بسم الله الرحمن الرحیم

الگوریتم دیفی \_هلمن

در سال 1997 یک موسسه تحقیقاتی جاسوسی در انگلستان ادعا کرد که پروتکل دیفی \_ هلمن قبل از سال 1976 توسط فردی به نام مالکولم ویلیا مسون دران موسسه اختراع شده وتنها به دلایل امنیتی از انتشار ان جلوگیری شده بوده است.

پروتکل تبادل کلیددیفی \_ هلمن یک پروتکل رمزنگاری است که با استفاده از ان دو نفر یا دو سازمان می توانند بدون نیاز به هرگونه اشنایی قبلی یک کلید رمز مشترک ایجاد وان را از طریق یک مسیر ارتباطی غیر امن بین خود تبادل نمایند این پروتکل اولین روش عملی مطرح شده برای تبادل کلید رمز در مسیر های ارتباطی غیر امن است ومشکل تبادل کلید رمز در الگوریتم کلید متقارن را اسان می سازد.

امنیت پروتکل دیفی \_هلمن

امنیت این پروتکل مبتنی بر دشواری حل مسئله لگاریتم گسسته است.باید درارتباط با امنیت پروتکل دیفی \_هلمن مسائل زیر در نظر گرفته شود

1.براساس قدرت محاسباتی رایانه های امروزی استفاده از عدداولpبا حدود300 رقم واعدادaوbباحدود 100 رقم میتواند شکستن امنیت این پروتکل ویافتن کلید رمز مشترک را در عمل غیر ممکن سازد.

2.در عمل هر عدد اول بزرگی را نمیتوان در این پروتکل به کار گرفت بلکه لازم است عدد Pمورد استفاده یک عدداول امن باشد در غیر این صورت شکستن امنیت این پروتکل ویافتن کلید رمز مشترک با استفاده از الگوریتم هایی مانند الگوریتم پولیگ \_ هلمن نسبتا اسان ودر زمان کمتری قابل انجام خواهد شد.

3.اعداد پنهان aوbباید به صورت عدد تصادفی تولید شوند ومولد عدد تصادفی مورد استفاده هم نباید تکرار پذیر وقابل پیش بینیباشد.در غیر این صورت یافتن کلید رمز مشترک اسانتر ودر زمان کمتری قابل انجام خواهد شد.