Diffie–Hellman key exchange

**Diffie–Hellman key exchange**[[nb 1]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-1) is a method of securely exchanging cryptographic keys over a public channel

Diffie–Hellman key exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network.

The simplest and the original implementation[[2]](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-Diffie_1976-3) of the protocol uses the [multiplicative group of integers modulo](https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n) *p*, where *p* is [prime](https://en.wikipedia.org/wiki/Prime_number), and *g* is a [primitive root modulo](https://en.wikipedia.org/wiki/Primitive_root_modulo_n) *p*. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to *p*–1

|  |  |  |  |
| --- | --- | --- | --- |
| P | G | Private Key | Time taken to break |
| 610292520201647 | 5 | 2  1 | 10ns  12ns |
| 610292520201647 | 125 | 54  49 | 11ms  19 ms |
| 610292520201647 | 63456456 | -1  -1  default return statement | System could not calculate |
| 610292520201647 | 610292520201644 | SYSTEM CRASHED | SYSTEM COULD NOT HANDLEOVERLOAD |

We see that for small valus of the primitive root the hacker is able to easily break into the system

But for really large values the system cannot handle such large calculatons so this algoritm does not fail and let the hacker steal our information