DSA - dvojí použití NONCE

Kryptografický modul provádějící výpočet podpisů algoritmem DSA byl napaden škodlivým programem. Ten způsobil, že byly vygenerovány dva podpisy dvou různých zpráv za použití stejné hodnoty NONCE k. Vypočtěte hodnotu soukromého klíče, máte-li dány veřejné parametry (p, q, g), veřejný klíč y, zprávy m_1, m_2 a podpisy (r_1, s_1) a (r_2, s_2):

In[67]:=
```
p =
   130 858 654 869 791 629 821 164 827 405 704 486 808 484 325 400 695 017 176 436 089 171 363 953 ⋱
    174 803 169 341 783 555 373 215 075 614 114 465 991 900 855 153 261 492 152 633 662 438 773 188 ⋱
    376 262 979 282 101 753 394 454 977 993 579 816 854 383 830 900 528 351 206 089 343 265 102 338 ⋱
    373 900 869 810 884 532 342 186 375 732 537 448 146 335 182 616 800 945 419 546 009 892 443 656 ⋱
    248 994 289 078 702 932 401;

q = 1 145 453 138 964 420 393 547 388 172 384 121 951 637 470 359 533;
g =
   4 510 475 759 927 193 526 244 850 661 638 601 201 466 195 136 403 848 318 403 359 059 899 867 868 ⋱
    318 147 275 934 379 724 895 322 117 241 223 218 798 069 129 765 949 195 037 342 214 140 393 033 ⋱
    814 169 823 170 684 197 166 558 267 035 082 959 568 504 164 187 769 201 853 006 016 871 456 716 ⋱
    631 831 496 741 971 210 395 589 377 317 000 612 633 487 892 357 425 274 282 531 110 618 387 991 ⋱
    431 638 379 437 562 001;
m1 = "IOU $1000";
m2 = "Merry Christmas";
r = r1 = r2 = 916 128 381 002 192 237 330 415 624 031 916 695 461 722 389 304;
s1 = 1 016 140 177 410 528 212 949 844 490 506 968 808 343 879 600 370;
s2 = 767 135 282 992 918 681 484 216 676 594 223 285 185 365 265 436;
```

Nejprve je potřeba zahashovat obě zprávy. Pro tuto úlohu byla zvolena hashovací funkce SHA-1, nicméně je možné

použít libovolnou hashovací funkci:

In[75]:=
```
hm1 = Hash[m1, "SHA"]
hm2 = Hash[m2, "SHA"]
```

Out[75]= 1 121 674 975 390 587 548 442 137 500 973 361 632 322 358 316 031

Out[76]= 1 346 228 819 325 514 031 437 030 502 708 334 465 394 093 600 592

Víme, že pro podepisování platí (s1 = k^-1 * (hm1 + x * r)) a analogicky (s2 = k^-1 * (hm2 + x * r)). Funkce Solve najde snadno řešení:

In[77]:=
```
solution =
 Solve[{s1 == kk^-1 * (hm1 + xx * r), s2 == kk^-1 * (hm2 + xx * r)}, {kk, xx}, Modulus → q]
solveK = kk /. solution[[1]];
solveX = xx /. solution[[1]];
```

Out[77]= {{kk → 290 906 610 810 690 179 972 018 179 239 952 193 088 672 167 188,
xx → 555 336 883 567 305 608 284 725 219 102 191 211 489 862 726 405}}

Pokud bychom však nechtěli použít funkci Solve, můžeme si ze soustavy rovnic v předchozím bodě odvodit (k = ((hm1 - hm2) / (s1 - s2)) mod q) a také (x = ((k * s1 - hm1) * r^-1) mod q):

In[80]:=
```
k = Mod[PowerMod[s1 - s2, -1, q] * (hm1 - hm2), q]
x = Mod[(k * s1 - hm1) * PowerMod[r, -1, q], q]
k == solveK
x == solveX
```

Out[80]= 290 906 610 810 690 179 972 018 179 239 952 193 088 672 167 188

Out[81]= 555 336 883 567 305 608 284 725 219 102 191 211 489 862 726 405

Out[82]= True

Out[83]= True

Tím získáme soukromý klíč x =

55533688356730560828472521910219121148986272640 5.