**الگوریتم رمزنگاری نامتقارن Diffie–Hellman**

یکی از مسائل قابل توجه در رمزنگاری نحوه توزیع کلید می باشد.کلیدهای ایجاد شده می بایست به نحوی بین مبدا و مقصد رد و بدل شوند و این دسترسی می بایست به نحوی انجام شود که کلید مورد نظر توسط افراد بدون صلاحیت قابل دسترسی و بهره برداری نباشد. نحوه ارسال کلید نیز میتواند به نحوی توسط فرایند رمزنگاری و یا انجام برخی از محاسبات انجام پذیرد. الگوریتم دیفی هیلمن از این قاعده مستثنی نبوده و با انجام محاسبات لازم ارسال کلید بین مبدا و مقصد را امکان پذیر می سازد.

این الگوریتم توسط Whitefield Diffie و Martin Hellman در سال 1976 ابداع شد. این الگوریتم میتواند برای ارسال کلید از یک کانال عمومی استفاده کند که نیاز به هیچگونه محدودیتی در استفاده از آن نیست و این کانال میتواند برای عموم قابل دسترس باشد. این کانال برای عموم قابل شنود بوده و انتقال کلید براساس انجام محاسبات بین مبدا و مقصد می باشد.

در مورد این الگوریتم میتوان گفت(martin):

1 - کلید های عومی و اختصاصی کاربران با زوج (P,S) شناخته میشود که میتواند موقتی باشد.

2 - برای رمزنگاری از تابع F استفاده میگردد که به ازای دو ورودی x,y خروجی مورد نظر را به صورت F(x,y) تولید کند.

ساختار کلی رمزنگاری در الگوریتم دیفی هیلمن به شرح زیر است.

1 - آلیس کلید عمومی خود را برای باب ارسال میکند.

2 - باب کلید عمومی خود را برای الیس ارسال میکند

3 - آلیس تابع F(Sa,Pa) را محاسبه میکند. الیس زمانی میتواند این کار را انجام دهد که کلید اختصاصی Sa را در اختیار داشته باشد.

4 - باب تابع F(Sb,Pb) را محاسبه میکند. باب زمانی میتواند این کار را انجام دهد که کلید اختصاصی Sb را در اختیار داشته باشد.

خصوصیت اساسی این سیستم رمزنگاری کلید عمومی را میتوان در تابع زیر عنوان نمود

F(Sa,Pb) = F(Sb,Pa)

این خصوصیت موجب می شود بر اساس محاسبه انجام شده ,کلید های بدست امده برای طرفین دارای مقداری یکسان باشد.

رمزنگاری به روش Diffie–Hellman

الگوریتم رمزنگاری را میتوان به شرح زیر عنوان نمود:

1 - آلیس و باب بر روی عدد اول بزرگ p,g توافق میکنند که عدد p بسیار بزرگ خواهد بود. نیازی نیست که این دو عدد مخفی نگه داشته شوند.

2 - آلیس و باب دو عدد اول Xa , Xb را به صورت تصادفی انتخاب می کنند که کوچکتر از p می باشند. این دو عدد به عنوان کلید خصوصی می باید مخفی نگه داشته شوند.

3 - آلیس کلید قابل ارسال را با استفاده از فرمول Ya= (g^Xa) mod p و بطور مشابه باب کلید قابل ارسال را با استفاده از فرمول Yb= (g^Xb) mod p محاسبه میکند . اعداد بدست آمده از طریق یک کانال ناامن برای طرفین ارسال خواهد شد.

4 - آلیس کلید مورد نظر را با استفاده از فرمول Za= (Yb^Xa) mod p و به طور مشابه باب با استفاده از فرمول

Zb=(Ya^Xb) mod p کلید مورد نظر را استخراج میکند.

5 - Za = Zb کلید مشترک محسوب شده و برای عملیات رمزنگاری متقارن قابل استفاده می باشد.

(عملگر ^ به معنی توان رساندن می باشد)

