تبادل کلید دیفی-هلمن از تعداد زیاد و محاسبات زیادی برای رمزنگاری استفاده می کند. این را می توان با نمودار نشان داده شده از یک تشبیه در زیر درک کرد.

فرض کنید دو نفر در مورد رنگ رنگی به نام آلیس و باب تصمیم می گیرند. ابتدا ، آنها در مورد یک رنگ تصادفی برای شروع توافق می کنند. فرض کنید آنها در مورد زرد به عنوان یک رنگ استاندارد تصمیم بگیرند.

هر کدام رنگ مخفی خود را انتخاب می کنند و انتخاب خود را فاش نمی کنند. بگذارید بگوییم آلیس قرمز را انتخاب می کند ، در حالی که باب آبی روشن را انتخاب می کند.

مرحله بعدی مخلوط کردن رنگ های مخفی توسط آلیس و باب ، با رنگ زرد است که به طور متقابل توافق شده است.

طبق نمودار ، آلیس رنگ نارنجی را انتخاب می کند در حالی که باب سراغ رنگ آبی تیره می رود.

پس از اتمام اختلاط ، نتیجه را برای طرف مقابل ارسال می کنند. آلیس آبی تیره دریافت می کند ، در حالی که باب رنگ نارنجی را دریافت می کند.

هرگاه نتیجه مخلوطی حاصل شد ، رنگ مخفی خود را به آن اضافه می کنند. آلیس آبی عمیق تر را می گیرد و رنگ قرمز مخفی را اضافه می کند ، در حالی که باب آبی عمیق پنهانی را به نارنجی دریافت کرده اضافه می کند. در پایان ، آنها دریافتند که همان رنگ را دریافت کرده اند که در اینجا قهوه ای است. این رنگ مشترک راز مشترک نامیده می شود.

با تعویض کلید Diffie-Hellman ، هر دو طرف نتیجه مشابهی را دریافت می کنند ، بدون اینکه رمز مشترک را از طریق کانال ارتباطی ارسال کنند. اگر برخی از دشمنان به تبادل نگاه کنند ، آنها فقط می توانند به رنگ زرد استاندارد و رنگهای مخلوط رد و بدل شده دسترسی پیدا کنند.

اجرای صحیح مبادله کلید Diffie-Hellman برای شکستن رمز و راز به زمان و منابع محاسباتی زیادی نیاز دارد.

این ساختار مبادله کلید دیفی-هلمن به دو طرف این امکان را می دهد تا از طریق اتصال ناامن ارتباط برقرار کنند و هنوز هم یک راز مشترک دارند که می تواند برای ساخت کلیدهای رمزگذاری برای ارتباطات آینده استفاده شود. راز مشترک کامل هرگز از طریق اتصال ارسال نمی شود. بنابراین ، مهاجمان نمی توانند آن را کنترل کنند. آلیس و باب هر دو عملیات مشابه را انجام می دهند اما به ترتیب متناوب اما با همان خروجی ارائه می شوند.