Při podpisu neznámé zprávy s využitím schématu RSASSA-PKCS1-v1_5 (viz PKCS#1) došlo k chybě při výpočtu podepisovací transformace RSASP1 (viz PKCS#1). K výpočtu byla použita Čínská věta o zbytku, chyba zasáhla právě jen parciální hodnotu podpisu modulo p, tj. hodnotu označovanou dle popisu v PKCS#1 jako s_1. Signatář později zjistil, že vypočtený podpis je neplatný, a nechal tutéž zprávu podepsat znovu. Nyní už vše proběhlo bez chyb. Nalezněte soukromý klíč signatáře, máte-li dán veřejný modul n, veřejný exponent e, hodnotu chybného podpisu f a hodnotu správného podpisu s:

In[43]:=
```
n =
 143 439 281 935 793 709 829 883 511 119 512 297 318 347 597 781 777 879 206 016 778 171 534 720 301 ⋱
  126 138 047 071 671 599 318 397 710 025 065 932 294 231 888 139 238 578 615 677 641 709 345 935 ⋱
  975 961 129 727 859 596 609 343 289 124 965 796 285 308 717 120 051 606 006 794 321 837 387 662 ⋱
  808 710 892 762 405 359 764 253 183 416 603 706 120 250 336 984 377 143 647 112 873 468 386 573 ⋱
  559 510 267 301 025 317

e = 2 ^ 16 + 1

f =
 71 251 176 378 222 026 591 825 270 924 710 333 598 755 025 600 583 408 398 417 673 044 948 036 838 ⋱
  605 203 199 365 453 395 684 541 835 766 338 661 162 672 639 861 182 656 220 165 947 252 131 425 ⋱
  810 938 132 667 168 370 928 457 399 579 218 032 946 166 229 495 635 857 434 396 515 864 365 919 ⋱
  188 222 925 205 058 641 667 971 268 925 279 334 818 704 393 729 730 175 259 569 121 845 705 737 ⋱
  661 313 402 980 864 137

s =
 15 223 702 582 445 980 286 808 606 927 407 147 872 606 816 408 515 094 671 195 941 573 747 873 776 ⋱
  542 763 859 988 851 309 420 835 589 410 131 772 963 096 153 108 282 509 175 871 696 342 163 196 ⋱
  550 032 899 522 429 025 717 395 838 274 305 099 296 786 258 069 032 517 578 628 430 962 210 476 ⋱
  221 001 719 559 330 646 207 213 315 978 859 400 699 157 086 660 962 631 721 005 185 511 377 251 ⋱
  893 703 145 230 857 109
```

Out[43]=
```
143 439 281 935 793 709 829 883 511 119 512 297 318 347 597 781 777 879 206 016 778 171 534 720 301 ⋱
 126 138 047 071 671 599 318 397 710 025 065 932 294 231 888 139 238 578 615 677 641 709 345 935 975 ⋱
 961 129 727 859 596 609 343 289 124 965 796 285 308 717 120 051 606 006 794 321 837 387 662 808 710 ⋱
 892 762 405 359 764 253 183 416 603 706 120 250 336 984 377 143 647 112 873 468 386 573 559 510 267 ⋱
 301 025 317
```

Out[44]=
```
65 537
```

Out[45]= 71 251 176 378 222 026 591 825 270 924 710 333 598 755 025 600 583 408 398 417 673 044 948 036 838 ⋱.
605 203 199 365 453 395 684 541 835 766 338 661 162 672 639 861 182 656 220 165 947 252 131 425 810 ⋱.
938 132 667 168 370 928 457 399 579 218 032 946 166 229 495 635 857 434 396 515 864 365 919 188 222 ⋱.
925 205 058 641 667 971 268 925 279 334 818 704 393 729 730 175 259 569 121 845 705 737 661 313 402 ⋱.
980 864 137

Out[46]= 15 223 702 582 445 980 286 808 606 927 407 147 872 606 816 408 515 094 671 195 941 573 747 873 776 ⋱.
542 763 859 988 851 309 420 835 589 410 131 772 963 096 153 108 282 509 175 871 696 342 163 196 550 ⋱.
032 899 522 429 025 717 395 838 274 305 099 296 786 258 069 032 517 578 628 430 962 210 476 221 001 ⋱.
719 559 330 646 207 213 315 978 859 400 699 157 086 660 962 631 721 005 185 511 377 251 893 703 145 ⋱.
230 857 109

V dokumentaci PKCS1 si v kapitole popisující RSASP1 můžeme najít následující vztahy:

s1 = m^dp mod p
s2 = m^dq mod q
h = (s1 - s2) * qinv mod p
s = s2 + q * h
s = s2 + ((s1 - s2) * qinv mod p) * q
f = s2 + ((f1 - s2) * qinv mod p) * q,

z čehož můžeme odvodit, že s-f = ((s1 - f1) * qinv mod p) * q. Vidíme, že výraz (s-f) by měl být dělitelný hodnotou q. Stejně tak modul n, který je definován jako p*q, by měl být dělitelný hodnotou q. GCD(s-f, n) by měl vrátit hodnotu q:

In[47]:=
```
q = GCD[s - f, n]
```

Out[47]= 11 145 675 583 776 161 284 741 912 926 727 745 648 703 060 011 516 338 086 549 608 716 744 154 655 ⋱.
738 423 874 335 992 638 362 226 875 566 767 011 901 243 344 195 332 769 827 451 303 171 056 161 026 ⋱.
441 313

Další složky soukromého klíče můžeme spočítat následujícím způsobem:

In[48]:=
```
p = n / q
phiN = (p - 1) * (q - 1);
numberInversion[number_, modul_] := ExtendedGCD[number, modul][[2, 1]];
d = numberInversion[e, phiN];
dp = Mod[d, p - 1]
dq = Mod[d, q - 1]
qinv = numberInversion[q, p]
```

Out[48]= 12 869 500 898 140 837 397 706 923 413 079 199 173 469 904 660 586 509 801 920 841 064 317 993 770 ⋱.
622 112 121 326 933 954 966 860 024 587 236 575 663 939 092 182 686 452 690 201 655 411 641 582 708 ⋱.
669 509

Out[52]= 11 803 604 520 901 896 564 364 640 728 699 476 373 927 743 095 399 461 642 792 008 110 458 066 245 ⋱.
911 844 263 558 610 755 742 603 250 345 823 020 989 421 470 192 549 246 757 638 147 994 848 160 505 ⋱.
293 429

Out[53]= 8 848 581 726 717 330 235 517 672 911 144 004 243 435 314 591 745 045 861 775 426 728 904 258 155 516 ⋱.
276 213 157 478 935 166 191 072 764 070 488 872 265 913 888 080 992 631 983 327 036 484 002 291 922 ⋱.
753

Out[54]= 5 026 835 150 067 583 972 020 801 402 186 043 934 621 540 841 569 760 878 519 113 653 182 701 347 598 ⋱.
328 017 405 215 298 044 810 415 161 553 104 166 360 627 379 921 882 593 749 815 857 032 934 461 149 ⋱.
556

Předpokládejme, že šestice SK = (n,p,q,dp,dq,qinv) by mohla představovat soukromý klíč signatáře. Nyní tento výsledek bude třeba ověřit. Nejprve můžeme ověřit základní vlastnosti RSA-CRT:

In[55]:=
```
Mod[e * dp, p - 1] == 1
Mod[e * dq, q - 1] == 1
```

Out[55]= True

Out[56]= True

Dále ověřme, že platí principy v dokumentaci PKCS1 v kapitolách RSAVP1 a RSASP1. Dle kapitoly RSAVP1 získáme šifrovanou reprezentaci zprávy m následujícím způsobem:

m = s^e mod n.

V kapitole RSASP1 jsou pak uvedeny vztahy, pomocí kterých lze vypočítat podpis

k dané šifrované reprezentaci zprávy m a soukromému klíči SK:

In[57]:=
```
m = Mod[s^e, n];
s1 = PowerMod[m, dp, p];
s2 = PowerMod[m, dq, q];
h = Mod[(s1 - s2) * qinv, p];
s == s2 + q * h
```

Out[61]=
```
True
```

Šestice SK = (n,p,q,dp,dq,qinv) tedy tvoří soukromý klíč signatáře.