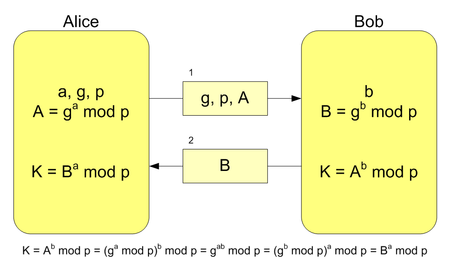
[](https://fa.m.wikipedia.org/wiki/%D9%BE%D8%B1%D9%88%D9%86%D8%AF%D9%87:Diffie-Hellman-Schl%C3%BCsselaustausch.png)

ایجاد و تبادل کلید رمز با پروتکل دیفی-هلمن

1. مقدار عدد اول دلخواه بزرگp (پیمانهٔ عمل ضرب) و مقدار محاسبه شده برای g میان دو طرف رد و بدل می‌شود.
2. هر یک از دو طرف یک عدد صحیح دلخواه(a, b) را به صورت پنهانی در نظر می‌گیرد.
3. هر یک از دو طرف با استفاده از عمل به توان رسانی پیمانه ای ومقادیر قبلی (p و g و مقدار پنهانی)یک مقدار جدید محاسبه کرده (A,B) و برای طرف مقابل ارسال می‌کند.
4. طرف اول با استفاده از مقادیر p و g و a و B، و طرف دوم با استفاده ازمقادیر p و g و b و A، و با همان عمل توان پیمانه‌ای مقدار جدیدی را محاسبه می‌کنند. مقدار جدید محاسبه شده -چنان‌که فرمول نشان می‌دهد- در دو طرف یکسان و همان کلید رمز مشترک است.

* مقادیر a و b و مقدار مشترک محاسبه شده، هرگز مستقیماً از کانال ارتباطی عبور نمی‌کنند. بقیهٔ مقادیر یعنی p و g و A و B از کانال ارتباطی عبور می‌کنند و برای دیگران قابل دسترسی هستند.
* دشواری حل مسئلهلگاریتم گسسته تضمین می‌کند که مقادیر a و b و مقدار کلید رمز مشترک، با داشتن مقدار اعداد دیگر در عمل قابل محاسبه نباشد.