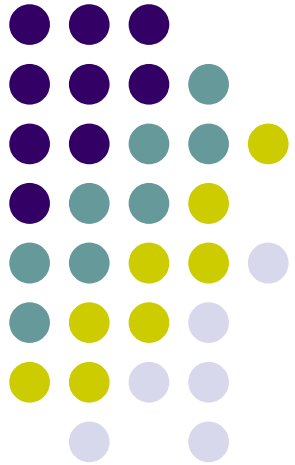
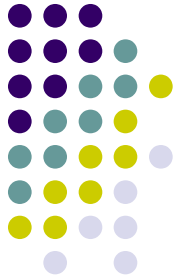
Crypto libraries OpenSSL (cont.)

Milan Brož
xbroz@fi.muni.cz

PV181, FI MUNI, Brno

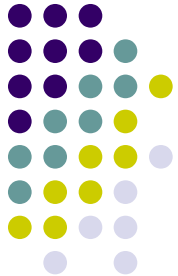


OpenSSL – www.openssl.org



- opensource cryptography toolkit
- OpenSSL3 ~ released 2021, many API improvements
- Apache-style license
- hash, symmetric/asymmetric encryption, PKI, CA, ...
- ASN.1, PKCS-5,7,8,12, X509, OCSP, PEM, SSL, 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, 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, key, iv)
EVP_EncryptUpdate(context, ciphertext, &clen, plaintext, plen)
EVP_EncryptFinal_ex(context, ciphertext + clen, &len)
EVP_CIPHER_CTX_free(context)
```

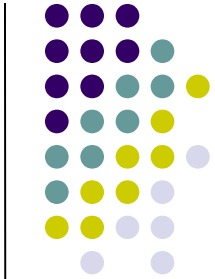
OpenSSL (3.0.x)

Encryption with EVP interface. Cipher mode is for example **”AES-256-CBC”.**

```
cipher = EVP_CIPHER_fetch(cipher_mode, ...)
EVP_CIPHER_CTX_new()
EVP_EncryptInit_ex2(context, cipher, key, iv, PARAMS)
EVP_EncryptUpdate(context, ciphertext, &clen, plaintext, plen)
EVP_EncryptFinal_ex(context, ciphertext + clen, &len)
EVP_CIPHER_CTX_free(context)
EVP_CIPHER_free(cipher)
```

*See **4_encryption_openssl, 4_encryption_openssl3** directory.*

Example 5: AEAD Authenticated encryption



OpenSSL (3.0.x)

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

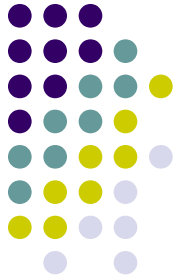
```
EVP_CIPHER_fetch(NULL/*lib*/, "AES-256-GCM", NULL/*props*/)
EVP_CIPHER_CTX_new()
EVP_EncryptInit_ex2(context, EVP_cipher, key, iv, PARAMS[])
EVP_EncryptUpdate(context, ciphertext, &clen, plaintext, plen)
EVP_EncryptFinal_ex(context, ciphertext + clen, &len)

/* 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

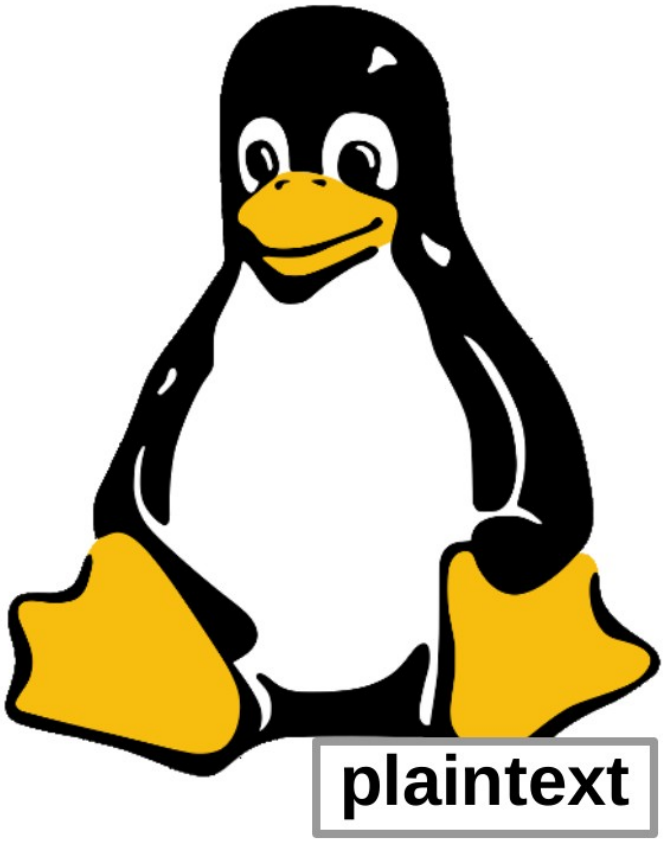


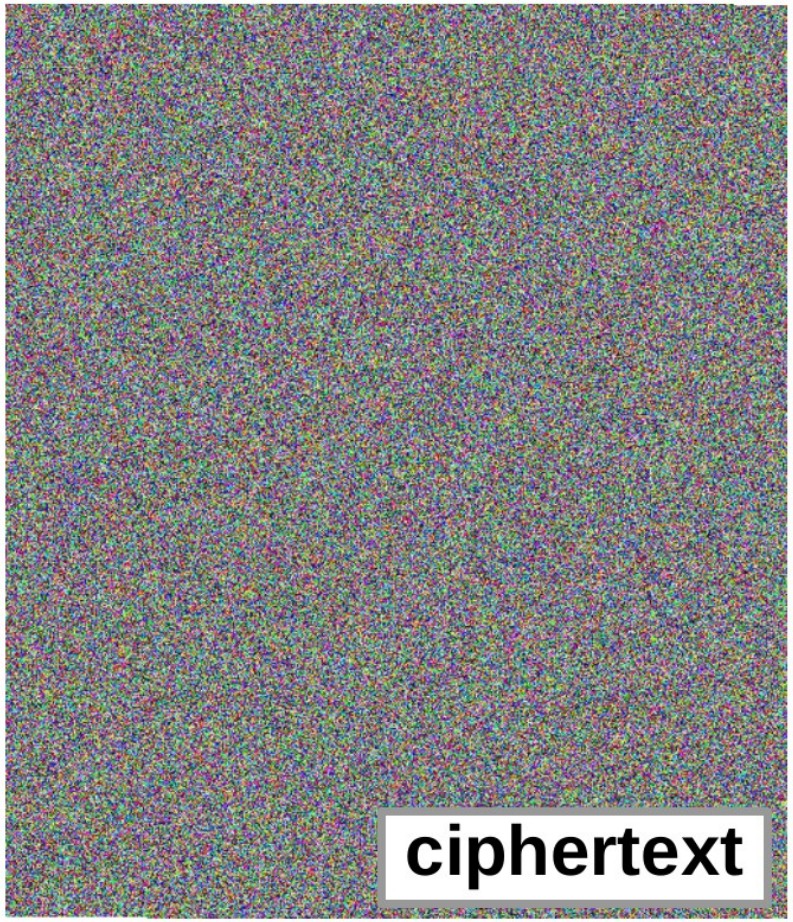
See **6_encryption_fails_openssl** example in git.

Comment out various sections a play with demos.

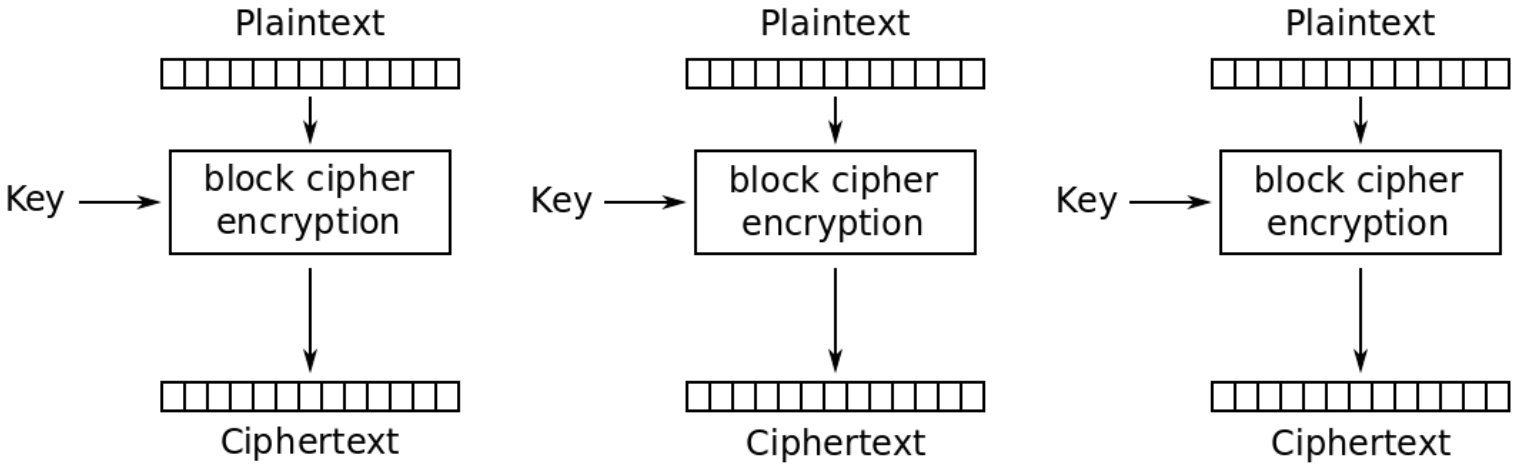
- Example 1: **ECB patterns**
- Example 2a: **CBC IV bit flips**
- Example 2b: **CBC bit flips in a consecutive block**
- Example 3: **XTS constant IV block patterns**
- Example 4: **GCM authenticated encryption and auth.tags**

Symmetric encryption: ciphertext





ECB mode
…should be never used



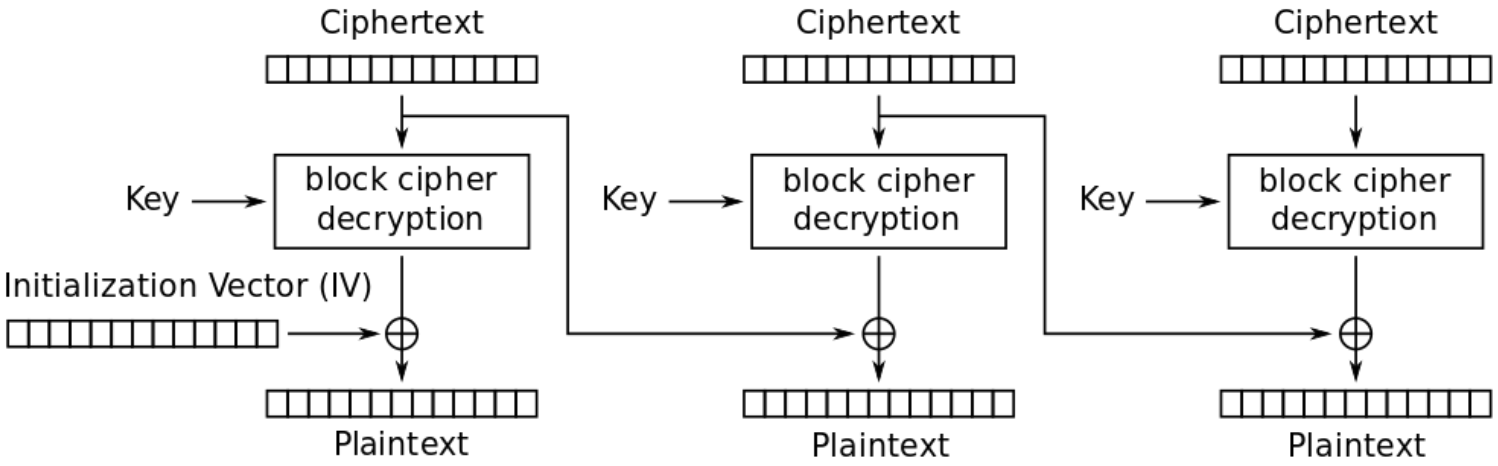
Electronic Codebook (ECB) mode encryption

Wrong use demo: ciphertext patterns, block relocation.

*See **6_encryption_fails_openssl** directory.*

picture: Wikipedia

CBC mode



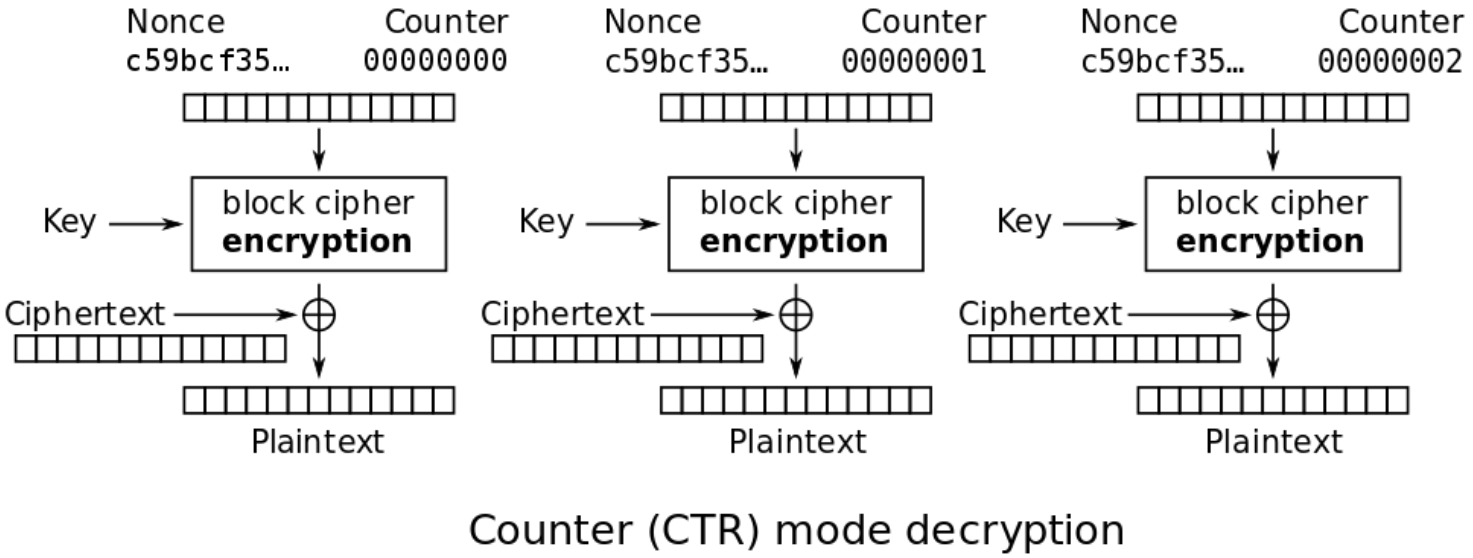
Cipher Block Chaining (CBC) mode decryption

Wrong use demo: first block bit flips (IV) and consecutive block change.

*See **6_encryption_fails_openssl** directory.*

picture: Wikipedia

CTR (counter) mode (optional example)



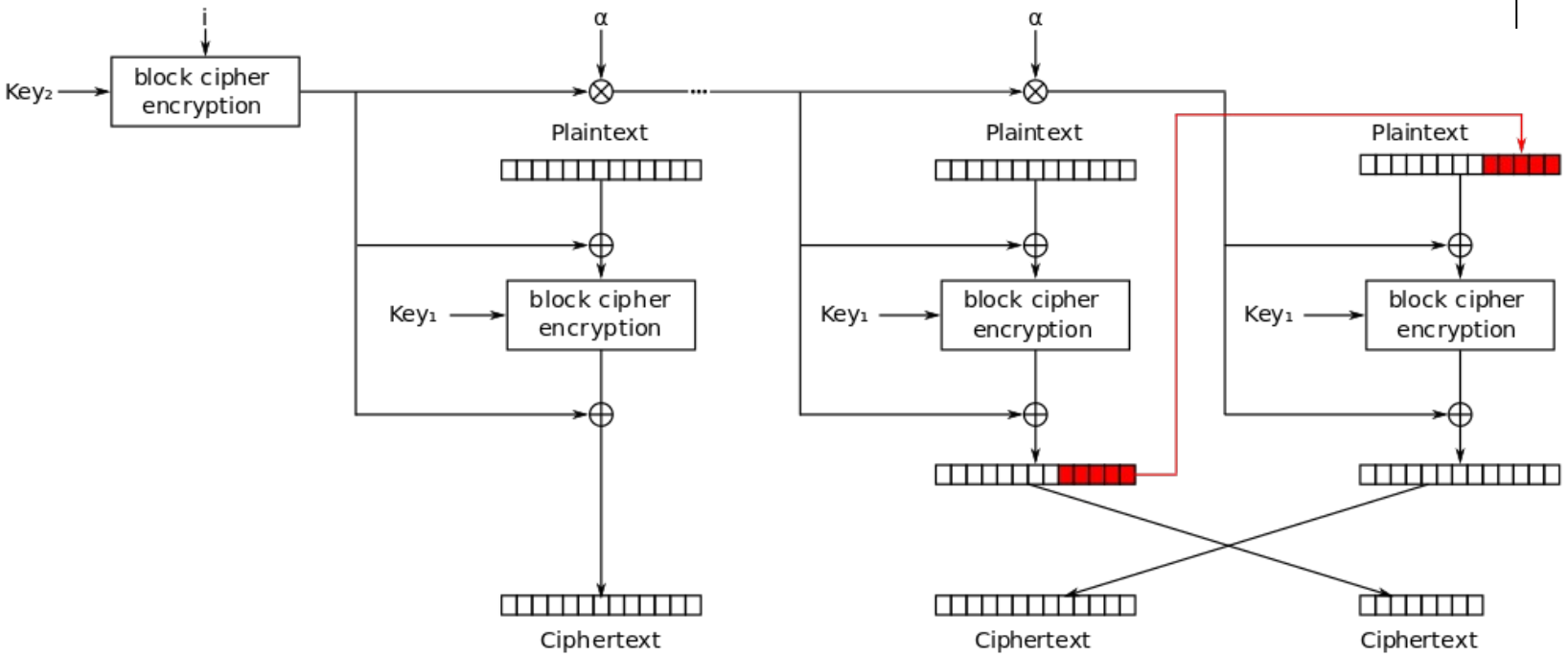
Counter (CTR) mode decryption

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



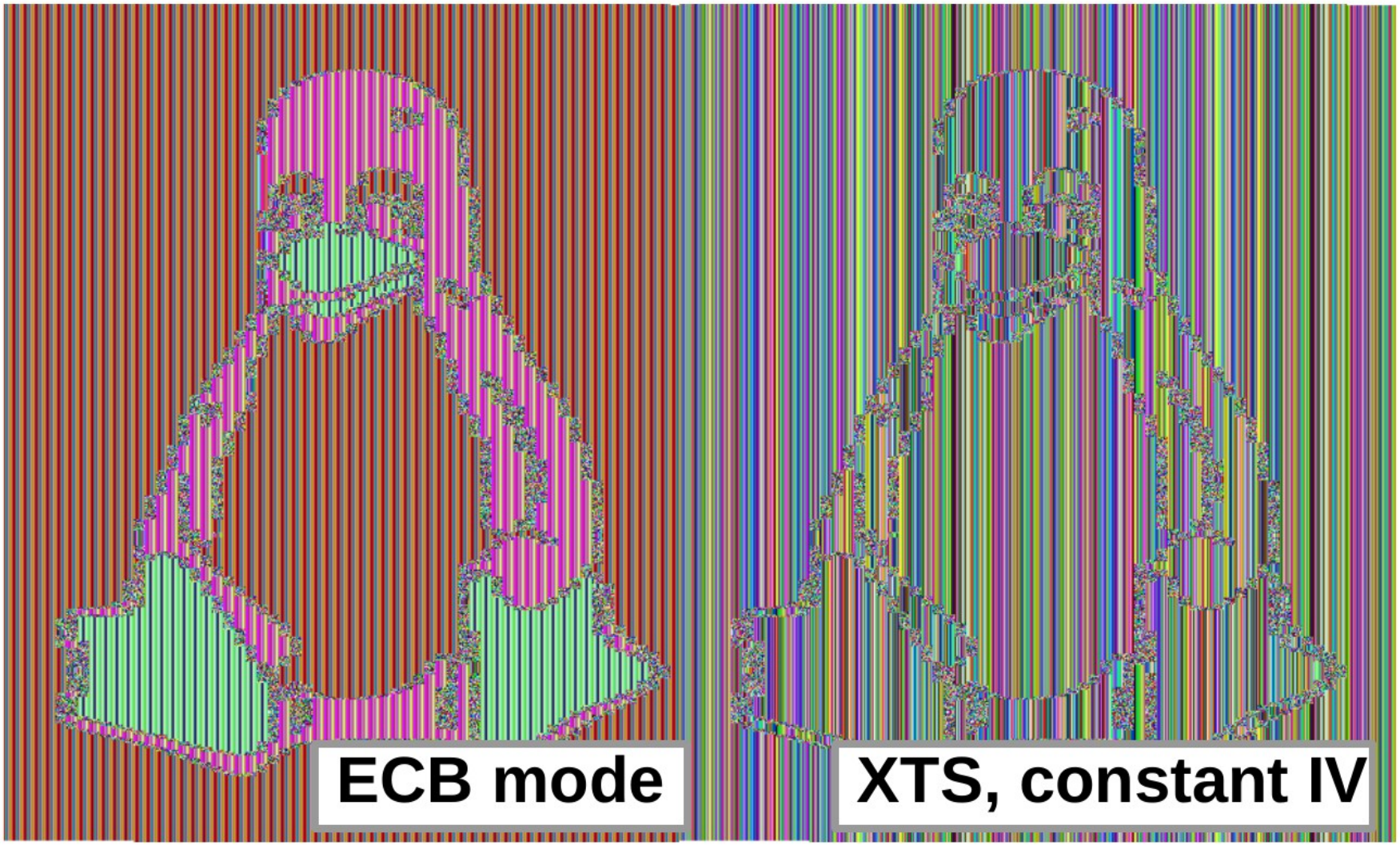
XEX with tweak and ciphertext stealing (XTS) mode encryption

Wrong use demo: block patterns with constant IV.

*See **6_encryption_fails_openssl** directory.*

picture: Wikipedia

Symmetric encryption fails: patterns in ciphertext



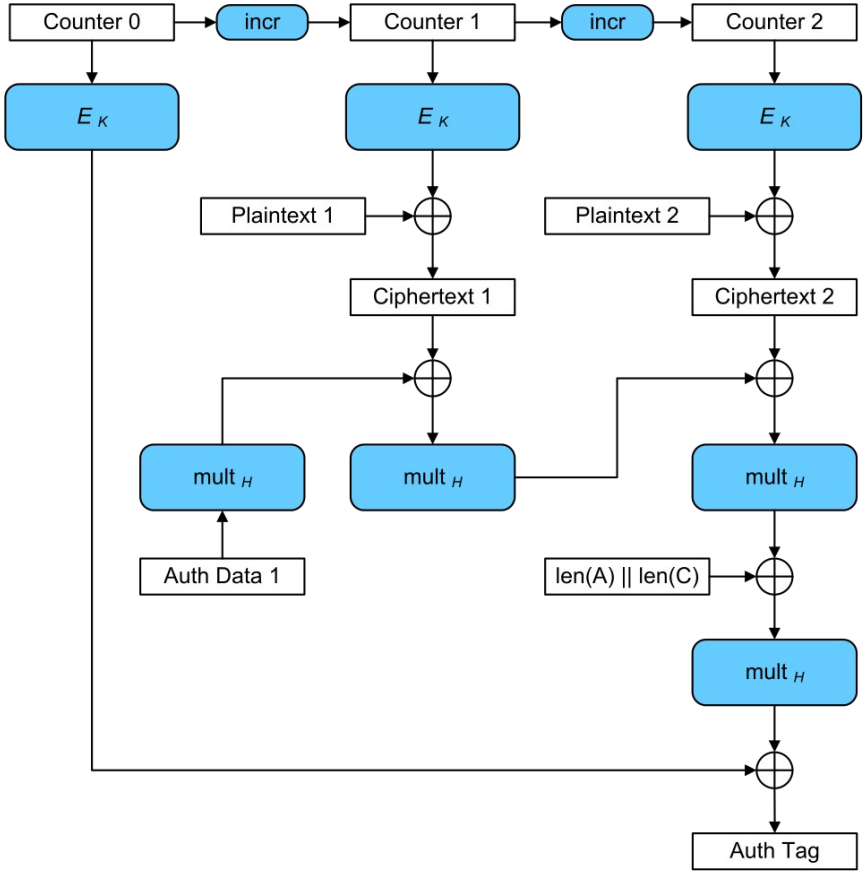
Why AEAD
integrity protection for data

Authenticated mode
GCM - Galois/Counter Mode

Authenticated Encryption with Additional Data (AEAD):

confidentiality + integrity.

- *additional auth. data (AAD)*
- *data (plaintext/ciphertext)*
- *authentication tag*



*See **6_encryption_fails_openssl** directory.*

picture: Wikipedia