een RSA-sleutelpaar

voorbeeld uit het boek

```
p = 239 635 170 197;
q = 856 802 627 729;
n = p q
d = 9587;
e = PowerMod[d, -1, (p - 1) (q - 1)]
```

```
205 320 043 521 075 746 592 613
```

```
70 760 135 995 620 281 241 019
```

twee willekeurige priemgetallen van 12 cijfers en hun product (de modulus)

```
p = RandomPrime[{10^11, 10^12}];
q = RandomPrime[{10^11, 10^12}];
n = p q
```

een kleine prive-exponent en de bijbehorende publieke exponent

```
d = RandomPrime[{9 × 10^3, 10^4}];
e = PowerMod[d, -1, (p - 1) (q - 1)]
```

versleutelen en ontsleutelen

een willekeurige boodschap

```
m = 12 345 678 901 234 567 890;
```

versleuteling

```
c = PowerMod[m, e, n]
```

```
157 155 551 477 630 030 243 615
```

ontsleuteling

```
PowerMod[c, d, n]
```

```
12 345 678 901 234 567 890
```

de methode van Mike Wiener

de kettingbreuk

```
cf = ContinuedFraction[e/n]
```

```
{0, 2, 1, 9, 6, 54, 5911, 1, 5, 1, 1, 3, 1, 2, 5, 3, 1, 3,
 1, 1, 2, 13, 1, 4, 5, 1, 2, 3, 11, 1, 1, 1, 1, 4, 17, 26, 1, 1, 10, 4}
```

het grootste wijzergetal en de bijbehorende convergent

```
pos = Position[cf, Max[cf]][[1, 1]]
cv = Convergents[e/n][[pos - 1]]
```

```
7
```

$$\frac{3304}{9587}$$

de geheimen lekken: *d*, *r* = *p* + *q*

```
k = Numerator[cv];
dd = Denominator[cv]
r = n + 1 - (e dd - 1)/k
```

```
9587
```

```
1 096 437 797 926
```

en de priemfactoren

$$pp = \frac{r + \sqrt{r^2 - 4n}}{2}$$

$$qq = \frac{r - \sqrt{r^2 - 4n}}{2}$$

```
856 802 627 729
```

```
239 635 170 197
```

controle

```
pp qq
n
```

```
205 320 043 521 075 746 592 613
```

```
205 320 043 521 075 746 592 613
```

de methode van Boneh en Durfee

een polynoom met een klein nulpunt

```
f[x_, y_] := x y - (n + 1) x - 1;
f[x, y]
X = 10^4;
Y = 10^12;
```

```
-1 - 205 320 043 521 075 746 592 614 x + x y
```

andere polynomen met hetzelfde nulpunt (mod e^2)

```
ma = {e^2 {1, 0, 0, 0, 0, 0, 0, 0, 0},
    e^2 {0, X, 0, 0, 0, 0, 0, 0, 0}, e {-1, -(n + 1) X, X Y, 0, 0, 0, 0, 0, 0},
    e^2 {0, 0, 0, X^2, 0, 0, 0, 0, 0}, e {0, -X, 0, -(n + 1) X^2, X^2 Y, 0, 0, 0, 0},
    {1, 2 (n + 1) X, -2 X Y, (n + 1)^2 X^2, -2 (n + 1) X^2 Y, X^2 Y^2, 0, 0, 0},
    e^2 {0, 0, 0, 0, 0, 0, Y, 0, 0}, e {0, 0, -(n + 1) X Y, 0, 0, 0, -Y, X Y^2, 0},
    {0, 0, 2 (n + 1) X Y, 0, (n + 1)^2 X^2 Y, -2 (n + 1) X^2 Y^2, Y, -2 X Y^2, X^2 Y^3}};
pol = ma.{1, x / X, x y / (X Y), x^2 / X^2, x^2 y / (X^2 Y), x^2 y^2 / (X^2 Y^2), y / Y, x y^2 / (X Y^2), x^2 y^3 / (X^2 Y^3)};
pol
```

```
{5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361,
 5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361 x, -70 760 135 995 620 281 241 019 -
  14 528 474 202 177 994 648 990 852 457 119 298 572 539 233 666 x + 70 760 135 995 620 281 241 019 x y,
 5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361 x^2, -70 760 135 995 620 281 241 019 x -
  14 528 474 202 177 994 648 990 852 457 119 298 572 539 233 666 x^2 + 70 760 135 995 620 281 241 019 x^2 y,
 1 + 410 640 087 042 151 493 185 228 x + 42 156 320 271 496 438 664 825 153 611 854 080 631 279 352 996 x^2 -
  2 x y - 410 640 087 042 151 493 185 228 x^2 y + x^2 y^2,
 5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361 y, -70 760 135 995 620 281 241 019 y -
  14 528 474 202 177 994 648 990 852 457 119 298 572 539 233 666 x y + 70 760 135 995 620 281 241 019 x y^2,
 y + 410 640 087 042 151 493 185 228 x y + 42 156 320 271 496 438 664 825 153 611 854 080 631 279 352 996 x^2 y -
  2 x y^2 - 410 640 087 042 151 493 185 228 x^2 y^2 + x^2 y^3}
```

polynomen met kleine coefficienten met hetzelfde nulpunt (mod e^2)

```
mared = LatticeReduce[ma];
pol =
  mared.{1, x / X, x y / (X Y), x^2 / X^2, x^2 y / (X^2 Y), x^2 y^2 / (X^2 Y^2), y / Y, x y^2 / (X Y^2), x^2 y^3 / (X^2 Y^3)};
pol
```

```
{10 916 416 + 23 938 342 240 568 299 824 x + 13 123 451 626 123 824 178 283 662 335 009 x^2 - 21 832 832 x y -
   23 938 342 240 568 299 824 x^2 y + 10 916 416 x^2 y^2, 233 791 489 329 529 409 220 326 776 +
   256 337 825 734 309 080 851 254 815 215 293 825 557 x - 233 791 489 329 529 409 220 326 776 x y,
 -34 244 998 536 - 4 334 885 573 961 565 702 235 x + 36 415 577 649 503 282 468 577 643 964 486 994 x^2 +
   68 489 997 072 x y + 4 334 885 573 961 565 702 235 x^2 y - 34 244 998 536 x^2 y^2,
 23 517 258 797 687 464 413 398 174 770 - 21 457 461 892 318 384 535 056 334 741 370 599 284 123 x +
   3 564 977 648 229 503 243 349 836 841 268 940 347 x^2 + y - 23 517 258 797 687 468 685 975 463 738 x y +
   3 902 776 845 615 498 674 375 400 x^2 y - 2 x y^2 + 4 272 577 288 968 x^2 y^2 + x^2 y^3,
 -45 137 346 686 686 502 676 224 576 964 + 41 325 719 826 265 032 354 140 092 404 145 191 951 096 x +
   4 741 616 008 913 032 689 629 796 938 210 150 475 x^2 - 34 y + 45 137 346 686 686 496 955 689 244 971 x y +
   5 208 123 192 485 652 359 241 654 x^2 y + 68 x y^2 + 5 720 535 331 993 x^2 y^2 - 34 x^2 y^3,
 5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361,
 -568 208 552 961 875 847 200 291 584 191 + 518 157 493 332 384 564 375 096 130 111 440 673 750 233 x +
   16 611 834 302 814 483 488 000 646 465 439 004 613 x^2 + 40 y + 568 208 552 961 875 827 251 118 183 840 x y +
   18 204 202 995 633 378 121 308 511 x^2 y - 80 x y^2 + 19 949 173 400 351 x^2 y^2 + 40 x^2 y^3,
 492 516 336 178 036 541 098 089 106 725 632 322 862 501 701 -
   146 280 201 423 686 442 301 663 811 029 988 345 294 808 x -
   3 564 977 648 229 503 243 349 836 841 268 940 347 x^2 - 70 760 135 995 620 281 241 020 y -
   160 194 876 443 117 616 410 519 971 316 x y - 3 902 776 845 615 498 674 375 400 x^2 y +
   70 760 135 995 620 281 241 021 x y^2 - 4 272 577 288 968 x^2 y^2 - x^2 y^3,
 5 006 996 846 118 677 009 964 688 373 575 770 070 768 158 361 y}
```

kies er twee uit om een variable te elimineren

```
i1 = 1;
i2 = 4;
polres = Resultant[pol[[i1]], pol[[i2]], x]
```

```
319 740 082 398 573 494 562 823 358 738 339 540 091 171 137 748 790 641 691 384 324 158 292 265 877 228 024 +
   783 758 940 187 339 729 231 945 674 951 113 705 764 -
 583 234 330 307 451 084 031 670 803 175 852 133 125 161 864 721 525 462 561 772 731 357 584 695 265 054 440 +
   431 769 854 915 773 733 411 239 628 y +
 265 967 814 777 402 593 985 877 157 386 069 041 929 499 443 855 861 753 250 338 178 709 265 341 158 015 108 +
   360 554 754 859 489 y^2
```

nu weten we het geheime $r = p + q$

```
r = y /. Solve[polres == 0, y][[1]]
```

```
1 096 437 797 926
```

en dus de priemfactoren van *n*

$$pp = \frac{r + \sqrt{r^2 - 4\,n}}{2}$$

$$qq = \frac{r - \sqrt{r^2 - 4\,n}}{2}$$

```
856 802 627 729
```

```
239 635 170 197
```

controle

```
pp qq
n
```

```
205 320 043 521 075 746 592 613
```

```
205 320 043 521 075 746 592 613
```

factoriseren met een hint

we weten nu (ruim) de bovenste helft van *p* en *q*

$$p0 = 10^5 \text{ Round}\left[\frac{p}{10^5}\right]$$

$$q0 = 10^5 \text{ Round}\left[\frac{q}{10^5}\right]$$

```
239 635 200 000
```

```
856 802 600 000
```

een polynoom *f* met een klein nulpunt, en de modulus *R*

```
f[x_, y_] := (p0 q0 - n) + q0 x + p0 y + x y;
f[x, y]
X = 10^5;
W = 10^17;
R = W X^4
```

```
18 890 444 253 407 387 + 856 802 600 000 x + 239 635 200 000 y + x y
```

```
10 000 000 000 000 000 000 000 000 000 000 000 000 000
```

en een variant *f1* met hetzelfde nulpunt (mod *R*)

```
c = PowerMod[p0 q0 - n, -1, R];
a = Mod[q0 c, R];
b = Mod[p0 c, R];
f1[x_, y_] := 1 + a x + b y + c x y;
f1[x, y]
```

```
1 + 8 484 786 446 172 314 818 140 725 024 439 800 000 x +
  9 007 801 209 970 408 465 039 807 616 569 600 000 y + 4 773 582 929 298 399 405 471 192 915 168 722 323 x y
```

andere polynomen met hetzelfde nulpunt (mod R)

```
ma = {X^4 {1, a X, b X, c X^2, 0, 0, 0, 0, 0}, X^4 {0, 1, 0, b X, a X, 0, c X^2, 0, 0},
    X^4 {0, 0, 1, a X, 0, b X, 0, c X^2, 0}, X^2 {0, 0, 0, 1, 0, 0, a X, b X, c X^2},
    X^2 R {0, 0, 0, 0, 1, 0, 0, 0, 0}, X^2 R {0, 0, 0, 0, 0, 1, 0, 0, 0}, X^3 R {0, 0, 0, 0, 0, 0, 1, 0, 0},
    X^3 R {0, 0, 0, 0, 0, 0, 0, 1, 0}, X^4 R {0, 0, 0, 0, 0, 0, 0, 0, 1}};
pol = ma.{1, x / X, y / X, x y / X^2, x^2 / X^2, y^2 / X^2, x^2 y / X^3, x y^2 / X^3, x^2 y^2 / X^4};
pol
```

```
{100 000 000 000 000 000 000 + 848 478 644 617 231 481 814 072 502 443 980 000 000 000 000 000 000 000 000 x +
   900 780 120 997 040 846 503 980 761 656 960 000 000 000 000 000 000 000 000 y +
   477 358 292 929 839 940 547 119 291 516 872 232 300 000 000 000 000 000 000 x y,
 1 000 000 000 000 000 x + 8 484 786 446 172 314 818 140 725 024 439 800 000 000 000 000 000 000 x^2 +
   9 007 801 209 970 408 465 039 807 616 569 600 000 000 000 000 000 000 x y +
   4 773 582 929 298 399 405 471 192 915 168 722 323 000 000 000 000 000 x^2 y,
 1 000 000 000 000 000 y + 8 484 786 446 172 314 818 140 725 024 439 800 000 000 000 000 000 000 x y +
   9 007 801 209 970 408 465 039 807 616 569 600 000 000 000 000 000 000 y^2 +
   4 773 582 929 298 399 405 471 192 915 168 722 323 000 000 000 000 000 x y^2,
 x y + 8 484 786 446 172 314 818 140 725 024 439 800 000 x^2 y +
   9 007 801 209 970 408 465 039 807 616 569 600 000 x y^2 +
   4 773 582 929 298 399 405 471 192 915 168 722 323 x^2 y^2,
 10 000 000 000 000 000 000 000 000 000 000 000 000 x^2, 10 000 000 000 000 000 000 000 000 000 000 000 000 y^2,
 10 000 000 000 000 000 000 000 000 000 000 000 000 x^2 y,
 10 000 000 000 000 000 000 000 000 000 000 000 000 x y^2,
 10 000 000 000 000 000 000 000 000 000 000 000 000 x^2 y^2}
```

polynomen met kleine coefficienten met hetzelfde nulpunt (mod e^2)

```
mared = LatticeReduce[ma];
pol = mared.{1, x / X, y / X, x y / X^2, x^2 / X^2, y^2 / X^2, x^2 y / X^3, x y^2 / X^3, x^2 y^2 / X^4};
pol
```

```
{-18 890 444 253 407 387 x y - 856 802 600 000 x^2 y - 239 635 200 000 x y^2 - x^2 y^2,
 -18 890 444 253 407 387 000 000 000 000 000 y - 819 841 589 567 594 330 511 023 832 x y +
   1 676 418 479 750 686 400 000 x^2 y - 239 635 200 000 000 000 000 000 000 y^2 +
   468 868 816 313 292 800 000 x y^2 + 1 956 598 264 x^2 y^2, -18 890 444 253 407 387 000 000 000 000 000 x -
   856 802 600 000 000 000 000 000 000 x^2 - 229 297 726 029 917 110 231 828 449 x y +
   468 869 634 072 129 800 000 x^2 y + 131 136 282 931 449 600 000 x y^2 + 547 232 973 x^2 y^2,
 1 889 044 425 340 738 700 000 000 000 000 000 000 + 85 680 260 000 000 000 000 000 000 000 000 x +
   23 963 520 000 000 000 000 000 000 000 000 y + 95 692 978 710 223 115 764 x y - 195 350 992 800 000 x^2 y -
   54 636 825 600 000 x y^2 - 228 x^2 y^2, -10 000 000 000 000 000 000 000 000 000 000 000 000 000,
 169 680 134 478 818 600 000 000 000 000 000 000 - 51 639 508 297 963 773 000 000 000 000 000 x -
   19 365 400 000 000 000 000 000 000 x^2 + 309 953 462 001 512 912 000 000 000 000 000 y -
   289 712 151 585 302 200 751 342 229 x y - 1 087 777 678 808 314 200 000 x^2 y -
   453 324 800 000 000 000 000 000 000 y^2 + 6 173 091 419 402 361 600 000 x y^2 - 12 886 341 244 877 967 x^2 y^2,
 3 485 355 883 984 502 400 000 000 000 000 000 000 - 24 367 047 946 256 727 000 000 000 000 000 x -
   156 534 600 000 000 000 000 000 000 x^2 - 104 951 632 712 382 199 000 000 000 000 000 y +
   198 177 674 128 924 058 224 800 200 x y - 7 010 473 528 072 040 000 000 x^2 y -
   484 550 400 000 000 000 000 000 000 y^2 + 23 503 326 169 393 920 000 000 x y^2 + 124 858 545 954 864 600 x^2 y^2,
 1 960 629 837 475 469 000 000 000 000 000 000 000 + 21 089 826 456 437 862 000 000 000 000 000 x +
   59 707 600 000 000 000 000 000 000 x^2 - 148 735 532 211 905 501 000 000 000 000 000 y -
   862 518 419 772 967 357 233 114 785 x y - 31 999 003 722 443 000 000 x^2 y +
   3 010 630 400 000 000 000 000 000 000 y^2 + 6 913 651 815 258 464 000 000 x y^2 - 189 290 254 050 845 555 x^2 y^2,
 -2 872 084 985 228 350 400 000 000 000 000 000 000 + 18 866 216 637 190 144 000 000 000 000 000 x -
   318 668 800 000 000 000 000 000 000 x^2 - 120 398 469 532 090 930 000 000 000 000 000 y +
   889 449 646 625 676 285 621 948 168 x y - 6 250 202 911 163 713 600 000 x^2 y -
   1 873 728 000 000 000 000 000 000 000 y^2 + 15 335 743 909 164 492 800 000 x y^2 - 385 023 685 309 445 736 x^2 y^2}
```

kies er een uit om samen met *f* een variable te elimineren

```
ii = 7;
polres = Resultant[pol[[ii]], f[x, y], x]
```

$$2\,897\,167\,807\,427\,494\,091\,706\,540\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000 - 79\,169\,533\,269\,942\,837\,710\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,y - 804\,717\,577\,770\,410\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,y^2 - 4\,097\,859\,190\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,y^3 + 7\,170\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,y^4$$

nu weten we het geheime *r* = *p* + *q*

```
r = y /. Solve[polres == 0, y][[1]]
```

$$27\,729$$

en dus de priemfactoren van *n*

```
qq = q0 + r
pp = n / qq
```

$$856\,802\,627\,729$$

$$239\,635\,170\,197$$

RSA met CRT

een CRT-sleutel

```
e = RandomPrime[{10^22, (p - 1) (q - 1) - 1}]
d = PowerMod[e, -1, (p - 1) (q - 1)];
dp = Mod[d, p - 1];
dq = Mod[d, q - 1];
u = PowerMod[p, -1, q];
```

```
64 840 917 519 105 238 937 317
```

een willekeurige boodschap

```
m = 12 345 678 901 234 567 890;
```

versleuteling

```
c = PowerMod[m, e, n]
```

```
52 351 645 516 689 791 464 130
```

ontsleuteling met de CRT-sleutel

```
mp = PowerMod[c, dp, p];
mq = PowerMod[c, dq, q];
Mod[mp + p u (mq - mp), n]
```

```
12 345 678 901 234 567 890
```

de magnetron-aanval

in de magnetron verandert in *dp* een willekeurig cijfer

```
dpfout = dp + 10^Random[Integer,{0,9}];
dpfout - dp
```

```
10 000
```

een willekeurige boodschap

```
m = 12 345 678 901 234 567 890;
```

versleuteling

```
c = PowerMod[m, e, n]
```

```
52 351 645 516 689 791 464 130
```

foute ontsleuteling met de veranderde CRT-sleutel

```
mpfout = PowerMod[c, dpfout, p];
mq = PowerMod[c, dq, q];
mfout = Mod[mpfout + p u (mq - mpfout), n]
```

```
161 478 381 379 682 538 006 385
```

dit lekt de priemfactoren

```
pp = GCD[mfout - m, n]
     n
qq = --
     pp
```

```
856 802 627 729
```

```
239 635 170 197
```