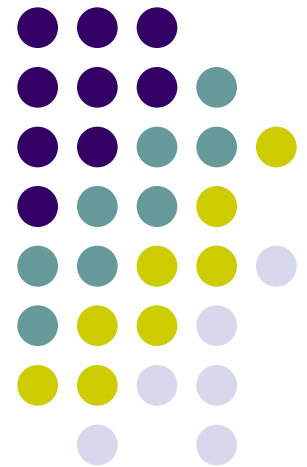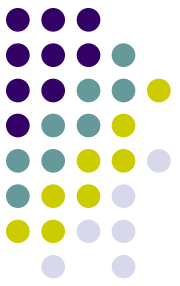# Crypto libraries OpenSSL II (cont.)

Milan Brož

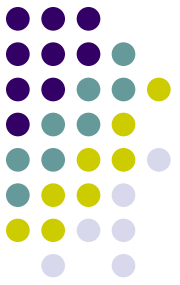xbroz@fi.muni.cz

PV181, FI MUNI, Brno

Today's exercise

- Continue with OpenSSL on Linux
- Work with certificates
- More complex example
- Trivial TLS client with https cert. validation
- Assignment (see separate file, 5+5 points)

Example 6: Signing and certificates

PKCS12
- PKCS12_verify_mac, PKCS12_parse

PKCS7
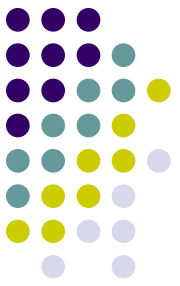- PKCS7_sign, PKCS7_verify

X509
- X509_STORE_add_lookup

BIO
- BIO_new, BIO_new_mem_buf, BIO_new_file
- BIO_push, BIO_f_cipher, BIO_set_cipher
- BIO_flush, BIO_free_all
- d2i_PKCS12_bio, d2i_PKCS7_bio

*See **6_cert_sign_openssl** directory.*

Example 7:
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, …
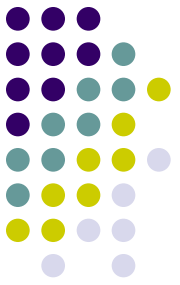
Connect to https://www.google.com.

Read and validate certificates.

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

*See **7_tls_client_openssl** directory.*

Assignment

- Two goals:
  - Generate RSA key in C [max 5 points]
  - Print certificate chain in TLS (HTTPS) connection [max 5 points]
  - Use OpenSSL in Linux environment
- See Assignment.txt in IS for details and deadline
- You can start with examples in git
- Read (and use) provided hints!
- Comment your code
- You can use provided Fedora VM or aisa server (or any OpenSSL Linux, even Win10 embedded Linux)