Diffie-Hellman Key Exchange Protocol

Alice and Bob are two parties communicating over an open channel (i.e. an insecure channel, such as a cellphone network, email server, or standard postal service that is subject to interception by a third party.) In order to preserve secrecy of their exchanges of information, they will use an encryption software package. This software requires the use of a secret numerical key without which encryption and decryption is impossible. So before secure communication can begin, Alice and Bob must obtain a shared secret key. The problem is how to achieve this over the open channel.

The following solution (the Diffie-Hellman protocol) requires that they first agree on a large prime p, which they choose at random. In practice, this prime can be chosen by Alice and transmitted to Bob over the open channel.

```
p=NextPrime[RandomInteger[{1,10^70}]]; Print["p = ",p]
```

p = 555 696 710 587 722 822 668 791 106 686 495 279 860 902 403 630 964 365 571 544 886 746 153

Next, they must agree on a large integer g between 1 and p, chosen randomly. This could be generated by either participant, and then sent to the other over the open channel (neither p nor g is secret):

```
g=RandomInteger[{1,p}]; Print["g = ",g]
```

g = 27 722 148 935 786 730 813 512 875 791 418 968 767 971 943 608 327 880 831 067 798 998 419

Alice randomly chooses a large integer a between 1 and p, known only to herself:

```
a=RandomInteger[{1,p}]; Print["a = ",a]
```

a = 363 593 814 354 106 009 568 251 647 233 089 870 363 436 100 598 843 256 488 193 686 332 296

She also computes g^a mod p, and she sends this value to Bob:

```
ga=PowerMod[g,a,p]; Print["ga = ",ga]
```

ga = 82 211 324 906 759 301 843 937 447 936 772 451 546 871 993 260 195 147 276 423 296 547 546

Likewise, Bob randomly chooses a large integer b between 1 and p, known only to himself:

```
b=RandomInteger[{1,p}]; Print["b = ",b]
```

b = 527 836 378 542 164 811 975 897 926 066 792 749 157 340 275 177 250 381 841 456 583 545 009

He also computes g^b mod p, and he sends this value to Alice:

```
gb=PowerMod[g,b,p]; Print["gb = ",gb]
```

gb = 81 114 173 369 403 480 235 002 497 014 517 101 108 201 500 092 132 759 546 341 546 747 915

Now both Alice and Bob have enough information to compute the secret key $g^{a\,b}$ mod p. Alice computes this value as

```
PowerMod[gb,a,p]
```

Out[•]=

537 034 467 538 939 032 131 952 159 496 373 649 279 012 745 507 681 122 128 847 852 903 099

and Bob determines exactly the same value as

```
PowerMod[ga,b,p]
```

Out[•]=

537 034 467 538 939 032 131 952 159 496 373 649 279 012 745 507 681 122 128 847 852 903 099

This secret key, known only to them, is used as the key for a publicly available symmetric key encryption algorithm which they both use.