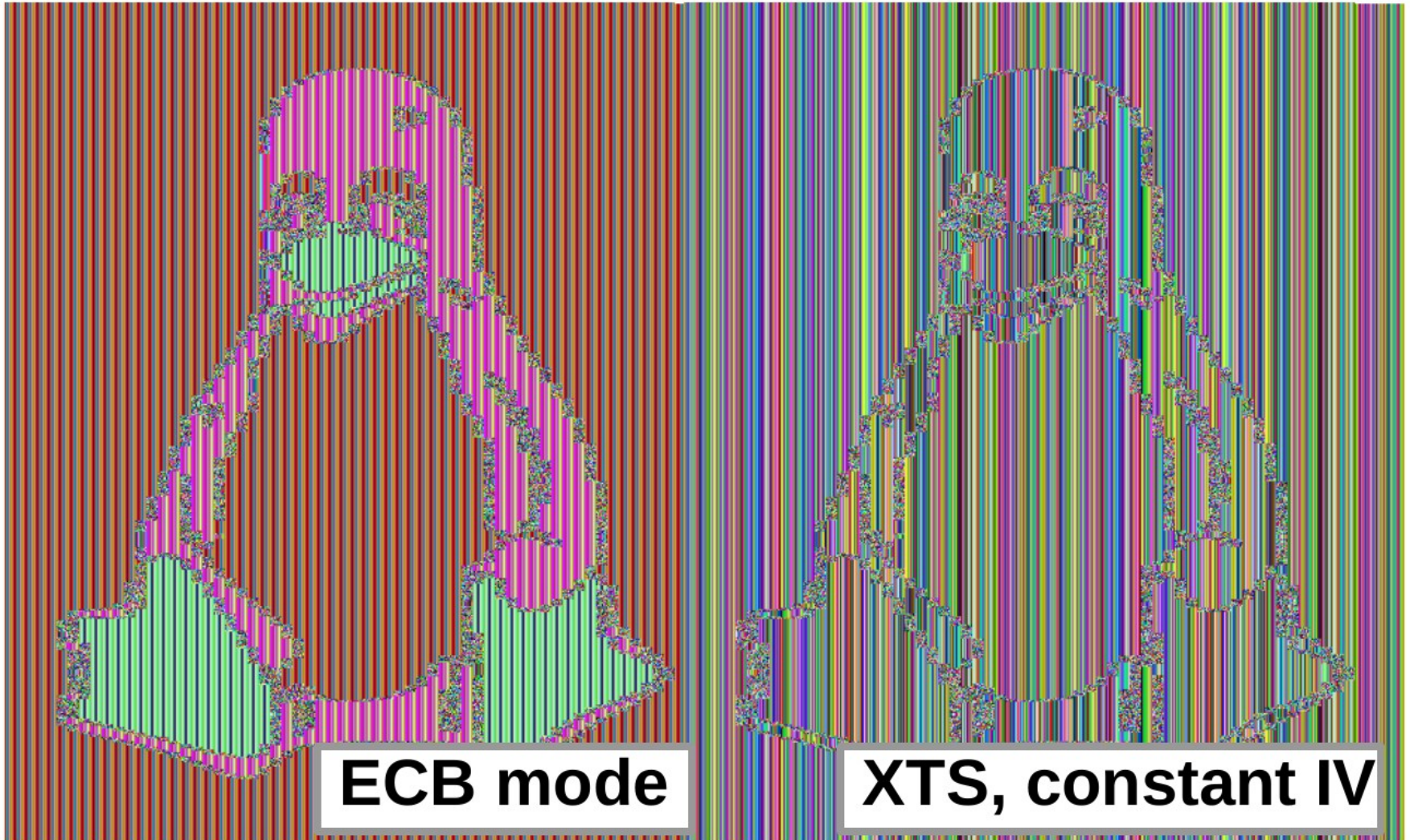
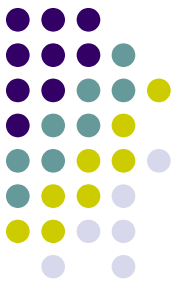
XEX with tweak and ciphertext stealing (XTS) mode encryption

*Wrong use demo: block patterns with constant IV.*

*See [6\\_encryption\\_fails\\_openssl](#) directory.*

*picture: Wikipedia*

# Symmetric encryption fails: patterns in ciphertext



**ECB mode**

**XTS, constant IV**

# No integrity protection... (no authentication of data)

