Çalışma Mantığı

Çalışma mantığını adım adım inceleyelim.

Birinci adım olarak; Kullanıcı "veri tabanı" oluşturur. Bu veri tabanı, tüm şifreleri ve diğer hassas bilgileri içerir.Veri tabanı oluşturulurken kullanıcıdan bir "ana parola" veya "anahtar kurtarma dosyası" gibi bir ana erişim yöntemi belirlemesi istenir.

Daha sonrasında ise kullanıcı, çeşitli kayıtları (örneğin, web siteleri, uygulamalar, hesaplar) ve bu kayıtlara ait kullanıcı adları ve şifreleri veri tabanına ekler. Eklenen bilgiler, veri tabanında "giriş" olarak kaydedilir.

KeePass, eklenen bilgileri güvence altına almak için AES (Advanced Encryption Standard) gibi güçlü şifreleme algoritmalarını kullanır. Ana parola veya anahtar kurtarma dosyası, bu şifreleme işleminde kullanılır. Veri tabanı içeriği, şifrelenmiş bir biçimde diskte saklanır. Bu sayede verilerin güvenliği sağlanmış olur.

Ana parola veya anahtar kurtarma dosyası, gerçek şifreleme anahtarı olarak kullanılmadan önce güvenli bir biçimde saklanır. Anahtar türetme işlemi, kullanıcının girdiği ana parolayı veya anahtar kurtarma dosyasını temel alarak gerçek şifreleme anahtarını türetir. Bu, veri tabanının şifresini çözmek için gereklidir.

Kullanıcı, KeePass uygulamasını başlattığında veri tabanına erişmek için ana parolasını girmesi veya anahtar kurtarma dosyasını sağlaması istenir. Girilen ana parola veya kullanılan anahtar kurtarma dosyası, gerçek şifreleme anahtarının türetilmesi için kullanılır. Doğru ana parolası veya anahtar kurtarma dosyası sağlandığında, veri tabanı açılır ve içeriği kullanıcıya görüntülenir.

Kullanıcı, veri tabanı içinde saklanan kayıtlardan birini seçerek ilgili kullanıcı adı ve şifreyi elde eder. Bu bilgileri kopyalayarak veya otomatik olarak ilgili hesaba giriş yapabilir.

Revision #1
Created 25 January 2024 13:44:35 by Ertan Sözer
Updated 25 January 2024 13:45:28 by Ertan Sözer