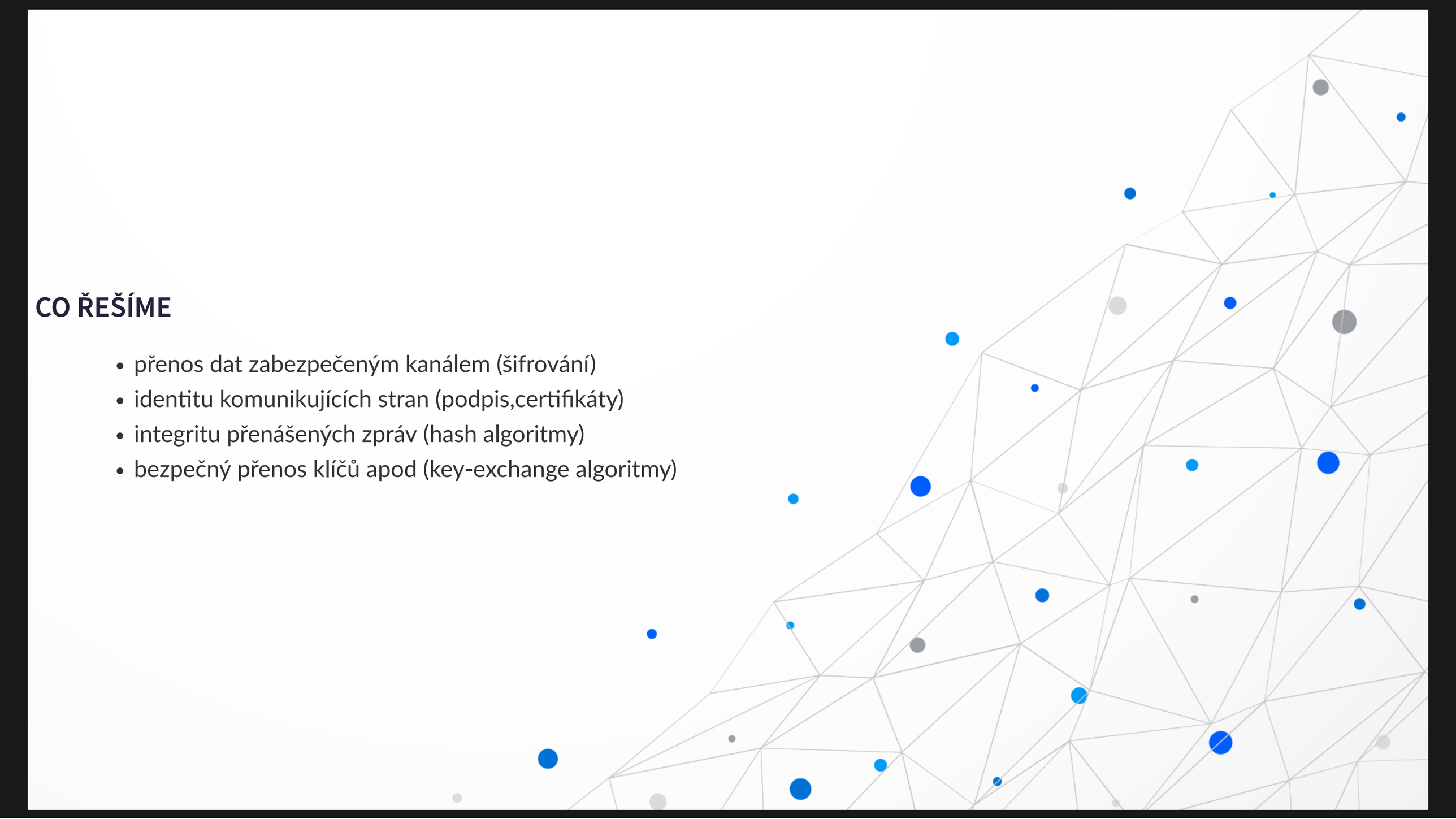
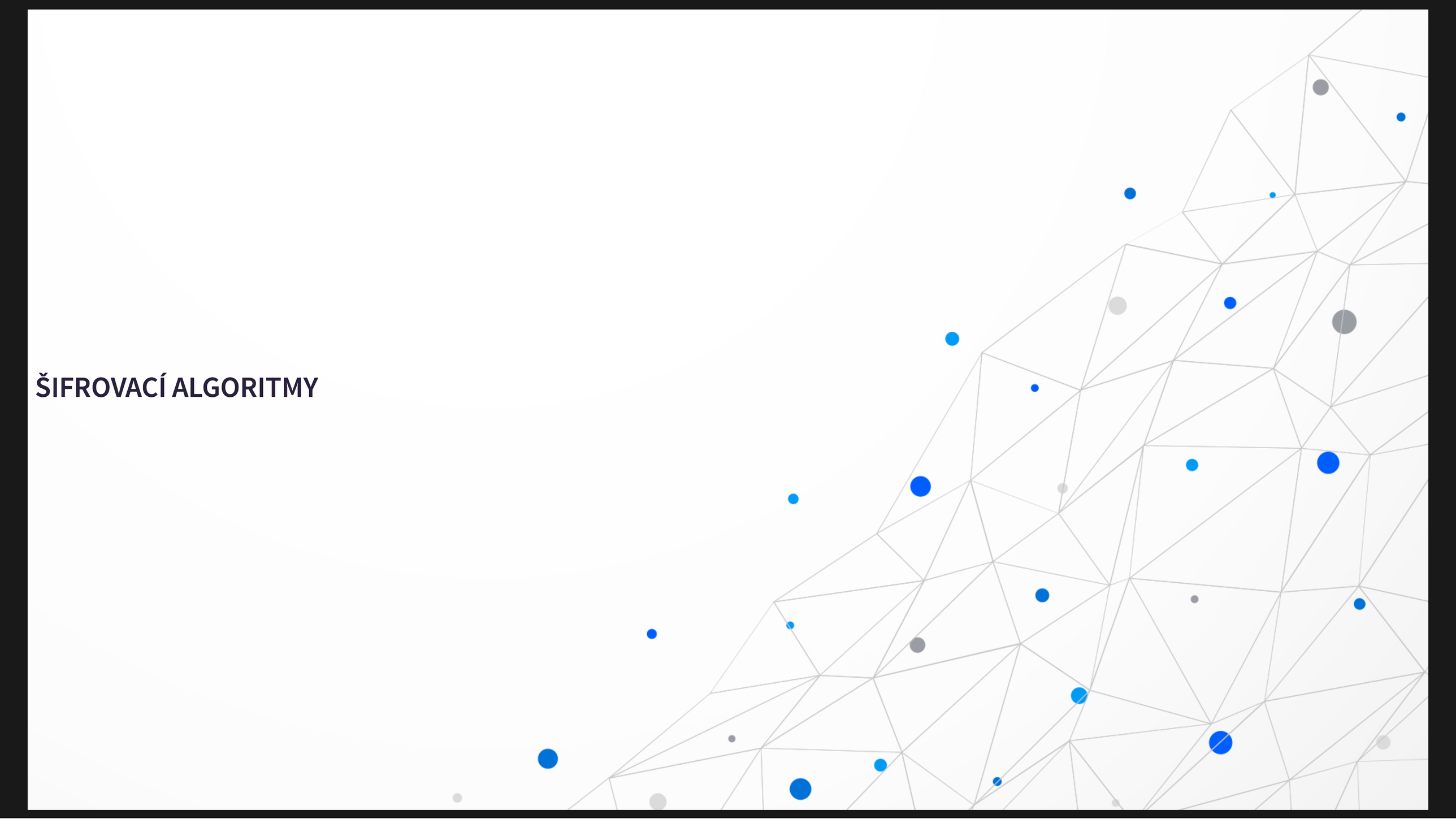
VELMI JEMNÝ ÚVOD DO KRYPTOGRAFIE

CO ŘEŠÍME

- přenos dat zabezpečeným kanálem (šifrování)
- identitu komunikujících stran (podpis,certifikáty)
- integritu přenášených zpráv (hash algoritmy)
- bezpečný přenos klíčů apod (key-exchange algoritmy)

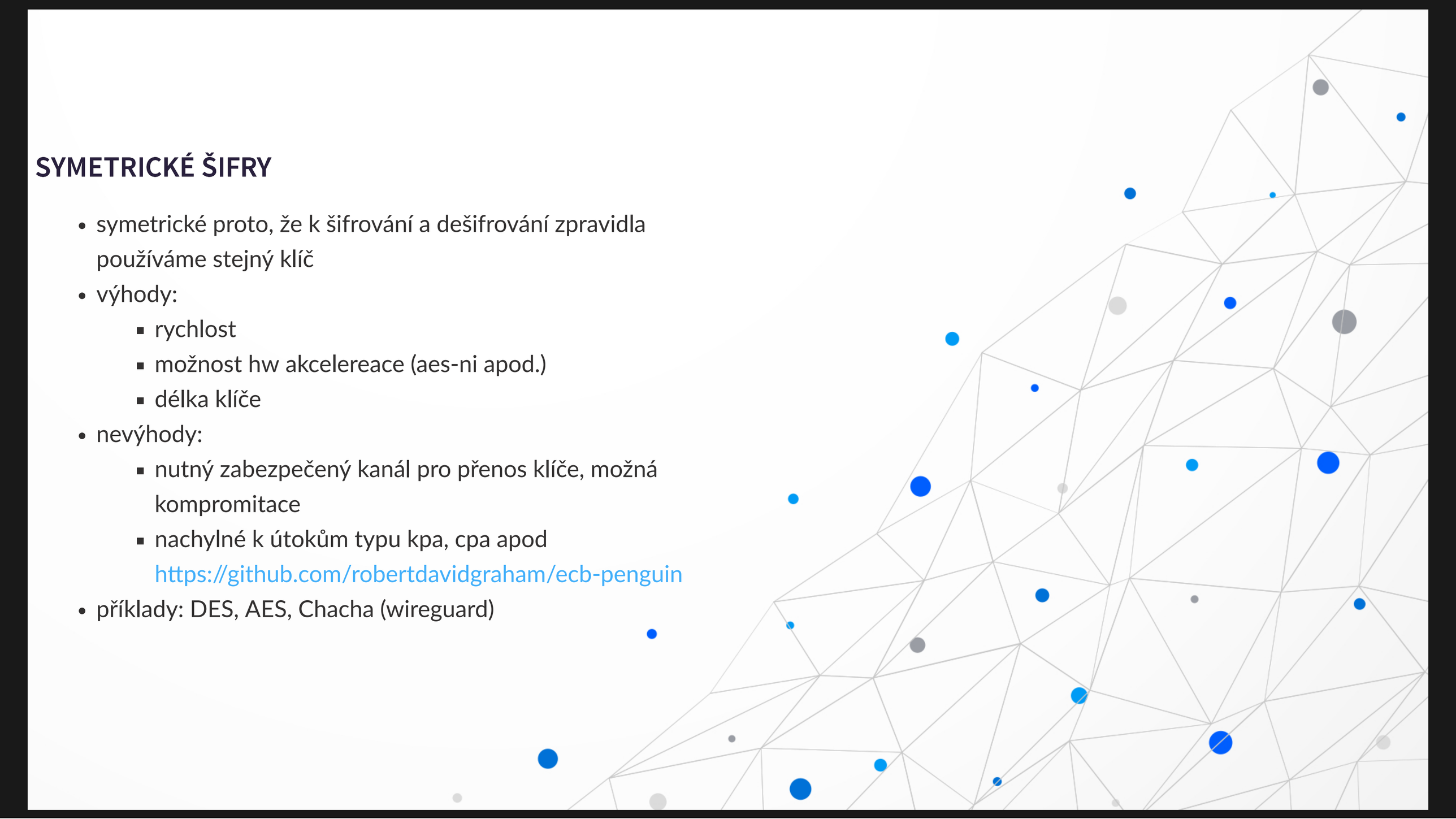


ŠIFROVACÍ ALGORITMY



SYMETRICKÉ ŠIFRY

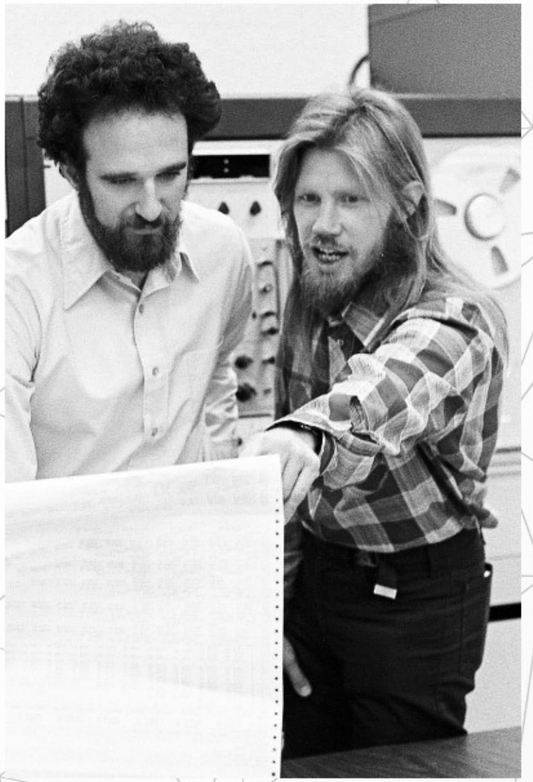
- symetrické proto, že k šifrování a dešifrování zpravidla používáme stejný klíč
- výhody:
  - rychlost
  - možnost hw akcelereace (aes-ni apod.)
  - délka klíče
- nevýhody:
  - nutný zabezpečený kanál pro přenos klíče, možná kompromitace
  - nachylné k útokům typu kpa, cpa apod https://github.com/robertdavidgraham/ecb-penguin
- příklady: DES, AES, Chacha (wireguard)



PROBLÉM - JAK BEZPEČNĚ PŘENÉST KLÍČE ??

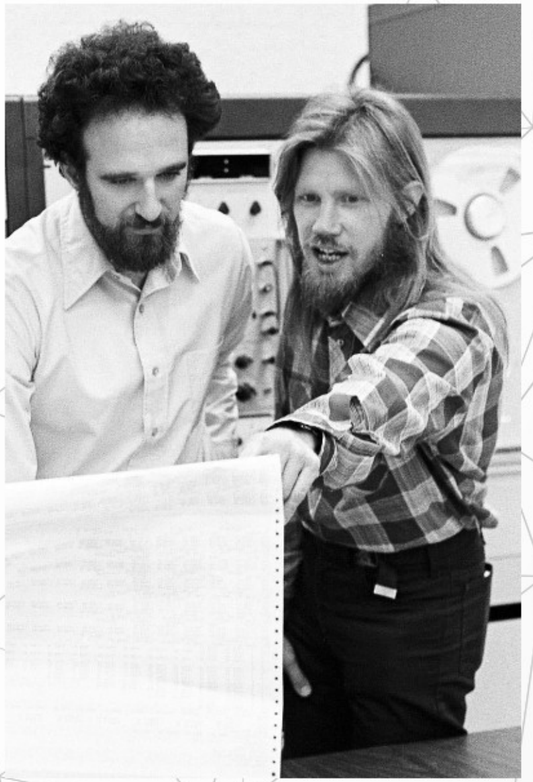
DIFFIE-HELLMAN ALGORITMUS

- Algoritmus umožňuje vytvořit klíč bez jeho fyzické výměny
  - základ je modulo aritmetika nad prvočísly a problém tzv. diskrétního logaritmu
  - long story short:
    - obě strany sezení si vygenerují pár prvočísel
    - jedno z nich zveřejní tomu druhému
    - na základě dalších výpočtů dojdou ke stejné hodnotě klíče
    - v praxi se používají velmi velká prvočísla a tím se zvyšuje bezpečnost (entropie) klíče
- Vygenerovaný klíč, je poté použit v nějaké symetrické šifře pro vytvoření zabezpečeného kanálu
  https://www.youtube.com/watch?v=d1KXDGgwIpA



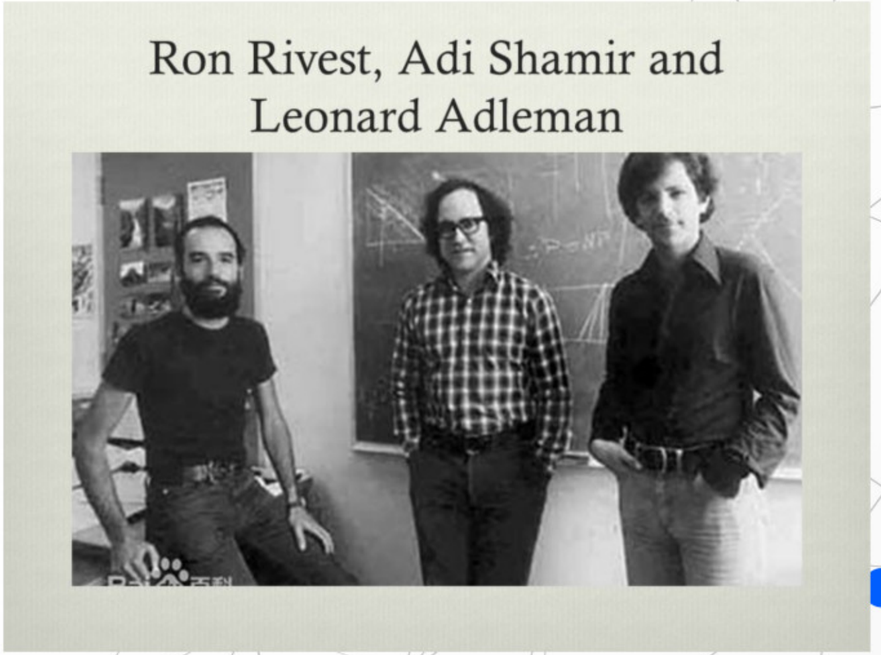
DIFFIE-HELLMAN ALGORITMUS - PRAKTICKÉ INFORMACE

- DH key exchange je nedílnou součástí TLS specifikace pro iniciální výměnu klíčů
- V praxi se přechází na novější schéma ECDH, které
  - je rychlejší
  - ma menší klíče
- TLS 1.2 nabízí jediné schéma bez DH, v TLS 1.3 jsou všechny schémata s DH
- Pokud TLS používá DH schéma není možné provoz dešifrovat pomocí privátního klíče: https://www.root.cz/clanky/desifrujeme-https-pomoci-nastroje-wireshark/



ASYMETRICKÉ ŠIFRY

- Dva na sobě závislé klíče:
  - Veřejný - protistrana využije k šifrování
  - Privátní - dešifrování zpráv zašifrovaným veřejným klíčem
- Můžeme ale klíče použít i pro podepisování zpráv
  - Privátním klíčem zprávu zašifrujeme
  - Veřejným klíčem zprávu rozšifrujeme => jsme autory zprávy
  - V praxi se kombinuje s hashovací funkcí
- výhody:
  - relativní bezpečnost
- nevýhody:
  - nutný zabezpečený kanál pro přenos klíčů, možná kompromitace
  - vyšší výpočetní náročnost
  - délka klíče (RSA)
- příklady: RSA, ElGamal, ECC algoritmy (ECDSA).

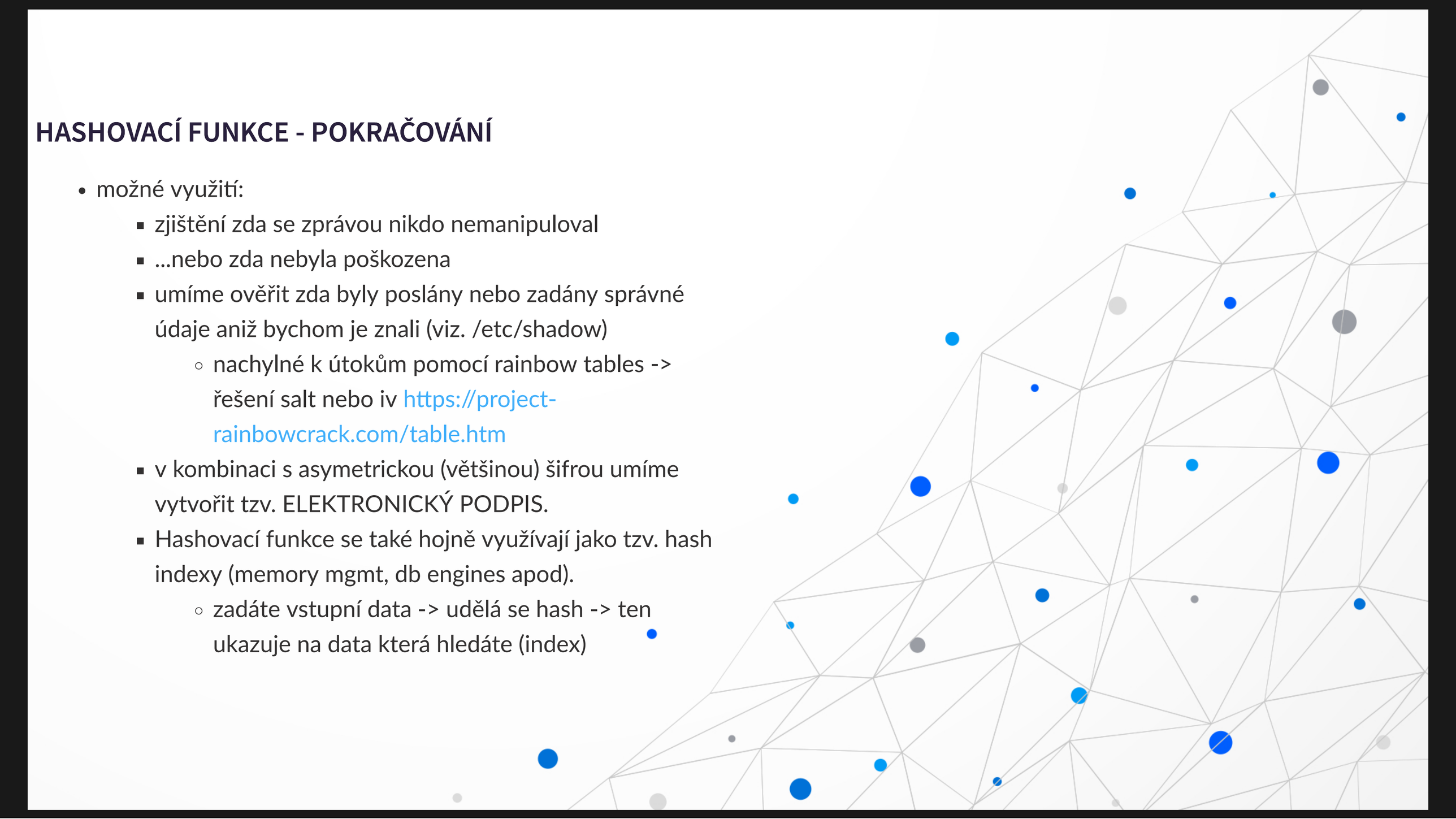


HASHOVACÍ FUNKCE - KONTROLA INTEGRITY PŘENÁŠENÝCH ZPRÁV

- Hashovací fce ja taková která převede vstupní data do množiny s menší mohutností (prostě udělá otisk/checksum etc)
- tato funkce by měla být nejlépe tzv. bezkolizní
- příklady: SHA family, MD5 (nepoužívá se, nalezeny kolize => prolemena)

HASHOVACÍ FUNKCE - POKRAČOVÁNÍ

- možné využití:
  - zjištění zda se zprávou nikdo nemanipuloval
  - ...nebo zda nebyla poškozena
  - umíme ověřit zda byly poslány nebo zadány správné údaje aniž bychom je znali (viz. /etc/shadow)
    - nachylné k útokům pomocí rainbow tables -> řešení salt nebo iv https://project-rainbowcrack.com/table.htm
  - v kombinaci s asymetrickou (většinou) šifrou umíme vytvořit tzv. ELEKTRONICKÝ PODPIS.
  - Hashovací funkce se také hojně využívají jako tzv. hash indexy (memory mgmt, db engines apod).
    - zadáte vstupní data -> udělá se hash -> ten ukazuje na data která hledáte (index)



...ALE CO KDYŽ KOMUNIKUJU S NĚKÝM JINÝM NEŽ SI MYSLÍM

- musíme nějak ověřit totožnost protistrany....

CO JE CERTIFIKÁT

- Certifikát je struktura popisující jeho vlastníka
- Obsahuje:
  - Atributy
  - Většinou veřejný klíč držitele (ale není podmínkou)
  - Je podepsán privátním klíčem Certifikační Autority (selfsigned neřešíme)
- Různé formáty (PEM, DER, P12...)
- X509 ITU Standard

```
$ openssl x509 -in ~/certs.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 108 (0x6c)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=LX.IFORTUNA.CZ, CN=Certificate Authority
        Validity
            Not Before: Jun 27 12:16:59 2019 GMT
            Not After : Jun 27 12:16:59 2021 GMT
        Subject: O=LX.IFORTUNA.CZ, CN=apigw-mw-sk.t.dc1.cz.ipa.ifortuna.cz
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:61:c2:4d:73:93:0c:08:2b:d3:fd:8b:00:ba:
                    5f:01:89:8e:8e:f3:ea:38:2b:6a:2b:1c:b2:90:65:
                    35:c9:95:5f:52:7b:13:f8:d7:82:2a:e8:62:7b:90:
                    ff:b0:66:81:62:41:39:c5:ea:04:31:d5:b1:7e:f5:
                    30:5b:6a:9a:4c:11:8d:c7:38:1d:27:7d:fd:7f:5f:
                    aa:f5:d3:c0:75:46:05:78:f2:15:ce:17:3a:7e:d5:
                    e8:66:3a:51:11:8e:68:44:7d:da:4c:39:4b:4e:d7:
                    c6:7d:cd:cd:1e:c1:e0:e5:e9:62:32:87:7b:b3:37:
                    22:11:ec:c7:5d:f9:59:61:5d:af:ba:ff:80:85:e1:
                    c9:67:62:31:da:33:36:7c:82:44:f0:7f:9c:84:e4:
                    f9:1f:82:15:de:c4:df:d1:df:29:bf:a5:82:09:0c:
                    6d:75:c8:32:6e:47:09:ae:b7:56:42:26:67:48:05:
                    0e:26:ab:09:cf:15:cd:94:1e:12:a0:e1:6b:08:0c:
                    ed:68:97:e6:55:3c:47:62:da:14:d9:31:17:ac:50:
                    fb:4d:9e:cb:51:1f:c7:05:7b:8f:c1:7e:ba:37:90:
                    88:8a:18:83:a9:ce:56:86:1c:ae:25:92:44:6d:82:
                    cc:34:f4:65:15:7c:ae:09:23:48:97:7e:63:a9:ff:
                    a7:5f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:0C:25:47:CE:60:92:C8:13:70:2D:A8:F2:45:09:42:92:D1:CC:20:3A

            Authority Information Access:
                OCSP - URI:http://ipa-ca.lx.ifortuna.cz/ca/ocsp

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ipa-ca.lx.ifortuna.cz/ipa/crl/MasterCRL.bin
                CRL Issuer:
                  DirName: O = ipaca, CN = Certificate Authority
```

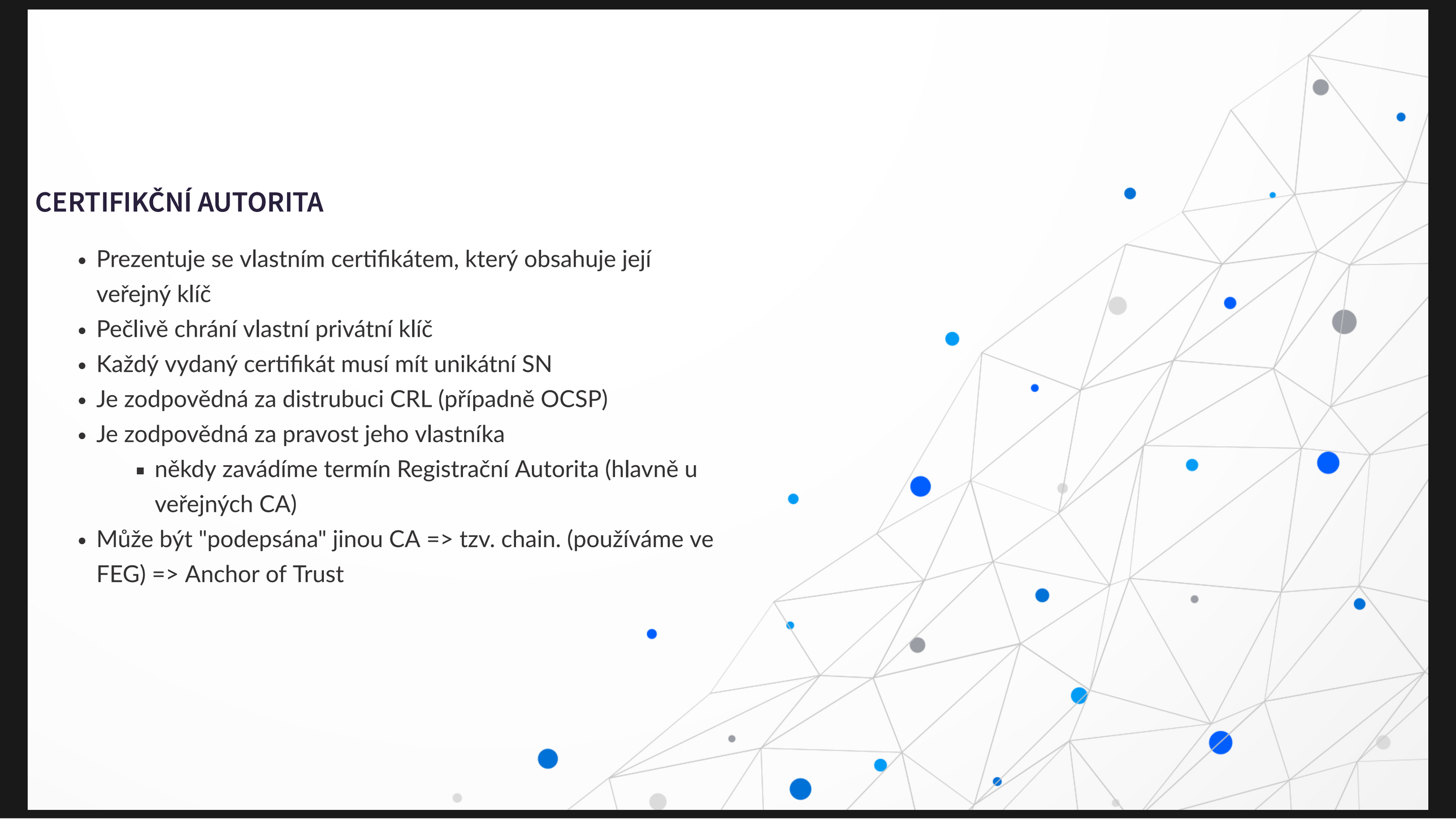
DŮLEŽITÉ ATRIBUTY

- Platnost
- Subject
- Seriové číslo
- Kdo ho vydal
- Informace o klíčích
- Podpis CA
- OCSP/CRL

```
$ openssl x509 -in ~/certs.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 108 (0x6c)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=LX.IFORTUNA.CZ, CN=Certificate Authority
        Validity
            Not Before: Jun 27 12:16:59 2019 GMT
            Not After : Jun 27 12:16:59 2021 GMT
        Subject: O=LX.IFORTUNA.CZ, CN=apigw-mw-sk.t.dc1.cz.ipa.ifortuna.cz
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cd:61:c2:4d:73:93:0c:08:2b:d3:fd:8b:00:ba:
                    5f:01:89:8e:8e:f3:ea:38:2b:6a:2b:1c:b2:90:65:
                    35:c9:95:5f:52:7b:13:f8:d7:82:2a:e8:62:7b:90:
                    ff:b0:66:81:62:41:39:c5:ea:04:31:d5:b1:7e:f5:
                    30:5b:6a:9a:4c:11:8d:c7:38:1d:27:7d:fd:7f:5f:
                    aa:f5:d3:c0:75:46:05:78:f2:15:ce:17:3a:7e:d5:
                    e8:66:3a:51:d1:8e:68:44:7d:da:4c:39:4b:4e:d7:
                    c6:7d:cd:cd:1e:c1:e0:e5:e9:62:32:87:7b:b3:37:
                    22:11:ec:c7:5d:f9:59:61:5d:af:ba:ff:80:85:e1:
                    c9:67:62:31:da:33:36:7c:82:44:f0:7f:9c:84:e4:
                    f9:1f:82:15:de:c4:df:d1:df:29:bf:a5:82:09:0c:
                    6d:75:c8:32:6e:47:09:ae:b7:56:42:26:67:48:05:
                    0e:26:ab:09:cf:15:cd:94:1e:12:a0:e1:6b:08:0c:
                    ed:68:97:e6:55:3c:47:62:da:14:d9:31:17:ac:50:
                    fb:4d:9e:cb:51:1f:c7:05:7b:8f:c1:7e:ba:37:90:
                    88:8a:18:83:a9:ce:56:86:1c:ae:25:92:44:6d:82:
                    cc:34:f4:65:15:7c:ae:09:23:48:97:7e:63:a9:ff:
                    a7:5f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:0C:25:47:CE:60:92:C8:13:70:2D:A8:F2:45:09:42:92:D1:CC:20:3A

            Authority Information Access:
                OCSP - URI:http://ipa-ca.lx.ifortuna.cz/ca/ocsp

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ipa-ca.lx.ifortuna.cz/ipa/crl/MasterCRL.bin
                CRL Issuer:
                  DirName: O = ipaca, CN = Certificate Authority
```

CERTIFIKČNÍ AUTORITA

- Prezentuje se vlastním certifikátem, který obsahuje její veřejný klíč
- Pečlivě chrání vlastní privátní klíč
- Každý vydaný certifikát musí mít unikátní SN
- Je zodpovědná za distrubuci CRL (případně OCSP)
- Je zodpovědná za pravost jeho vlastníka
    - někdy zavádíme termín Registrační Autorita (hlavně u veřejných CA)
- Může být "podepsána" jinou CA => tzv. chain. (používáme ve FEG) => Anchor of Trust



POSTUP PŘI VYTVÁŘENÍ CERTIFIKÁTŮ

- uživatel vytvoří dvojici klíčů
- vytvoří tzv. CSR který obsahuje:
  - atributy popisující uživatele (případně server, email)
  - veřejný klíč
  - Poznámka: openssl umí vytvořit klíče a příslušný CSR v jediném kroku.
- Paranoici si vytvoří klíče + CSR sami, v praxi je většinou vytvořen na nějakém trusted zařízení CA/RA
- CA ověří uživatele a to že informace v CSR jsou v pořádku
- CA vydá certifikát s unikátním SN a přidá atributy, které ji popisují, případně další atributy vlastníka

SROVNÁNÍ PKI A JWT/OPENID CONNECT

- Certifikační autorita
- Longterm validita (typicky rok)
- Šifrováni, Autentizace, Podpis
- Osoby, Servery
- Atributy, kliče, podpis

- Identity Provider (IdP)
- Shortterm (minuty max dny)
- Autentizace, Autorizace
- Osoby, Aplikace
- Atributy, podpis

MALÝ SLOVNÍČEK POJMŮ

- plain text/šifrovaná zpráva
- šifrovací alogitmus
- hash algoritmus
- key-exchange algoritmus
- klíč
- inicializační vektor
- certifkát
- salt
- TLS