## 数据包前端加密和后端加密的优缺点

**前端加密**

**优点：**

1. 在 HTTP 协议下，数据是明文传输，如账号密码。这些数据一旦被中间人获取，会给用户带来极大的安全隐患。前端加密能够解决中间人攻击的问题，中间人将无法获取到用户的原始账号和密码数据。
2. 不会加重数据库服务器的负载。

**缺点：**

1. 前端加密无法解决重放的问题。虽然发送的数据是加密的，但攻击者如果把拦截的密文重发一遍，依旧能够通过验证进行登录。

2. 有些加密工具和协议不够高效，如LTS会导致客户端和服务端的性能下降。

**后端加密**

**优点：**

1. 加密后，数据以密文的方式存储，防止数据直接暴露。

2. 系统中可以选择需要加密的数据库列，以便于用户选择那些敏感信息进行加密而不是全部数据都加密。只对用户的敏感数据加密可以提高数据库访问速度。这样有利于用户在效率与安全性之间进行自主选择。

**缺点：**

1. 加密解密过程将降低数据库的使用效率。
2. 如果仅在后端加密，数据以明文方式进行传输，很可能被中间人获取。

参考资料：

[1] 关于Web前端密码加密是否有意义的总结！

https://blog.csdn.net/hla199106/article/details/45114801

[2] 当我们在谈论前端加密时，我们在谈些什么

<https://segmentfault.com/a/1190000006226236>

[3] Web 前端密码加密是否有意义？

https://www.zhihu.com/question/25539382

[4] 数据库加密-百度百科

https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%BA%93%E5%8A%A0%E5%AF%86

[5] 关于数据库加密，你不能不知道的秘密(一)

http://netsecurity.51cto.com/art/201701/528298.htm