Diffie–Hellman key exchange (DH) example (source: wikipedia)

The simplest and the original implementation[2] of the protocol uses the multiplicative group of integers modulo *p*, where *p* is prime, and *g* is a primitive root modulo *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. Here is an example of the protocol, with non-secret values in blue, and secret values in **red**.

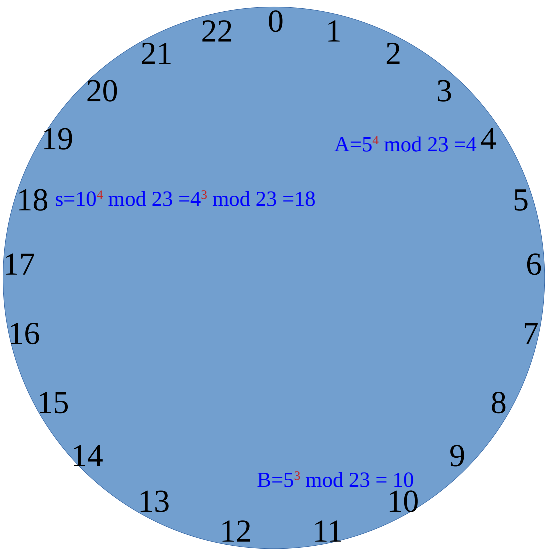
1. Alice and Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).

> *g* is a primitive root modulo *n* if for every integer *a* coprime to *n*, there is an integer *k* such that $g^k \equiv a \pmod n$. Such a value *k* is called the index or discrete logarithm of *a* to the base *g* modulo *n*. Note that g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n
> $k \rightarrow g^k \bmod n$
> $5^1 \bmod 23 = 5$; $5^2 \bmod 23 = 2$; $5^3 \bmod 23 = 10$; $5^4 \bmod 23 = 4$; $5^5 \bmod 23 = 20$;
> $5^6 \bmod 23 = 8$; $5^7 \bmod 23 = 17$; $5^8 \bmod 23 = 16$; $5^9 \bmod 23 = 11$; $5^{10} \bmod 23 = 9$;
> $5^{11} \bmod 23 = 22$; $5^{12} \bmod 23 = 18$; $5^{13} \bmod 23 = 21$; $5^{14} \bmod 23 = 13$; $5^{15} \bmod 23 = 19$;
> $5^{16} \bmod 23 = 3$; $5^{17} \bmod 23 = 15$; $5^{18} \bmod 23 = 6$; $5^{19} \bmod 23 = 7$; $5^{20} \bmod 23 = 12$;
> $5^{21} \bmod 23 = 14$; $5^{22} \bmod 23 = 1$;
> Hence:
> $1 = \log_5 5 \bmod 23$; $2 = \log_5 2 \bmod 23$; $3 = \log_5 10 \bmod 23$; $4 = \log_5 4 \bmod 23$; $5 = \log_5 20 \bmod 23$;
> $6 = \log_5 8 \bmod 23$; $7 = \log_5 17 \bmod 23$; ...
> $21 = \log_5 14 \bmod 23$; $22 = \log_5 1 \bmod 23$;
> Sorted out:
> 22, 2, 16, 4, 1, 18, 19, 6, 10, 3, 9, 20, 14, 21, 17, 8, 7, 12, 15, 5, 13, 11

2. Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p$
   - $A = 5^4 \bmod 23 = 4$
3. Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod p$
   - $B = 5^3 \bmod 23 = 10$
4. Alice computes $s = B^a \bmod p$
   - $s = 10^4 \bmod 23 = 18$
5. Bob computes $s = A^b \bmod p$
   - $s = 4^3 \bmod 23 = 18$
6. Alice and Bob now share a secret (the number 18).

Both Alice and Bob have arrived at the same values because under mod p,

Only *a* and *b* are kept secret. All the other values – p, g, $g^a \bmod p$, and $g^b \bmod p$ – are sent in the clear. The strength of the scheme comes from the fact that **$g^{ab} \bmod p = g^{ba} \bmod p$ take extremely long times to compute just from the knowledge of p, g, $g^a \bmod p$, and $g^b \bmod p$.** Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel.



a and *b* are kept secret. All the other values – p, g, $g^a \bmod p$, and $g^b \bmod p$ – are sent in the clear.

4 and *3* are kept secret. All the other values – *23*, *5*, $(5^4 \bmod 23) = 4$, and $(5^3 \bmod 23) = 10$ – are sent in the clear.