

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]
```

$p = 9\ 207\ 261\ 398\ 175\ 022\ 812\ 982\ 858\ 288\ 405\ 088\ 957\ 672\ 621\ 340\ 472\ 190\ 870\ 879\ 651\ 975\ 019\ 557$

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]
```

$g = 4\ 229\ 774\ 176\ 824\ 358\ 850\ 803\ 035\ 909\ 773\ 711\ 754\ 377\ 120\ 619\ 882\ 368\ 659\ 186\ 101\ 569\ 700\ 659$

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

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

$a = 3\ 797\ 827\ 269\ 684\ 878\ 512\ 029\ 681\ 296\ 193\ 270\ 522\ 090\ 479\ 347\ 204\ 192\ 431\ 956\ 015\ 254\ 661\ 991$

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

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

$ga = 980\ 236\ 606\ 478\ 400\ 964\ 451\ 595\ 550\ 176\ 458\ 266\ 291\ 620\ 859\ 390\ 490\ 615\ 224\ 393\ 939\ 861\ 923$

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

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

$b = 3\ 384\ 526\ 179\ 929\ 010\ 071\ 340\ 435\ 660\ 214\ 903\ 985\ 337\ 932\ 191\ 971\ 123\ 935\ 528\ 864\ 798\ 370\ 885$

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

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

```
gb = 8 469 829 967 632 309 326 858 122 719 632 598 104 300 134 398 809 335 764 545 932 904 030 483
```

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

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

Out[*]=

```
4 763 414 219 741 215 286 102 650 310 909 394 458 371 804 292 999 074 604 335 801 610 017 554
```

and Bob determines exactly the same value as

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

Out[*]=

```
4 763 414 219 741 215 286 102 650 310 909 394 458 371 804 292 999 074 604 335 801 610 017 554
```

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