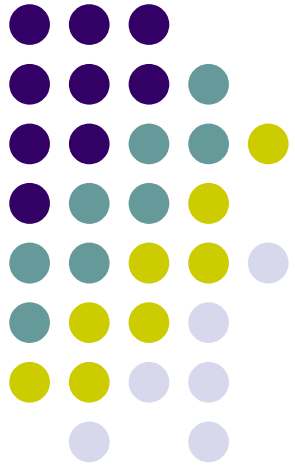
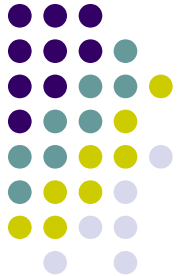
Crypto libraries OpenSSL (cont.)

Milan Brož
xbroz@fi.muni.cz

PV181, FI MUNI, Brno

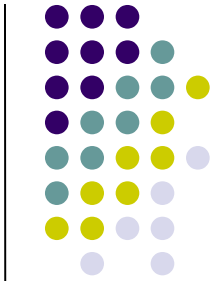


OpenSSL – www.openssl.org



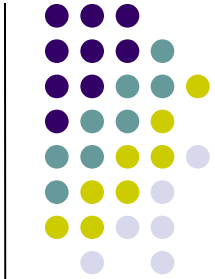
- opensource cryptography toolkit
- Apache-style license
- hash, symmetric/asymmetric encryption, PKI, CA, ...
- ASN.1, PKCS-5,7,8,12, X509, OCSP, PEM
- SSL and TLS
- command line tool
- C/C++ library bindings (+many other library wrappers)
  - on Linux compile with **-lcrypto –lssl**
  - #include <openssl/...>

Today’s goals



- Symmetric Encryption
- Demonstration of failures in some modes
- BIO (I/O abstraction)

Example 4: Symmetric encryption



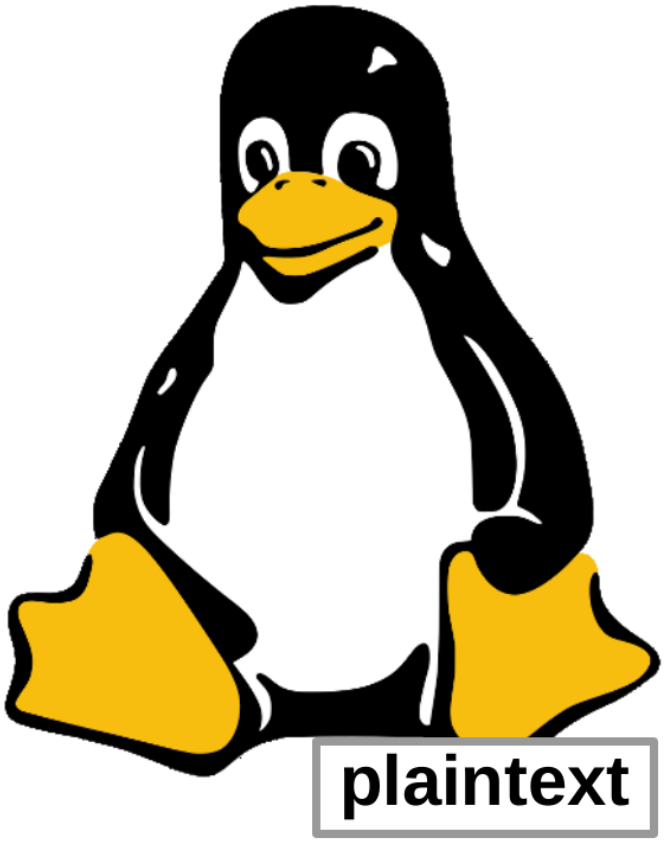
OpenSSL

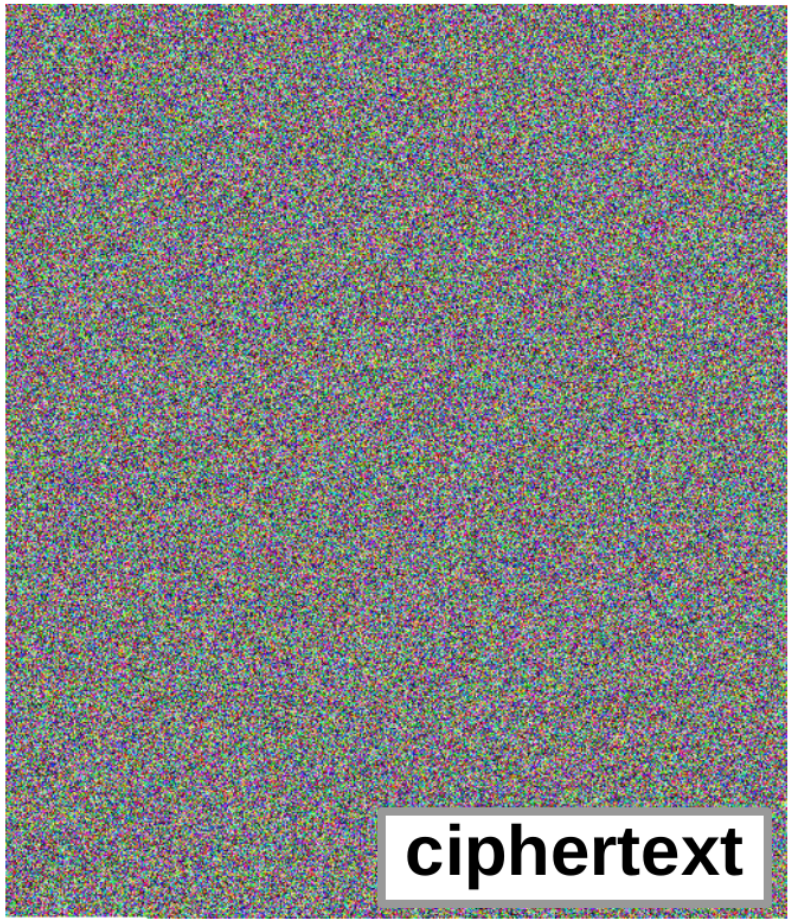
Encryption with EVP interface. Cipher mode is for example **EVP_aes_256_cbc().**

```
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)
```

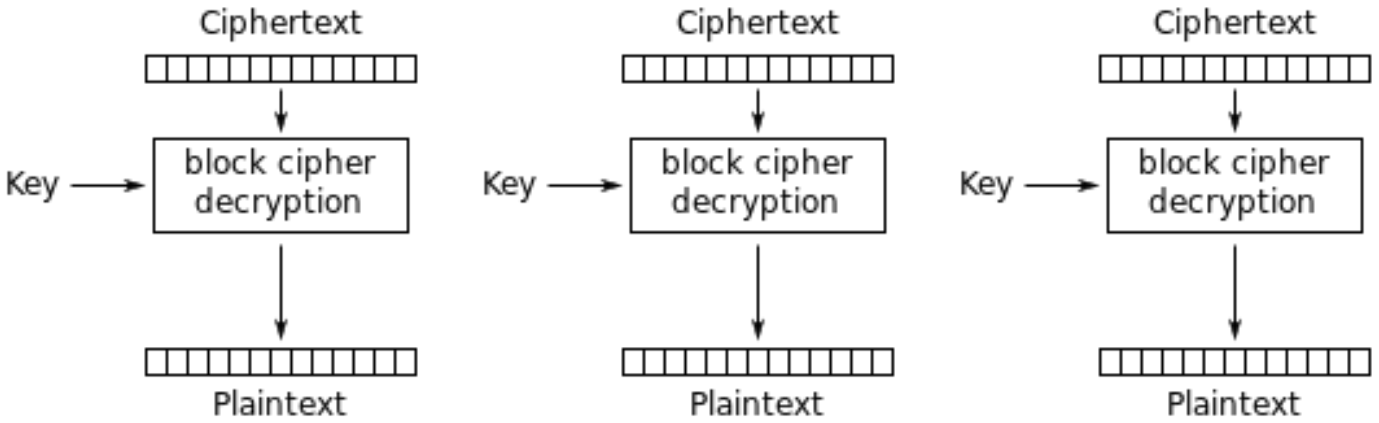
*See **4_encryption_openssl** directory.*

Symmetric encryption: ciphertext





ECB mode
…should be never used



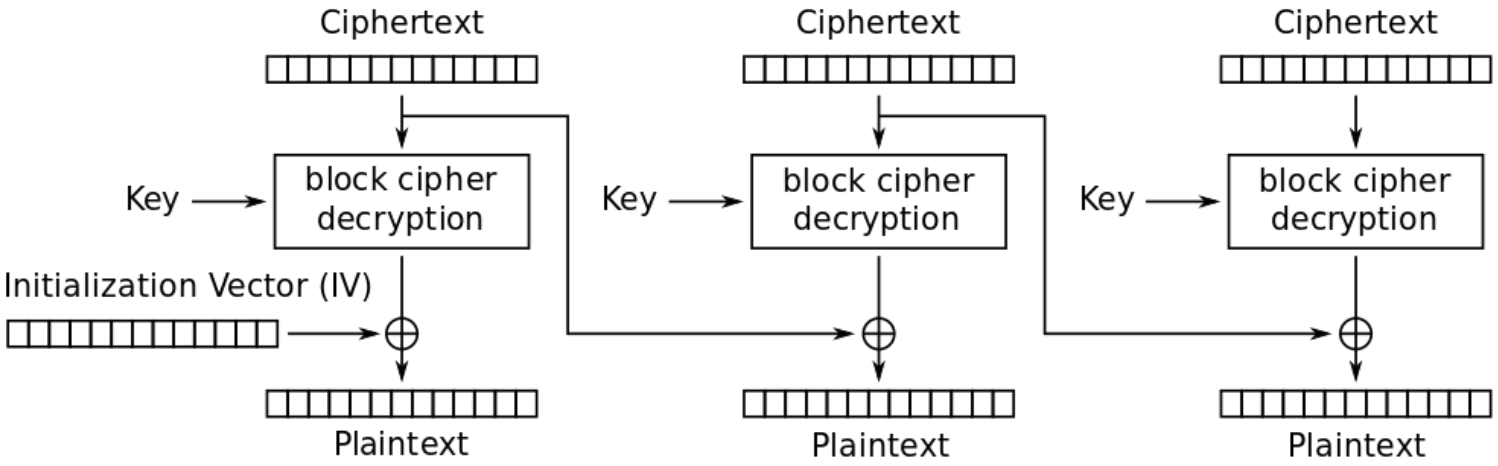
Electronic Codebook (ECB) mode decryption

Wrong use demo: ciphertext patterns, block relocation.

*See **4a_encryption_fails_openssl** directory.*

picture: Wikipedia

CBC mode



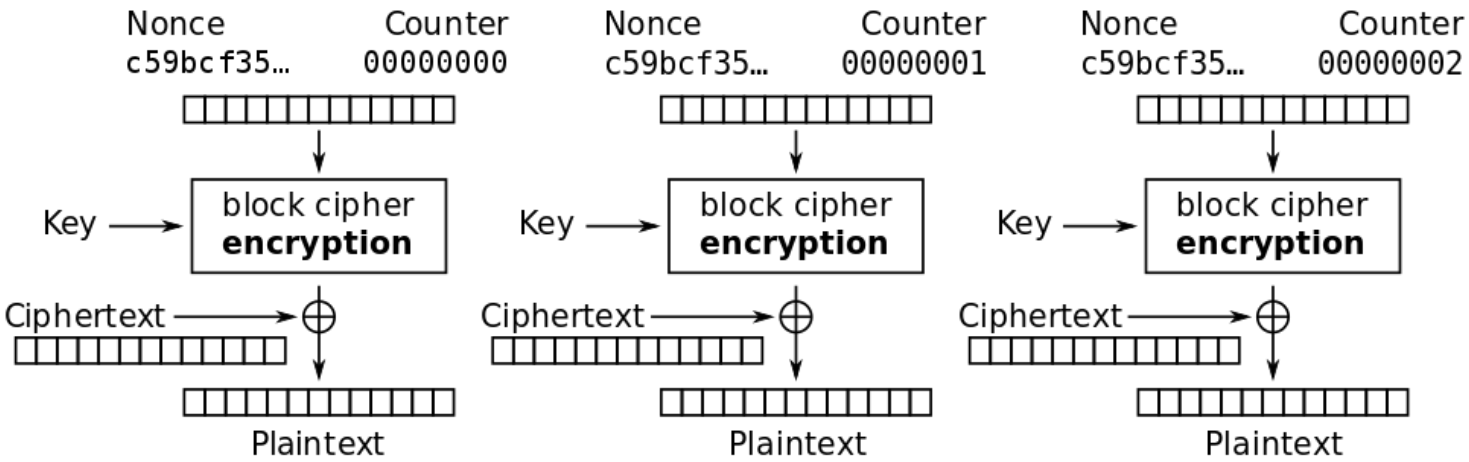
Cipher Block Chaining (CBC) mode decryption

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

*See **4a_encryption_fails_openssl** directory.*

picture: Wikipedia

CTR mode (counter mode)



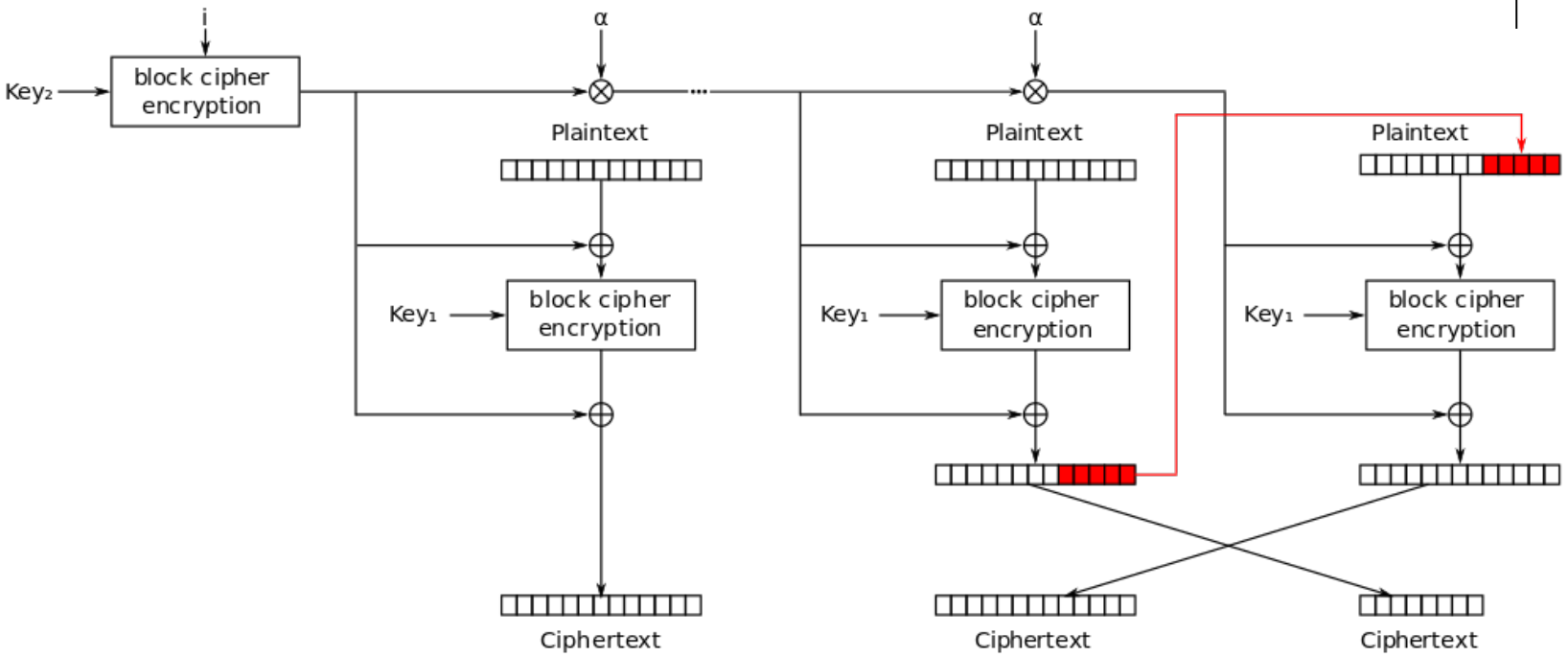
Counter (CTR) mode decryption

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

*See **4a_encryption_fails_openssl** directory.*

picture: Wikipedia

XTS mode storage (file, disk) encryption



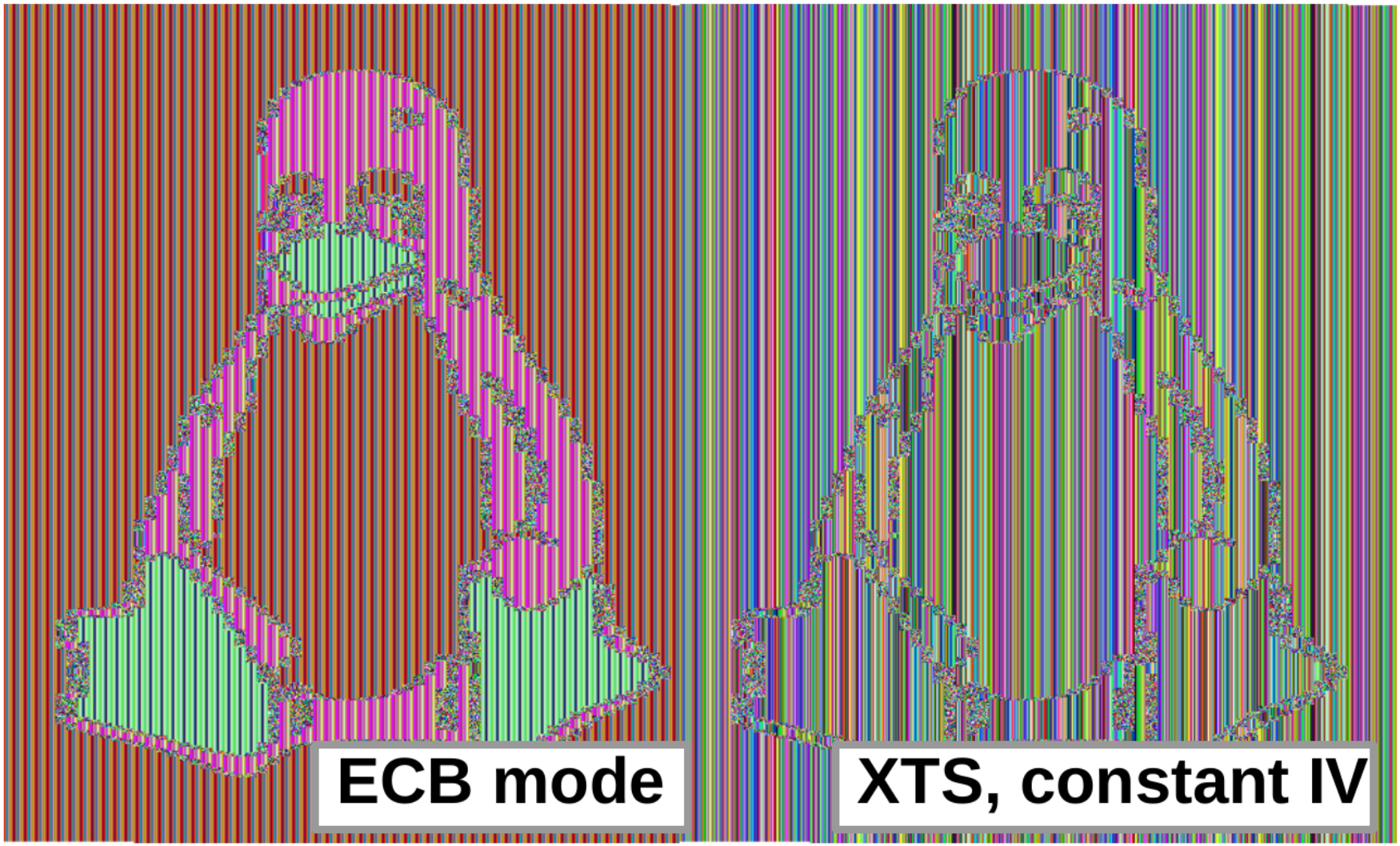
XEX with tweak and ciphertext stealing (XTS) mode encryption

Wrong use demo: block patterns with constant IV.

*See **4a_encryption_fails_openssl** directory.*

picture: Wikipedia

Symmetric encryption fails: patterns in ciphertext



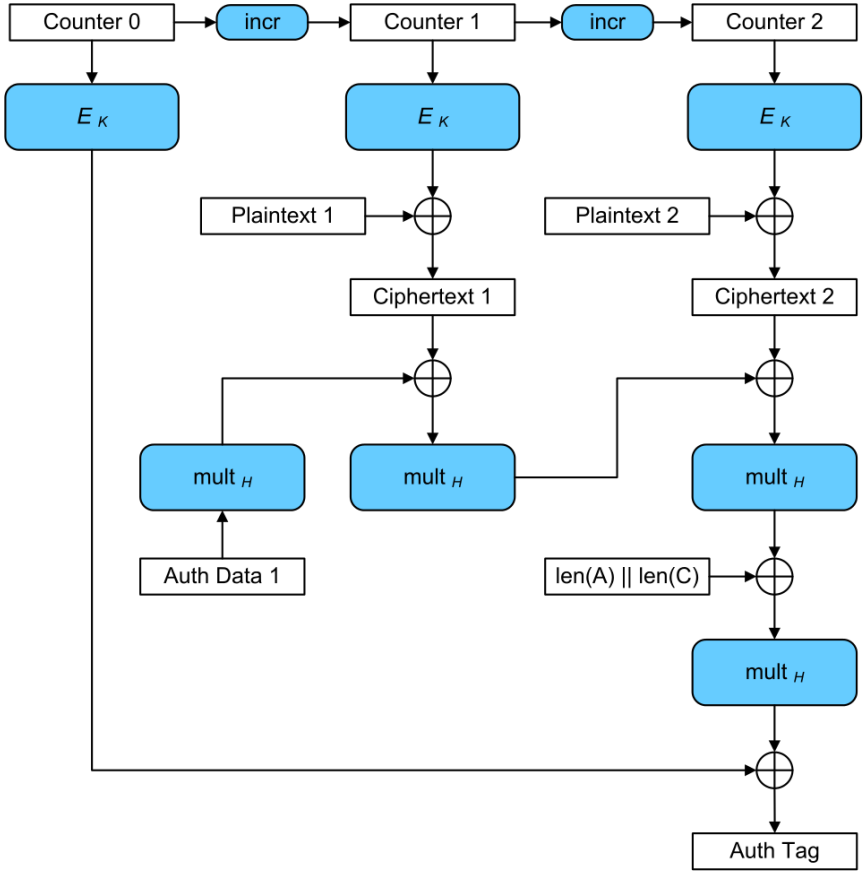
No integrity protection… (no authentication of data)

Authenticated mode
GCM - Galois/Counter Mode

Authenticated Encryption with Additional Data (AEAD):

confidentiality + integrity.

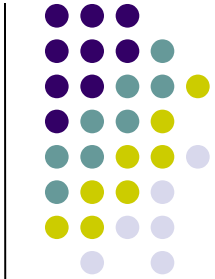
- *additional auth. data (AAD)*
- *data (plaintext/ciphertext)*
- *authentication tag*



*See **4a_encryption_fails_openssl** directory.*

picture: Wikipedia

Example 5: OpenSSL BIO (I/O abstraction)

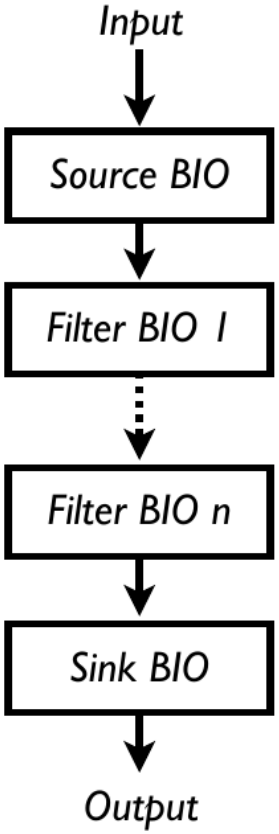


Source/sink BIOs:

BIO_s_mem() - memory I/O
BIO_s_file() - file I/O
BIO_s_fd() - file descriptor IO
BIO_s_socket() - sockets
BIO_s_accept()
BIO_s_connect()
BIO_s_null() - discard (like /dev/null)

Filters

BIO_f_base64() - Base64 encoding
BIO_f_buffer() - buffering I/O
BIO_f_cipher() - encryption/decryption
BIO_f_md() - message digest
BIO_f_ssl() - SSL support for BIO



Example 5: the same encryption as in Example 4 using BIO interface.
*See **5_bio_openssl** directory**.*