

کلید خصوصی (Private Key) :

کلید خصوصی یک کلید مخفی است که برای رمز گذاری و رمزگشایی پیام ها استفاده می شود. کلید خصوصی همراه با کلید عمومی استفاده می شود. باید در همه زمان ها خصوصی نگه داشته شود و هرگز نباید با کسی در میان گذاشته شود.

کلید عمومی (Public Key):

از کلید عمومی فقط برای رمز گذاری پیام استفاده می شود. می تواند برای افراد دیگر ارسال شود. هنگامی که فرستنده پیامی را با استفاده از کلید عمومی شما رمز گذاری کرد، می توانید قفل آن را فقط با استفاده از کلید خصوصی خود باز کنید.

رمزنگاری نامتقارن

رمزنگاری نامتقارن مشابه رمزنگاری متقارن است ، اما کمی پیچیده تر است. تمایز اصلی با رمزنگاری متقارن استفاده از جفت کلید است. رمزنگاری نامتقارن به منظور رمز گذاری و رمزگشایی داده ها، به جای یک کلید مشترک، از جفت کلید استفاده می کند. جفت کلید از ۲ قسمت، یک کلید عمومی و یک کلید خصوصی تشکیل شده است.

یک کلید عمومی می تواند به عنوان یک نام کاربری دیده شود، برای همه در دسترس است ، قابل اشتراک گذاری است و همه می توانند با آن نام کاربری سابقه حساب را مشاهده کنند. نام کاربری به یک رمز عبور (کلید خصوصی) گره خورده است. اما هیچ راهی برای استخراج رمز ورود (کلید خصوصی) از روی نام کاربری وجود ندارد. یک کلید خصوصی می تواند به عنوان رمز ورود حساب با نام کاربری خاص دیده شود. در دسترس عموم نیست و نباید با کسی به اشتراک گذاشته شود. کلید خصوصی برای تأیید اقدامات در حساب ها استفاده می شود. برای دسترسی به حساب یا اجازه دادن به هر اقدامی در حساب، فقط کلید خصوصی مورد نیاز است.