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 = 8 082 467 080 689 718 678 699 615 622 403 236 192 972 094 057 761 178 393 307 684 311 913 327

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 = 3 566 804 667 389 994 587 885 383 802 949 881 921 138 268 369 967 757 820 428 111 570 907 842

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

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

a = 1 570 417 695 486 444 069 605 736 351 488 681 252 389 866 226 242 395 055 414 040 104 142 463

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

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

ga = 6 317 411 377 424 384 978 027 489 586 860 481 207 836 504 189 831 500 223 999 810 911 101 993

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

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

b = 7 837 020 047 583 632 876 237 503 864 728 381 735 842 409 313 852 043 440 830 226 024 548 262

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

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

gb = 6 357 185 211 658 756 834 578 530 708 705 729 821 088 832 336 488 995 754 964 052 001 474 471

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[•]=

6 772 842 581 890 757 305 240 311 067 357 512 254 092 998 353 404 973 929 426 209 569 180 456

and Bob determines exactly the same value as

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

Out[•]=

6 772 842 581 890 757 305 240 311 067 357 512 254 092 998 353 404 973 929 426 209 569 180 456

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