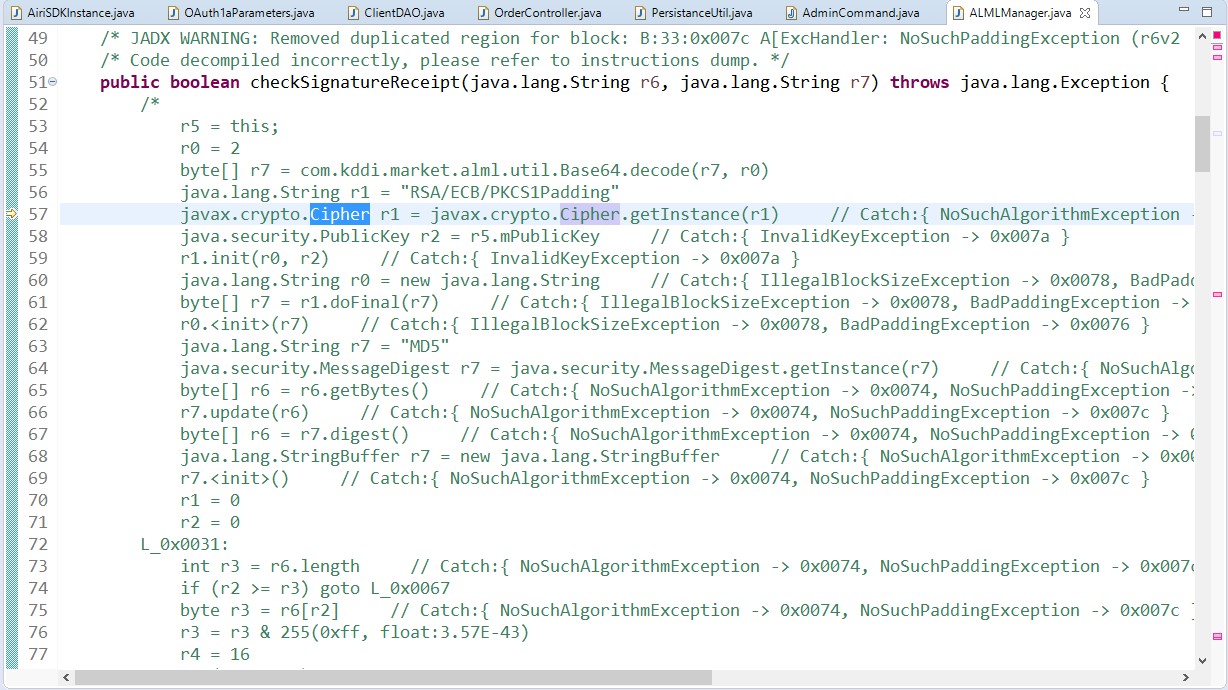
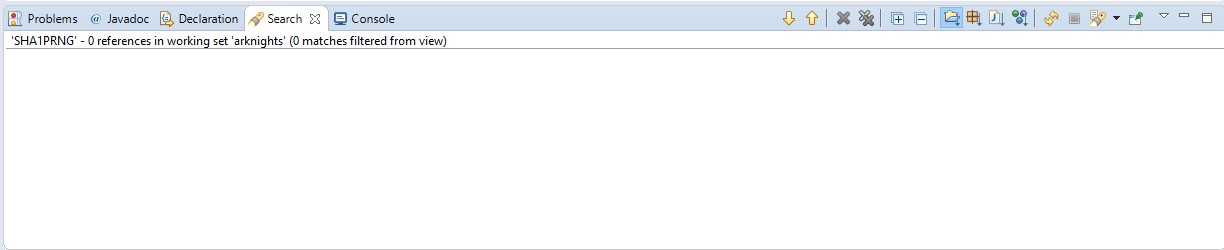
1. Searched for any cryptographic activities in source code, found this one in AiriSDK, that’s used for all authorization/authentication in this app:

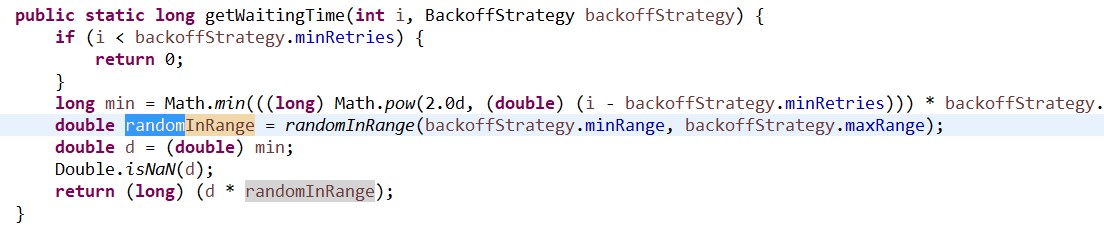
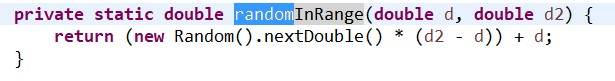


This code is responsible for checking the signature in receipt that comes from the server when user authorizes some transfer in the in-game shop. There are no hardcoded keys or anything suspicious.

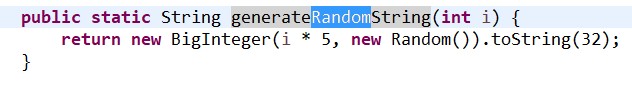
Also search for SHA1PRGN gave no results:



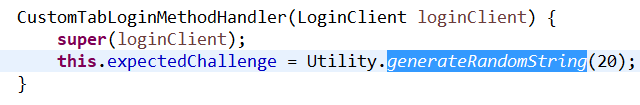
1. Found some Random usages in couple of SDKs:



This one is straightforward: here Random is used for probably generating random connection await request time. This was found in Adjust SDK.



This one was in Facebook SDK. It’s used here.



Seems like it’s used for generating login challenge. That’s not secure.



This one is hard to wrap your head around. Found it in Aliyun SDK. But it doesn’t seem to be involved in generating any sort of keys or challenges.