الگوریتم DHKE

پروتکل تبادل کلید دیفی-هلمن، یک پروتکل رمزنگاری است که با استفاده از آن، دو نفر یا دو سازمان، می‌توانند بدون نیاز به هر گونه آشنایی قبلی، یک کلید رمز مشترک ایجاد و آن را از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل نمایند. این پروتکل، اولین روش عملی مطرح شده برای تبادل کلید رمز در مسیرهای ارتباطی غیر امن است و مشکل تبادل کلید رمز در الگوریتم کلید متقارن را آسان می‌سازد .

این پروتکل، در سال ۱۹۷۶ توسط دو دانشمند رمزشناس به نام‌های ویتفیلد دیفی و مارتین هلمن طراحی شده و در قالب یک مقاله علمی منتشر گردیده‌است. مطرح شدن این پروتکل، گام مهمی در معرفی و توسعه رمزنگاری کلید عمومی یا الگوریتم نامتقارن به حساب می‌آید .

مراحل پیاده‌سازیDiffie_Helman :

مقدار عدد اول دلخواه بزرگ p و مقدار محاسبه شده برای g توسط دو طرف به صورت توافقی انتخاب‌وردوبدل می‌شود.
هر یک از دو طرف یک عدد صحیح دلخواه a و b را به صورت پنهانی در نظر می‌گیرند.
هر یک از دو طرف با استفاده از عمل به توان رسانی پیمانه ای و مقادیر قبلی p و g و مقدار پنهانی، یک مقدار جدید (A,B) را محاسبه کرده و برای طرف مقابل ارسال می‌کند.

$$A = ga \bmod p$$

$$B = gb \bmod p$$

طرف اول با استفاده از مقادیر p و g و a وB ، و طرف دوم با استفاده از مقادیر p و g و b وA ، 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.

$$Ka = Ba \bmod p$$

$$Kb = Ab \bmod p$$

توجه به نکات زیر درباره‌ی این پروتکل لازم است:

مقادیر a و b و مقدار مشترک محاسبه شده، هرگز مستقیماً از کانال ارتباطی عبور نمی‌کنند. بقیهی مقادیر یعنی p و g و A و B از کانال ارتباطی عبور می‌کنند و برای دیگران قابل دسترسی هستند. دشواری حل مسئلهی لگاریتم گسسته تضمین می‌کند که مقادیر a و b و مقدار کلید رمز مشترک، با داشتن مقدار اعداد دیگر در عمل قابل محاسبه نباشد.
در فرمول‌های پیشنهادی اولیه این پروتکل، از گروه همنهشتی اعداد صحیح با پیمانهی عدد اول p و عملگر ضرب اعداد صحیح استفاده شده است. در این گروه عددی، یک ریشهی اولیه محاسبه می‌شود که آن را با g نشان می‌دهند.