Choose large integers a,k,n

In[•]:=
```
a = 328 499 784 359 823 465 234 562 564 983 253;
k = 232 758 273 589 326 529 386 529 356 239 856 235 896 592 556 995 831;
n = 123 365 648 235 623 489 567 243 105 687 023 672 304 624 367 534 687;

a^k
```

Out[•]=

70 345 588 133 872 290 045 290 125 821 352 538 038 992 740 993 177 920 709 735 360 239 667 341 821 088 098 ⁖
712 698 785 639 942 708 069 814 324 535 367 842 372 126 605 620 082 917 548 410 779 808 743 913 808 347 ⁖
012 380 542 296 828 112 773 706 364 563 816 317 257 492 999 453 918 151 034 909 823 598 334 650 092 314 ⁖
327 428 481 294 497 717 900 539 137 700 019 768 398 882 759 781 016 158 039 900 993 545 600 175 290 808 ⁖
578 569 773 394 066 221 661 885 131 761 378 829 032 029 804 533 697 649 387 678 868 331 733 539 814 302 ⁖
989 364 165 396 908 995 049 188 248 091 805 295 981 111 450 818 546 128 598 212 062 482 804 729 333 604 ⁖
095 916 695 187 113 898 391 469 913 618 212 984 872 470 564 129 897 752 090 428 069 488 566 324 746 507 ⁖
940 095 801 672 065 419 784 826 463 982 713 326 491 910 696 526 593 422 934 663 591 191 652 053 513 714 ⁖
005 265 077 657 311 719 396 599 927 666 974 467 161 709 940 257 739 176 453

```
Mod[a^k, n]
```

Out[•]=

65 107 987 613 474 905 458 022 517 482 890 798 498 749 246 295 124

```
PowerMod[a, k, n]
```

Out[•]=

121 571 656 183 179 059 547 369 174 671 034 003 242 518 922 084 536

```
FactorInteger[12 461 932 578 235 723 985 729 587 329 853 252 549]
```

Out[•]=

{{19, 1}, {11 378 953 134 301, 1}, {57 640 732 024 026 116 259 571, 1}}

Smallest open factoring challenge (270 decimal digits)

In[•]:=
```
RSA270 =
  233 108 530 344 407 544 527 637 656 910 680 524 145 619 812 480 305 449 042 948 611 968 495 918 245 135 ⁖
   782 867 888 369 318 577 116 418 213 919 268 572 658 314 913 060 672 626 911 354 027 609 793 166 341 626 ⁖
   693 946 596 196 427 744 273 886 601 876 896 313 468 704 059 066 746 903 123 910 748 277 606 548 649 151 ⁖
   920 812 699 309 766 587 514 735 456 594 993 207;


FactorInteger[RSA270]

p = NextPrime[RSA270]
```

Out[•]=

233 108 530 344 407 544 527 637 656 910 680 524 145 619 812 480 305 449 042 948 611 968 495 918 245 135 782 ⁖
867 888 369 318 577 116 418 213 919 268 572 658 314 913 060 672 626 911 354 027 609 793 166 341 626 693 ⁖
946 596 196 427 744 273 886 601 876 896 313 468 704 059 066 746 903 123 910 748 277 606 548 649 151 920 ⁖
812 699 309 766 587 514 735 456 594 994 467

```
FactorInteger[p]
```

Out[•]=

```
{{233 108 530 344 407 544 527 637 656 910 680 524 145 619 812 480 305 449 042 948 611 968 495 918 245 135 ×
    782 867 888 369 318 577 116 418 213 919 268 572 658 314 913 060 672 626 911 354 027 609 793 166 341 626 ×
    693 946 596 196 427 744 273 886 601 876 896 313 468 704 059 066 746 903 123 910 748 277 606 548 649 151 ×
    920 812 699 309 766 587 514 735 456 594 994 467, 1}}
```

```
PowerMod[a, p - 1, p]
```

Out[•]=

```
1
```

```
PowerMod[a, RSA270 - 1, RSA270]
```

Out[•]=

```
53 667 377 849 585 559 331 921 772 593 613 385 080 253 944 626 904 000 111 644 874 409 184 090 353 741 914 ×
 451 569 879 770 059 987 239 966 658 107 989 476 670 375 707 058 834 428 020 967 895 809 450 481 612 013 ×
 437 131 661 287 564 787 439 478 401 167 674 419 109 734 842 113 829 644 324 922 142 059 919 282 118 397 ×
 135 461 443 606 289 302 091 083 532 997 723
```