Crypto libraries OpenSSL II (cont.)

Milan Brož
xbroz@fi.muni.cz

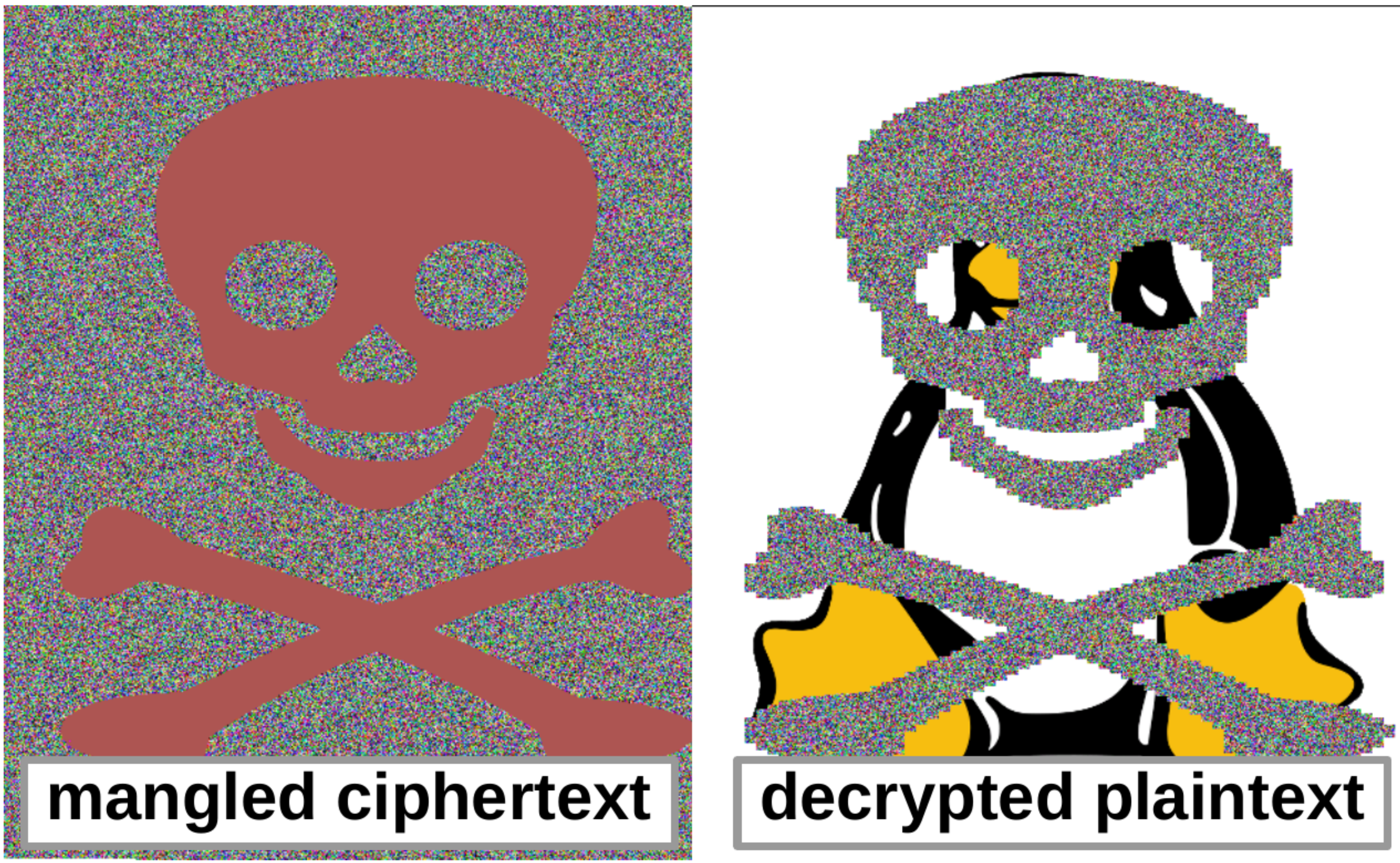
PV181, FI MUNI, Brno

Today's exercise

- Notes: common mistakes in 1st assignment

- Continue with OpenSSL on Linux
- **Authenticated encryption**
  AEAD – Authenticated Encryption with Associated Data
  GCM example
- **OpenSSL3 ECC** (elliptic curves) keygen
- **Trivial TLS client**
- Bonus: OpenSSL3 providers example

Why AEAD
integrity protection for data

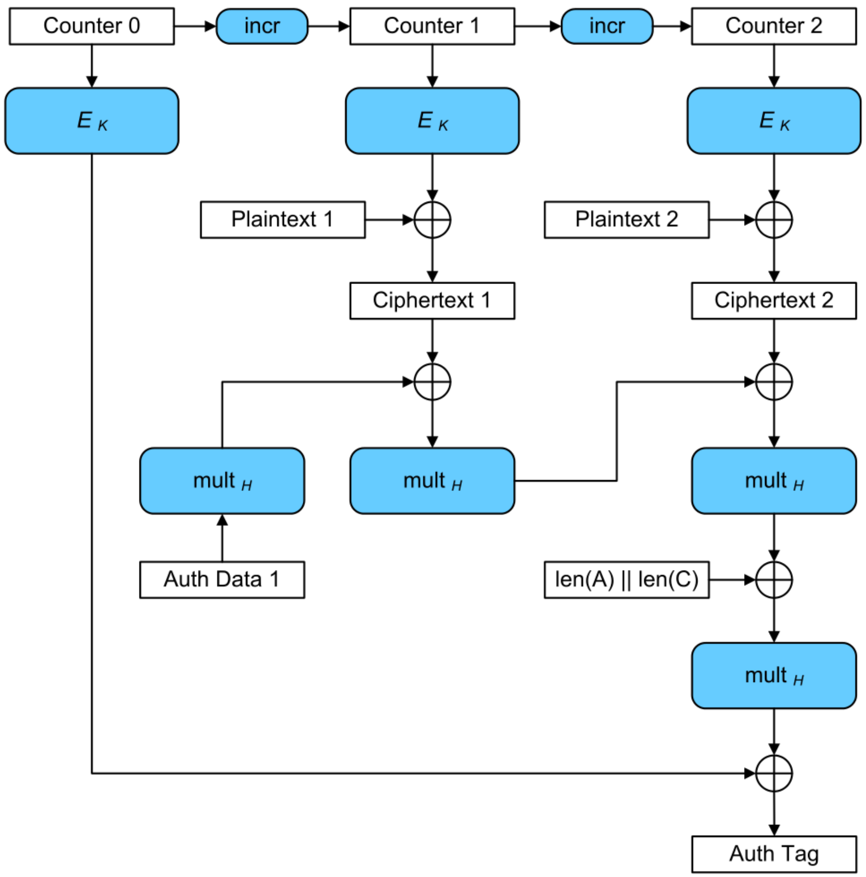


Authenticated mode
GCM - Galois/Counter Mode

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

Example 5: AEAD Authenticated encryption

OpenSSL (3.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.*

Example 8:
TLS connection & certificates

BIO TLS connection

- `SSL_CTX_set_verify, SSL_get_peer_certificate, SSL_get_verify_result`
- `BIO_new_ssl_connect, BIO_get_ssl, BIO_do_connect, BIO_do_handshake`

X509

- `X509_STORE_CTX_get_current_cert, X509_print_ex_fp, X509_NAME_get_entry, …`

Connect to https://www.google.com.

Read and validate certificates.

Sent HTTP GET and receive /robots.txt through a secured connection.

*See **8_tls_client_openssl** directory.*

Example 9: ECC keys, sign & verify with ED25519

EC key (pair) generation

EVP_PKEY_CTX_new_from_name
EVP_PKEY_keygen_init
EVP_PKEY_CTX_set_params
EVP_PKEY_generate

// Also: EVP_EC_gen(), EVP_PKEY_Q_keygen()

Signature – there can be differences for different curves

ED25519: EVP_DigestSign/EVP_DigestVerify (one-shot)

Export of keys and attributes

EVP_PKEY_get_* functions
PEM_write_bio_PrivateKey
PEM_write_bio_PUBKEY

*See **9_ecc_gen_openssl3** directory.*

Bonus: OpenSSL3 providers

You can define you own library;
It is loaded and used through OpenSSL3 API

Provider Corner
A place for public OpenSSL provider modules, including demos and lessons. This is NOT part of the OpenSSL organization.

https://github.com/provider-corner

- **Toy example: Vigenere cipher** (historic 16th century cipher)
  git clone https://github.com/provider-corner/vigenere
  git submodule init
  git submodule update
  cmake .
  make
- Need to copy to ossl-modules dir or use config

```
$ echo ahoj | openssl enc -provider vigenere -e -vigenere -K 000102030405060708090a0b0c0d0e0f
aiqm
```