

**p = RandomPrime[{10<sup>99</sup>, 10<sup>101</sup>}]**

51 873 745 306 824 941 949 225 039 866 838 738 001 999 251 081 489 699 \\  
673 154 292 047 922 112 543 489 211 103 758 960 880 667 054 567

**22 322 406 847 957 573 735 774 242 315 736 451 451 761 424 528 666 009 \\  
966 541 796 681 662 102 308 786 881 417 807 241 058 303 061 837**

22 322 406 847 957 573 735 774 242 315 736 451 451 761 424 528 666 009 \\  
966 541 796 681 662 102 308 786 881 417 807 241 058 303 061 837

**a = RandomPrime[{10<sup>41</sup>, 10<sup>42</sup>}]**

278 762 772 538 066 383 106 300 586 373 609 459 239 701

**SecretA = 1492**

**SecretB = 1962**

1492

1962

**SaysA = PowerMod[a, SecretA, p]**

11 077 274 045 198 182 377 010 526 459 946 013 503 639 285 114 609 118 \\  
485 162 128 713 617 494 144 165 052 583 677 437 840 555 324 669

**SaysB = PowerMod[a, SecretB, p]**

22 165 138 427 387 462 478 480 443 125 148 171 304 185 533 138 545 403 \\  
537 852 246 170 393 194 208 012 552 860 968 016 092 176 549 768

**PowerMod[SaysA, SecretB, p]**

14 010 407 514 952 118 918 417 276 800 274 552 856 969 723 459 993 639  
373 175 104 113 535 168 078 919 012 704 382 304 655 513 312 589

**PowerMod[SaysB, SecretA, p]**

14 010 407 514 952 118 918 417 276 800 274 552 856 969 723 459 993 639  
373 175 104 113 535 168 078 919 012 704 382 304 655 513 312 589

**PowerMod[SaysA, SecretB, p] - PowerMod[SaysB, SecretA, p]**

0