

Algoritmus RSA

Jáchym Tomášek

info@tomasek.work

www.tomasek.work/RSA.pdf

Komunikace pomocí RSA

Před začátkem komunikace pomocí RSA

- Zvolí se dvě velká prvočísla p a q
- Spočítá se jejich součin n : $n = pq$
- Spočítá se hodnota Eulerovy funkce $\phi(n) = (p - 1)(q - 1)$
- Zvolí se číslo e : $e < \phi(n)$ a e je nesoudělné s $\phi(n)$
- Zjistí se číslo d : $de = 1 \pmod{\phi(n)}$

Komunikace RSA

- Veřejný klíč – e a n
 - e je šifrovací exponent
 - n je modul
- Soukromý klíč – d a n
 - d je dešifrovací exponent
 - n je modul

Zašifrování komunikace RSA

- Zpráva se převede na číslo j : $j < n$
- Zpráva se zašifruje na číslo k : $k = j^e \bmod n$
- Číslo k je zašifrovaná zpráva, která se odešle příjemci

Dešifrování komunikace RSA

- Příjemce dostane zašifrovanou zprávu k
- Původní zprávu j získá pomocí: $j = k^d \bmod n$

Digitální podpisy

Certifikát

- Certifikační autorita vytvoří soukromý a veřejný klíč
- Veřejný klíč je dostupný všem (i příjemci)
- Soukromý klíč je uložený na počítači majitele nebo na nějakém externím zařízení
- Pomocí certifikátu se ukládá soukromý klíč na počítač

Certifikát

- Soubor s příponou CRT

```
0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCD
000 3082 052B 3082 0413 A003 0201 0202 1009 0 .+0 .. .....
010 EA1D A77C 15E1 7621 A4D7 8922 1981 3F30 ê.š|.áv!hx ". ?0
020 0D06 092A 8648 86F7 0D01 0108 0500 3081 ...* H ÷.....0
030 9631 0B30 0906 0355 0406 1302 4742 311B 1.0...U...GB1.
040 3019 0603 5504 0813 1247 7265 6174 6572 0...U...Greater
050 204D 616E 6368 6573 7465 7231 1030 0E06 Manchester1.0..
060 0355 0407 1307 5361 6C66 6F72 6431 1830 .U...Salford1.0
070 1606 0355 040A 130F 5365 6374 6967 6F20 ...U...Sectigo
080 4C69 6D69 7465 6431 3E30 3C06 0355 0403 Limited1>0<..U..
090 1335 5365 6374 6967 6F20 5253 4120 436C .5Sectigo RSA Cl
0A0 6965 6E74 2041 7574 6865 6E74 6963 6174 ient Authenticat
0B0 696F 6E20 616E 6420 5365 6375 7265 2045 ion and Secure E
0C0 6D61 696C 2043 4130 1E17 0D32 3031 3132 mail CA0...20112
0D0 3130 3030 3030 305A 170D 3230 3132 3231 1000000Z..201221
0E0 3233 3539 3539 5A30 2531 2330 2106 092A 23595920%1#0!..*
0F0 8648 86F7 0D01 0901 1614 6A61 6374 6F6D H ÷.....jactom
100 6173 656B 4067 6D61 696C 2E63 6F6D 3082 aseka@gmail.com0
110 0122 300D 0609 2A86 4886 F70D 0101 0105 ."0...* H ÷.....
120 0003 8201 0F00 3082 010A 0282 0101 009D ... ..0 ... ..
130 239A 4121 6233 662A 98DF 7C6F 5641 A12C # A!b3f* B|oVAj,
140 1DCD 8705 062D 1121 F928 87C2 68DD ED10 .í ...!ù+ ÁhÝí.
150 AE15 102B C0A1 89F2 A8F6 D2C5 0F9B E22B @..+À; ò"òÀ. á+
160 0157 A388 6687 423E 7580 A5B8 90E9 CDBB .WE f B>u*%& éi»
170 000F 4532 3909 A964 E538 BAF9 67A2 ECAC ..E29.@dâ8=ùg#i-
180 9ED9 F057 2541 6152 6445 28FD FE2E 6AB6 ÛðW%AaRdE(ýp.jj
190 6EFF C87A 0ADF B8A4 686B ED24 4A52 E4BE nýËz.B,hkí$JRa%
1A0 358C 1018 ADAA 2EA0 0844 76A9 D26F A914 5%..-#. .Dv00o0.
1B0 FD47 408E 3699 EE0E FD06 4EDA 7148 66D2 ýG@ 6 i.y.NúqHfD
1C0 1F07 69F4 2DCF 9293 D515 C128 37FF 629C ..i0-i Ô.Á(7yb
1D0 7777 24D1 ED48 4DFD 873F 2E5D 4CBF FE55 ww$ñíHMý ?.]LzþU
1E0 4F91 D3E7 A2CA BAA5 656D 764E 57BA 3A26 O ÓççÊÈ$emvNÑe:&
1F0 5EC1 07FC D585 9523 0A12 2820 D7AF 0711 ^Á.úö #..( x^-..
200 5C5E 1237 3768 9465 A543 1601 6410 AC04 \^.77h e%ç..d.-.
210 4106 6DED D752 E4CD EEA9 F245 28A7 9210 A.míxRáíiòèE($ .
220 34EB 7469 308D D380 6733 EA0A 27A1 4902 4èti0 ó°g3è.'jI.
230 0301 0001 A382 01E3 3082 01DF 301F 0603 ....E .ã0 .R0...
240 551D 2304 1830 1680 1409 C0F2 FC0B DA94 U.#..0. ..làü.Ú
250 DB5F FE2B DFA8 9942 CFC9 E0AD 0030 1D06 Û_p+B" BÍÉà-.0..
260 0355 1D0E 0416 0414 62CF D851 C5C7 A5D7 .U.....bí0QÁçyx
270 EE1C 3361 AA7E D6DF 08EB 0FBD 300E 0603 i.3a~òB.è.%0...
280 551D 0F01 01FF 0404 0302 05A0 300C 0603 U....ý..... 0...
290 551D 1301 01FF 0402 3000 3020 0603 551D U....ý..0.0 .U.
2A0 2504 1930 1706 082B 0601 0505 0703 0406 %..0...+.....
2B0 082B 0601 0401 B231 0103 0502 3011 0609 .+....²1....0...
2C0 6086 4801 86F8 4201 0104 0403 0205 2030 ` H. 0B..... 0
2D0 4006 0355 1D20 0439 3037 3035 060C 2B06 @..U. .90705..+.
2E0 0104 01B2 3101 0201 0101 3025 3023 0608 ...²1....0%0#..
2F0 2B06 0105 0507 0201 1617 6874 7470 733A +.....https:
300 2F2F 7365 6374 6967 6F2E 636F 6D2F 4350 //sectigo.com/CP
310 5330 5A06 0355 1D1F 0453 3051 304F A04D S0Z..U...S0Q00 M
320 A04B 8649 6874 7470 3A2F 2F63 726C 2E73 K Ihttp://crl.s
330 6563 7469 676F 2E63 6F6D 2F53 6563 7469 ectigo.com/Secti
340 676F 5253 4143 6C69 656E 7441 7574 6865 goRSAClientAuthe
```

Soukromý klíč

- Soubor s příponou PFX
- Dlouhý kolem 150 řádků
- Veřejný klíč vypadá podobně

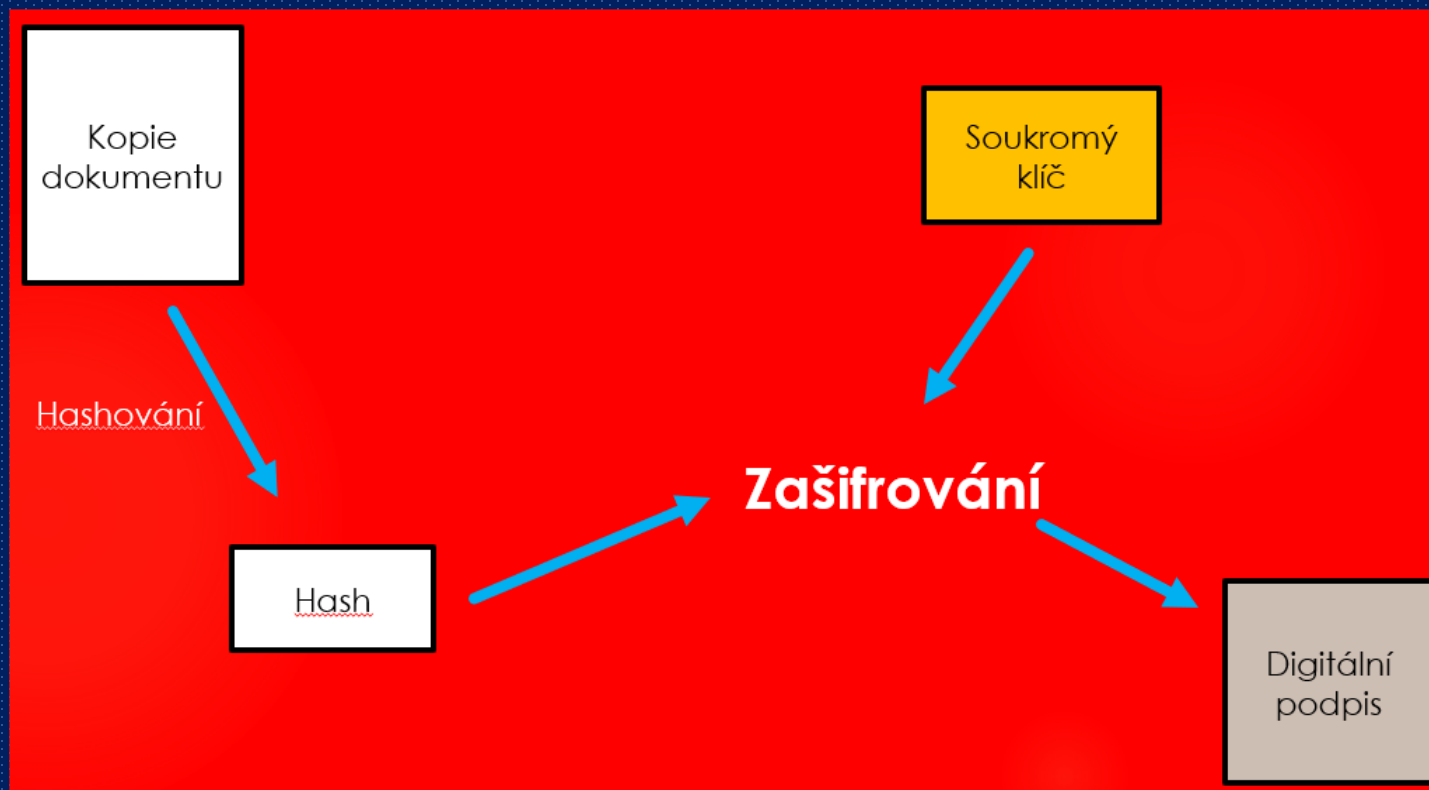
The screenshot shows a HEX editor window with a menu bar (Soubor, Hledat, Zobrazit, Formát, Kódová stránka, Nástroje, HTML, Nastavění, Okno, Nápověda) and a toolbar. The main area displays a list of hexadecimal values in two columns, with the corresponding ASCII characters shown to the right. The file name 'd.pfx' is visible in the top left corner. The data appears to be a concatenation of hexadecimal and ASCII representations of a private key.

```
0001 0203 0405 0607 0809 0A0B 0C0D 0E0F 0123456789ABCDEF
030 06A0 8203 DC30 8203 D802 0100 3082 03D1 . .ü0 .0...0.Ň
040 0609 2A86 4886 F70D 0107 0130 2806 0A2A ..* H ÷....0(..*
050 8648 86F7 0D01 0C01 0630 1A04 142F 3B19 H +....0.../;.
060 B5EC C927 ABF2 670A 8CD9 7A01 FB8A 8F4E μiÉ'«òg. Ůz.Ů N
070 0402 0204 0080 8203 98BA 4633 7056 C1FB ..... *F3pVÁŮ
080 5303 4D8E C568 8370 E3BE A6FE 1807 30E0 S.M Åh pãk|p..0à
090 0B10 EFA1 3C09 1687 0E99 3F7D B889 A5E1 ..i;<... ?}. ¥á
0A0 4689 BC4E 883F D14B 7700 9A76 55EA F7D4 F %N ?ŇKw. vUë±0
0B0 4B90 0D43 84C4 546D 2A1E F2CD C1D0 1B50 K .C ÅTm*.òÍÁ.P
0C0 5592 7D62 93DC 08DF B74A 6E5C F600 53AB U }b Ů.B·Jn\0.S«
0D0 C586 C23C 2306 D40F 8DEF 20F7 55B5 458F Å Å<#.0. i ±UμE
0E0 00C9 B5F9 DE6D A0BE 361D 421A 4983 F2DC .ÉμòPm %6.B.I òŮ
0F0 39E5 0216 EA08 4AC6 4183 82C7 7157 0776 9ã..ë.JÆA CqM.v
100 5D65 3BD6 70B1 4872 34BB 1E55 3516 8B5E ]e;0p±Hr4».â5. ^
110 1263 3C51 9AD1 0FE7 BDC1 41FB F235 4063 .c<Q Ň.c%ÁA005@c
120 6A3A 5D2D 205A BCA8 C3F8 32CC FB52 9EC3 j;]- ZX"Å02ÏUR Å
130 0AB2 6588 72B2 DCEB D30C 2A5D D1C9 1236 .²e.r²Üëó.*]ŇÉ.6
140 4B32 EFC7 BA2E 4E2B 9B00 B2A4 53FA 8ECC K2iC².N+ .²Msú Ī
150 2BD6 BFAD 4ABB 66C5 D3F1 D33C D535 9C92 +0¿-J»æÅ0Ň0<05
160 34DD F134 07AE 302F 21DD 56B9 B1FC B771 4ÝŇ4.00/!ÝV²±ü·q
170 4D2A D95E AF26 AC84 A686 8C03 E973 2B39 M*Ů^&- | .és+9
180 E263 DBA6 752F 9A23 FDFB 05F3 88A4 3821 äcŮ!u/ #yŮ.ó #8!
190 143B 871B F18E 8783 62BF D26C F14C 28A8 .; .ñ b¿0lŇL(Ų
1A0 8528 BF79 C684 DF99 D796 56CE 955D 9F7A (¿yÆ B x VÎ ] z
1B0 0C9F A014 8842 2067 7120 85A2 7C39 7E35 . .B gq ¶|9~5
1C0 31FC 6074 7273 6CB5 9CED 18BD F5DF 596F 1ü"trs|μ i.%08Yo
1D0 E627 C2DA F5FB E0D8 7E10 C1E6 6C0A C6FD æ'ÅÜ00à0~.Áæ1.Æý
1E0 6C05 6CBF 2398 A60D 2BE4 CEFA F070 5448 1.l¿# |.+ãĪú0pTH
1F0 4808 CD23 44BC 8F28 E188 5E77 6845 104C H.Í#D% (á ^wkE.L
200 C8C1 D0B8 AD52 C3FF 3FE0 A2AD F219 26E0 ÈÁ0.-RÃy?àç-ò.&à
210 00AA 7768 061F 25FC 90DE D454 73E8 937D .èwk..%ü P0T5è }
220 F909 3923 5A3A 46BE 5F15 523C E0BE 05E7 ù.9#Z:F%_.R<à%ç
230 CEAE 1658 F4D5 A520 0DCA E67F C817 FEE3 i°.X00% .ÈæĪ E.pã
240 ADEB 17FE 4D0D 18A2 FB0E A038 298F FFDD -è.βM..çú. 8) ýÝ
250 D004 8891 B5C2 C007 CFC1 7C42 7E05 505D 0. μÅÀ.ĪÁ|B~.P]
260 6396 2C4D 49A6 66D6 59B0 14D2 0A3C 9A04 c ,MI|f0Y°.ò.< .
270 F0F8 9172 A234 B763 0553 37FC 004A B197 0ø rç4·c.S7ü.J±
280 A700 A021 61E7 D6F4 303C 9C27 334E 0773 $ .!ac000< '3N.s
290 CA7C E87C D1C5 90A0 2AD1 51C2 FC9A 9E93 È|è|ŇÅ *ŇQÅü
2A0 9A31 2A25 F727 E5F5 F227 FA27 A396 1726 1*%+'â00'ú'ε .&
2B0 0480 2DC4 ADA6 84CF 639C 1BAF 67E1 5BEB .°-Å-| Īc ."gá[è
2C0 2228 0F94 ACAC F945 6A61 63EB 845A 2E9B "(. -üEjacè Z.
2D0 B6ED 5ECE FC11 1A60 3A47 200D 9574 8353 ¶i^Īü..':g . t s
2E0 1167 F851 E1D3 6109 CEB0 8AC0 98D1 D5A2 .g0Qá0a.Ī° Å Ň0ç
2F0 C5E3 F75A 88F4 ECF6 0FBE 993B AE11 7A64 Åã÷Z.0i0.X ;0;izd
300 75E6 75EA D710 5648 DE59 7855 8258 DEF2 uæuèx.VHPYxU Xpò
310 2B6D 11EA 00B8 8189 C0A0 E859 C20D 4ACC +m.è. Å èYÅ.JĪ
320 1462 8FF0 897A 87C6 B27C 1822 161F B28B .b 0 z æ²|."..²
330 D46E 3E9F 797A A151 4A73 D103 778A 7661 0n> yz;QJ5Ň.w va
340 2657 2EB3 F656 14F3 7D17 A4B2 3738 8F23 &W.³0V.0}.M²78 #
350 EF7F 57FC 11F0 B44B EA30 4A66 96FC EFE9 ĪĪWü.ð'Kè0Jf üiÉ
360 9B97 C2C3 4332 7CEF 8C54 8C97 CC87 5441 ÅÃC2|Ī T Ī·TA
370 31C3 86D0 FE45 A71F 1121 E84E 7C49 FC34 1Ī 0pE$..!èN|Iü4
```

Digitální podepsání dokumentu

- Vytvoření kopie podepisovaného dokumentu
- Zahashování kopie dokumentu (SHA, MD5, ...)
- Zašifrování hashe (j) soukromým klíčem (d) autora: $k = j^d \bmod n$
- Podpis k je přiložen k podepsanému dokumentu

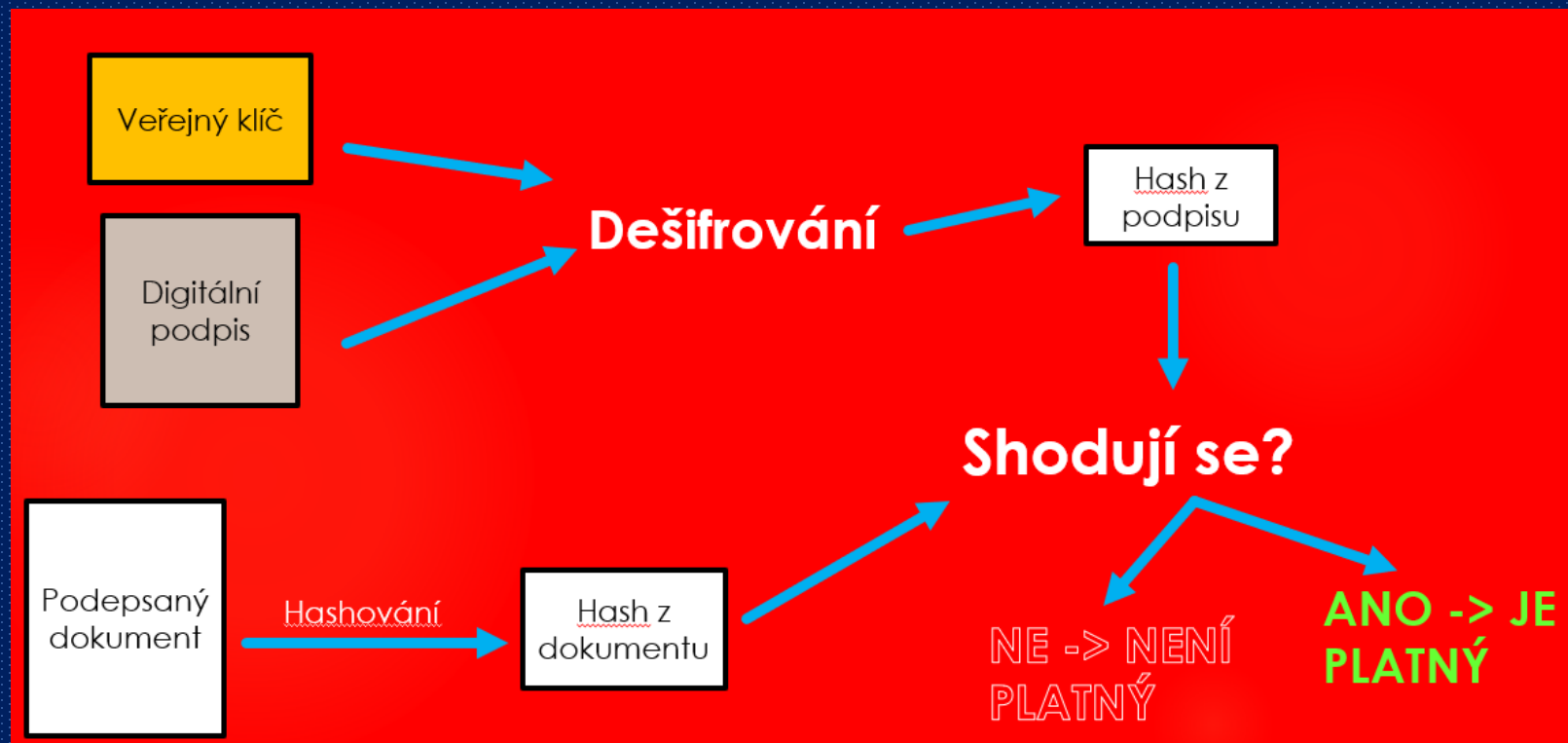
Digitální podepsání dokumentu



Ověření podepsaného dokumentu

- Podpis je zahashován stejnou funkcí jako při podepisování
 - Výsledek je hash přijatého dokumentu m
- Dešifrování podpisu (k) veřejným klíčem (e) autora: $j = k^e \bmod n$
 - j je hash kopie původního dokumentu
- Pokud se j a m shodují, s dokumentem se od podepsání nic nestalo.
- Pokud se j a m neshodují, dokument byl změněn a není důvěryhodný.

Ověření podepsaného dokumentu



Odkazy

- <https://is.muni.cz/th/tk3wj/thesis.pdf>
- https://is.ambis.cz/th/wpg59/DP_nastroje_pro_generovani_klicu.pdf
- https://knihy.nic.cz/files/edice/bajecny_svet_elektronickeho_podpisu_cznic.pdf