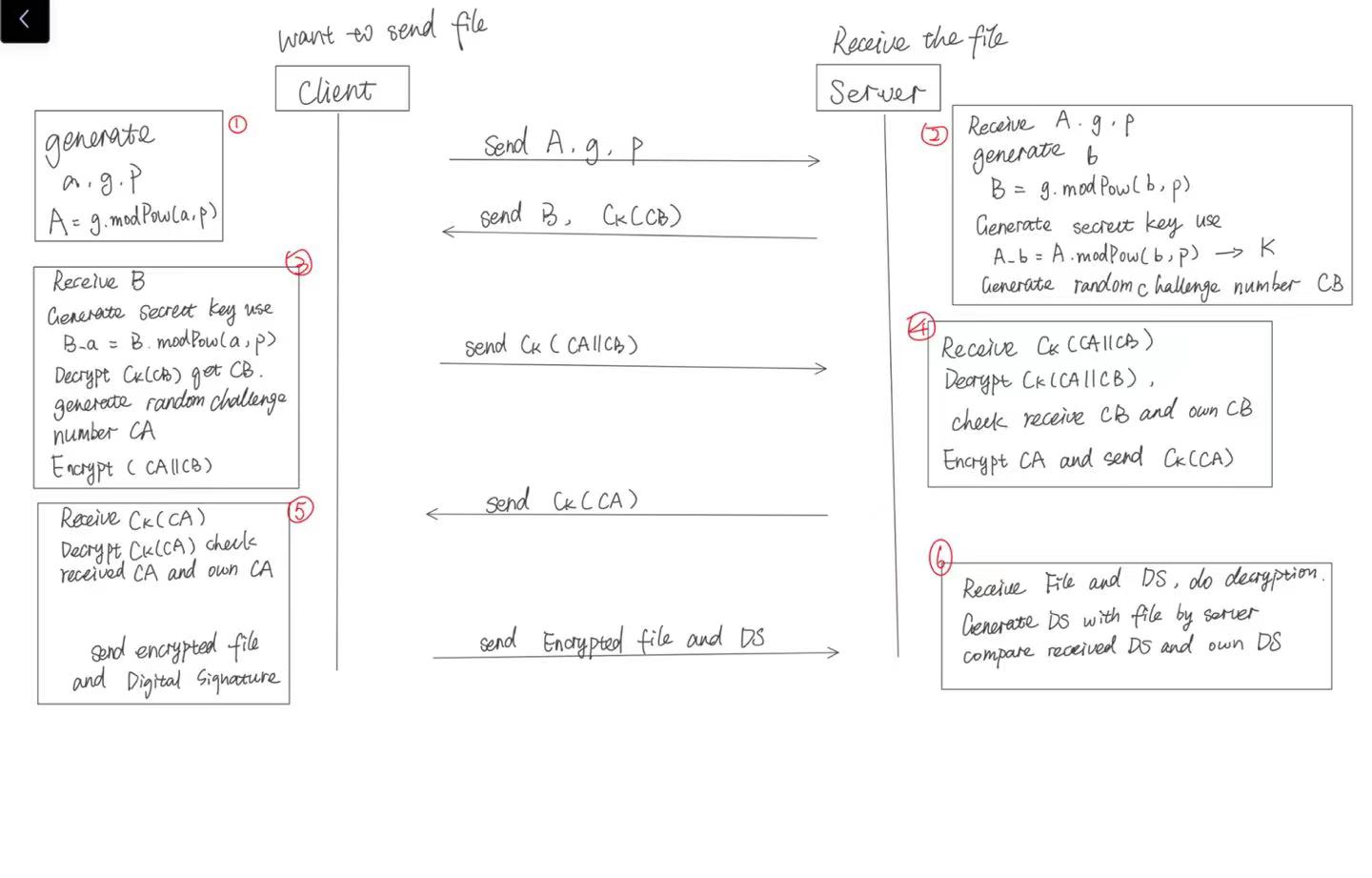
This is the read me file of **SecureFileTransfer**.

Ps: The ReadMe.docx and ReadMe.pdf have the **same content**. In case of you cannot open the file in right format.

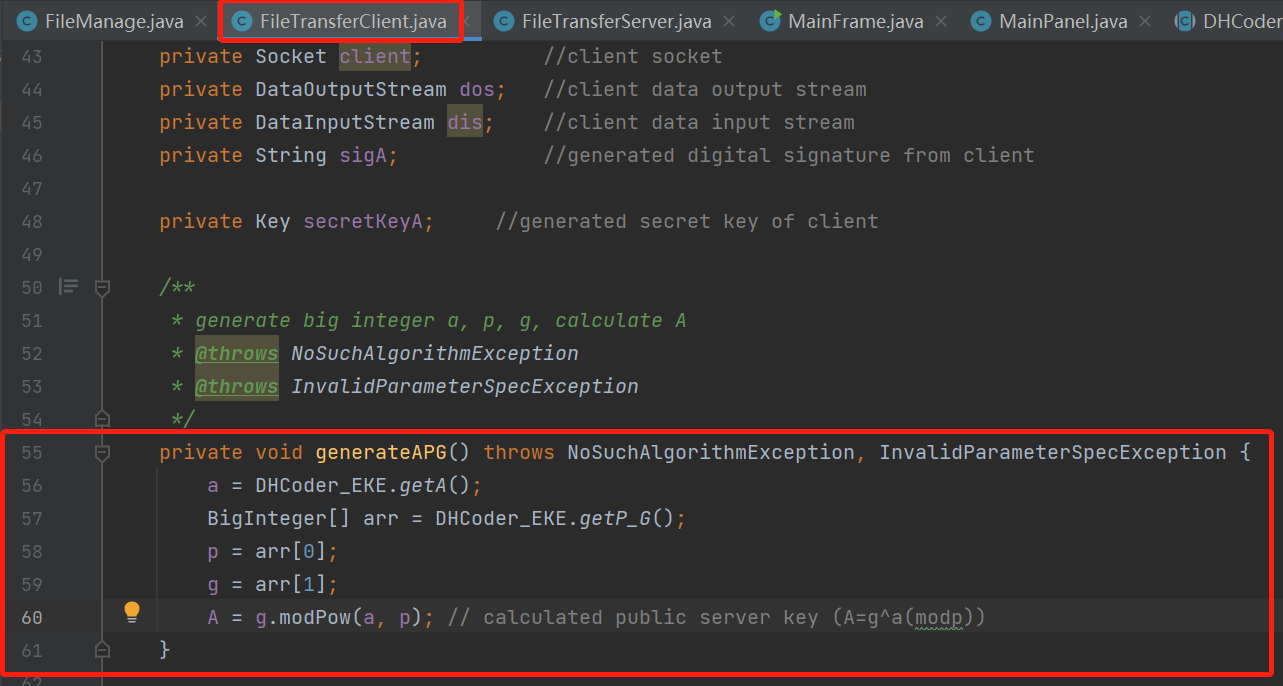
This program does the authentication with **DH-EKE** algorithm and generate secret key in the process firstly. Then transfer the encrypted file (**AES**) and the generated digital signature with algorithm **MD5**. The server checks the DS to decide trust file or not.

The progress:

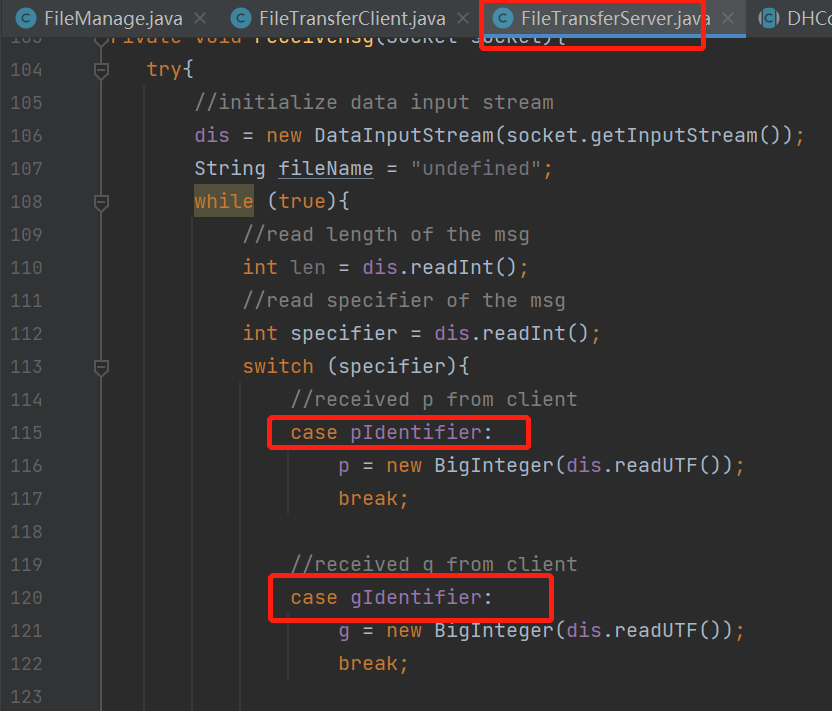


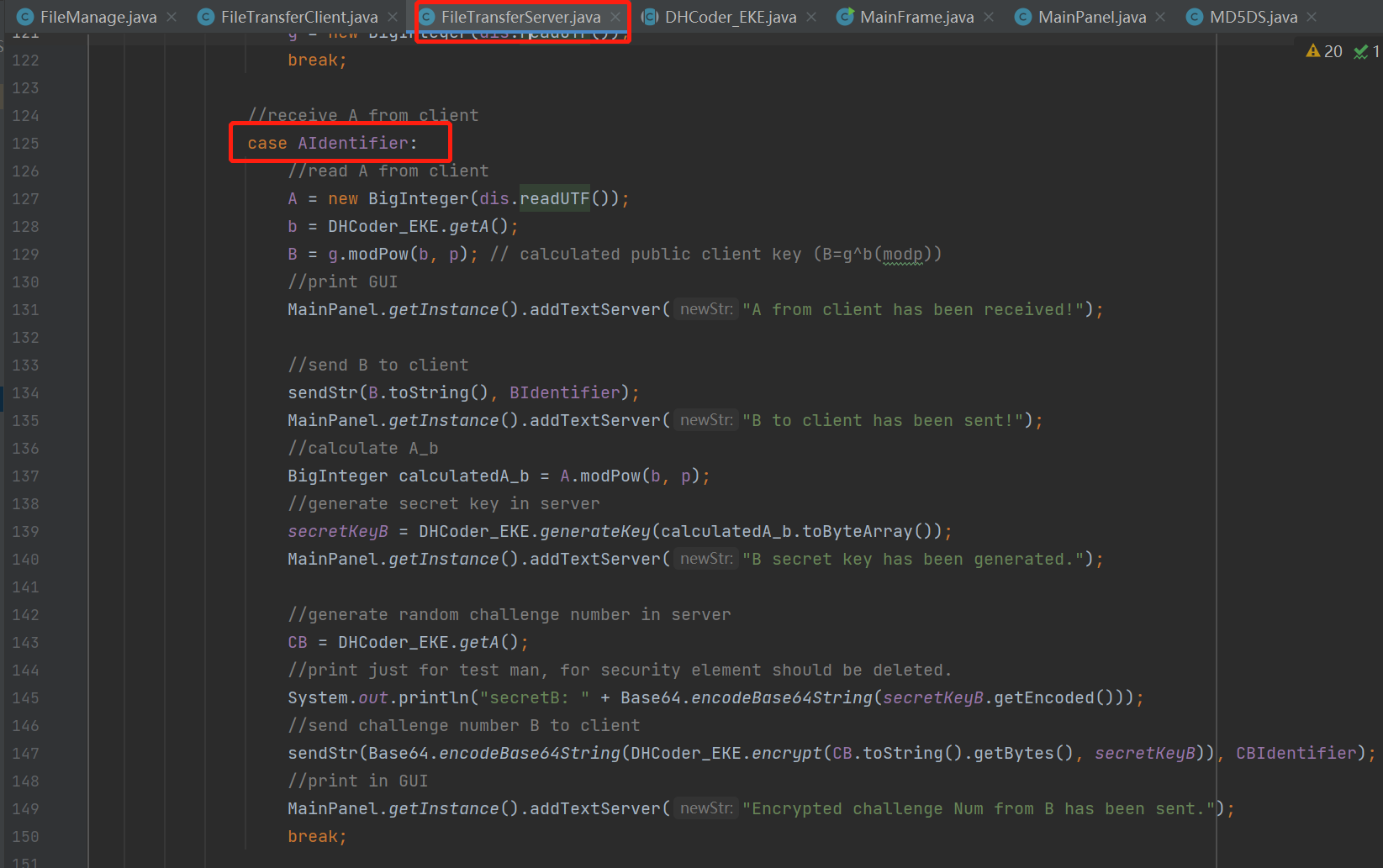
**Authentication, DH-EKE:**

1. **Client** Generate a, p, g

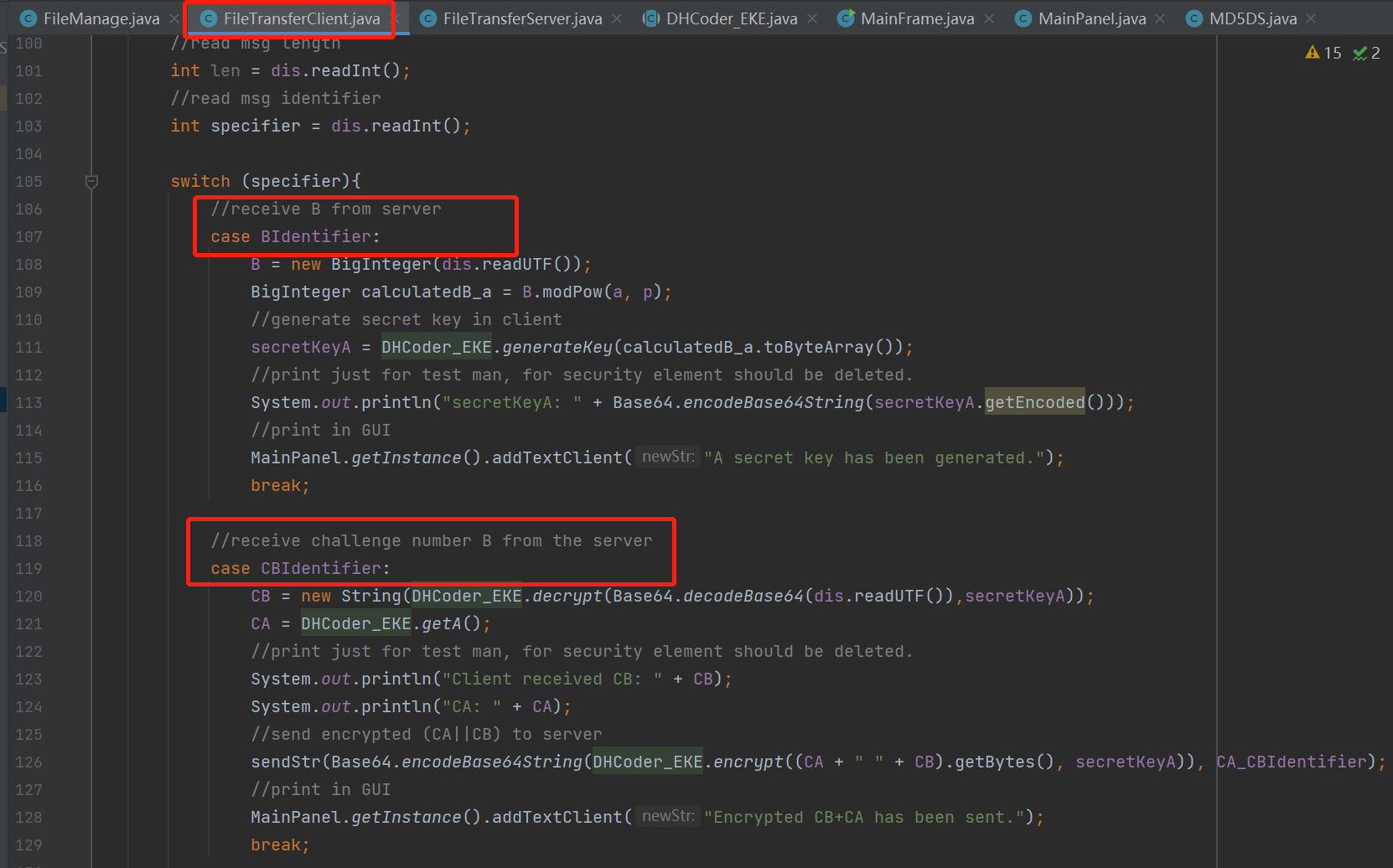


1. **Server**: Receive A, g, p. Generate b, calculate B. Calculate secret key from A and b.

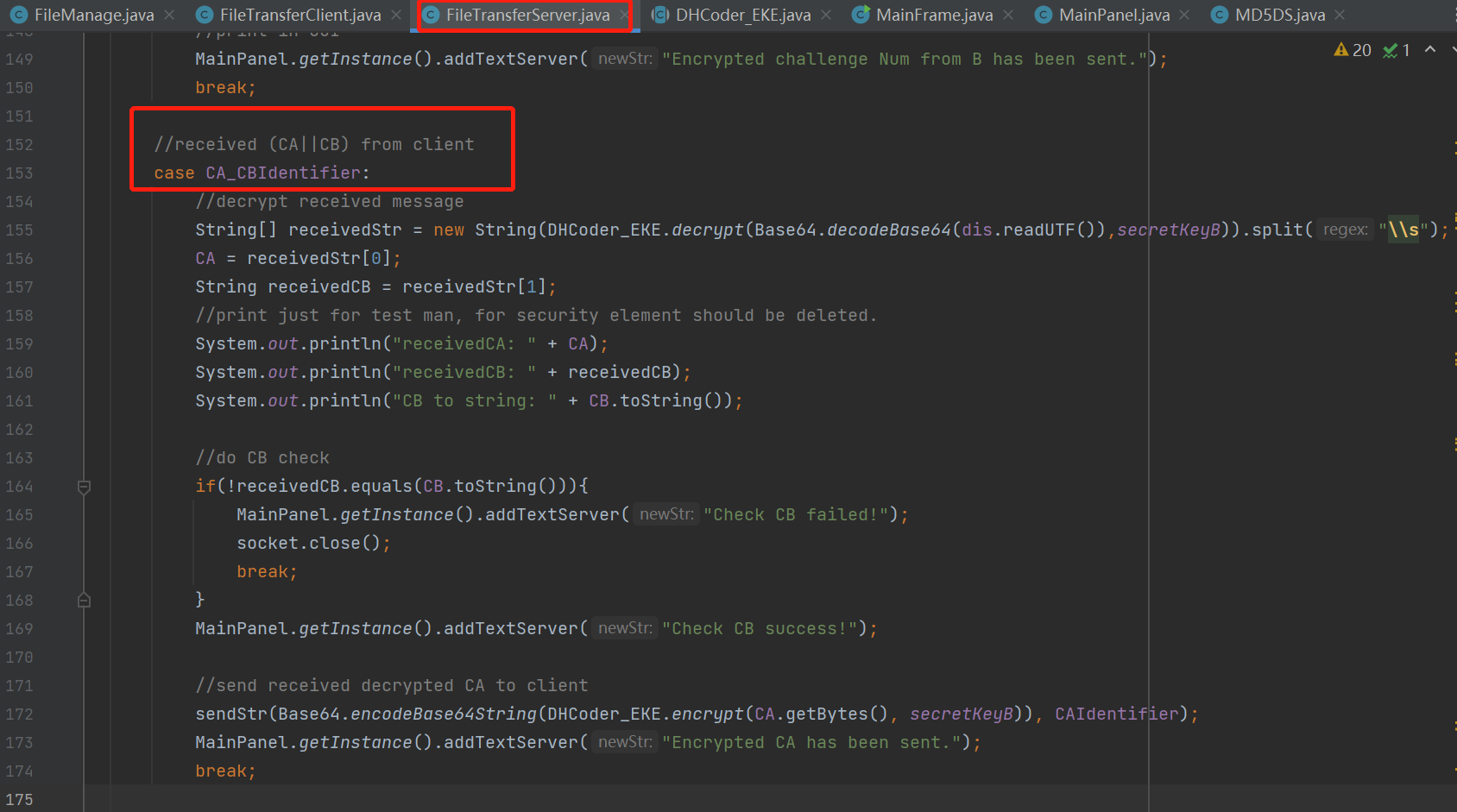




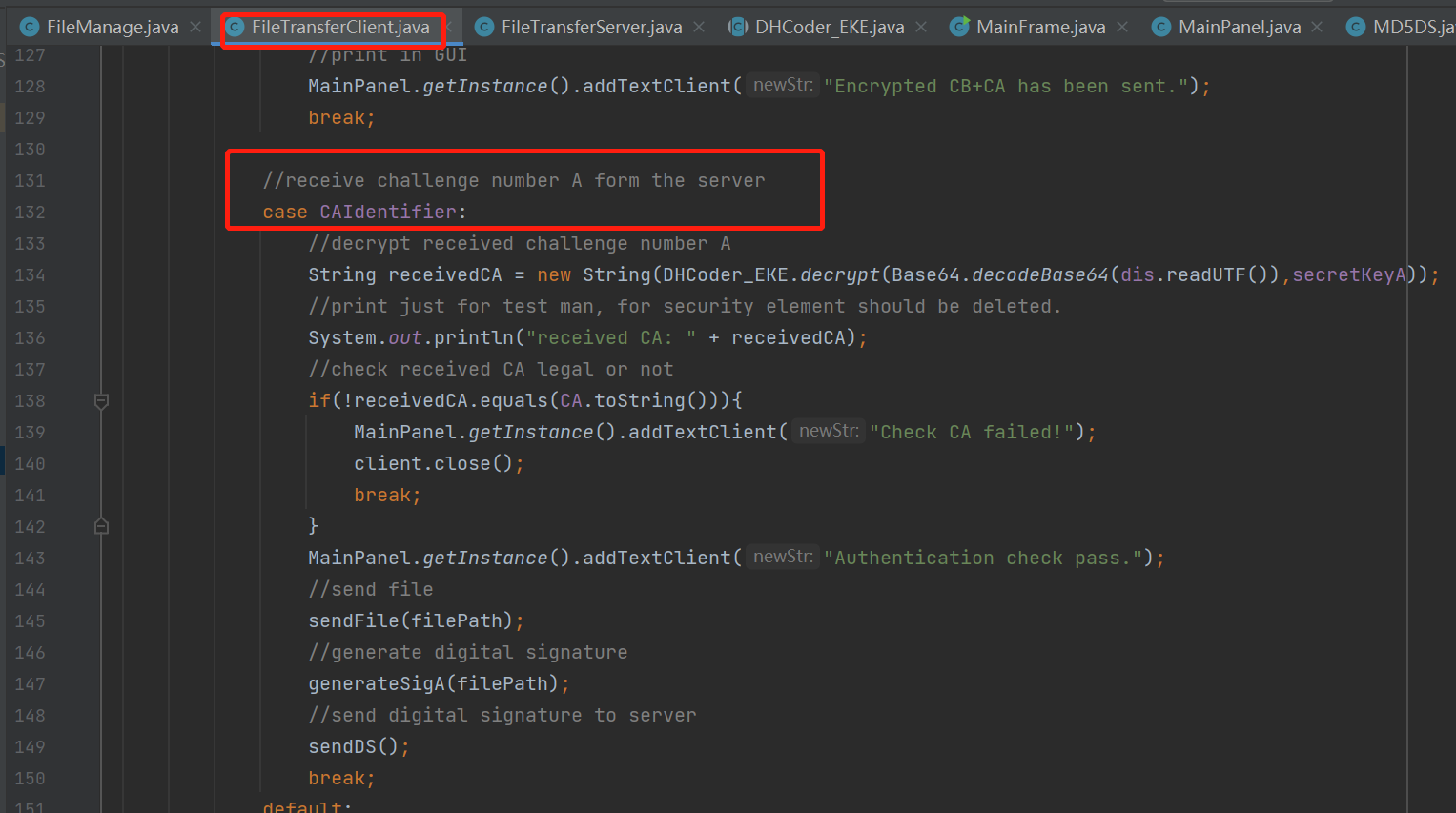
1. **Client**: Receive B. Generate secret key with B and a. Decrypt received CB. Generate CA. Encrypt CA||CB.



1. **Server** received and decrypt CA||CB. Check CB is right or not. If check pass, encrypt and send CA.

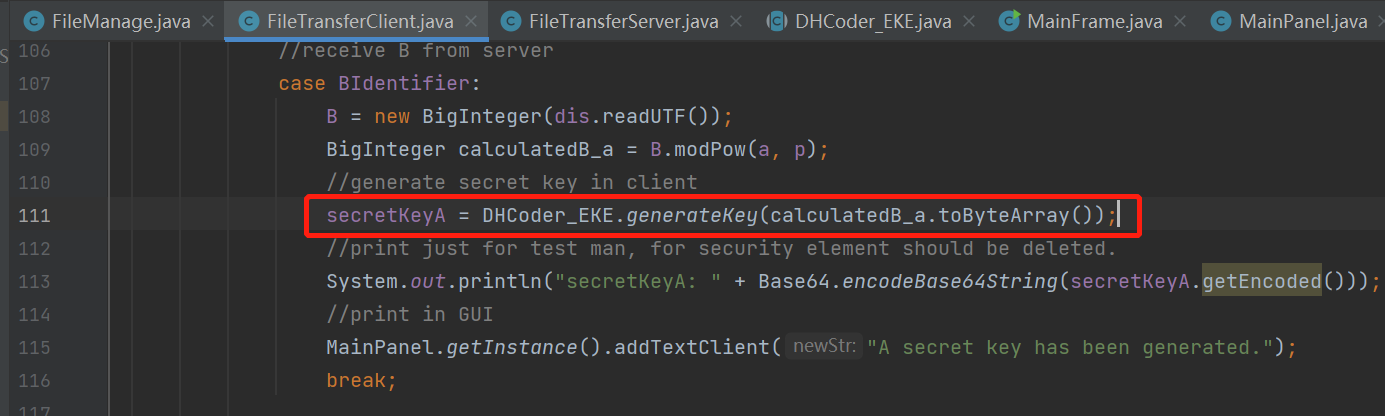


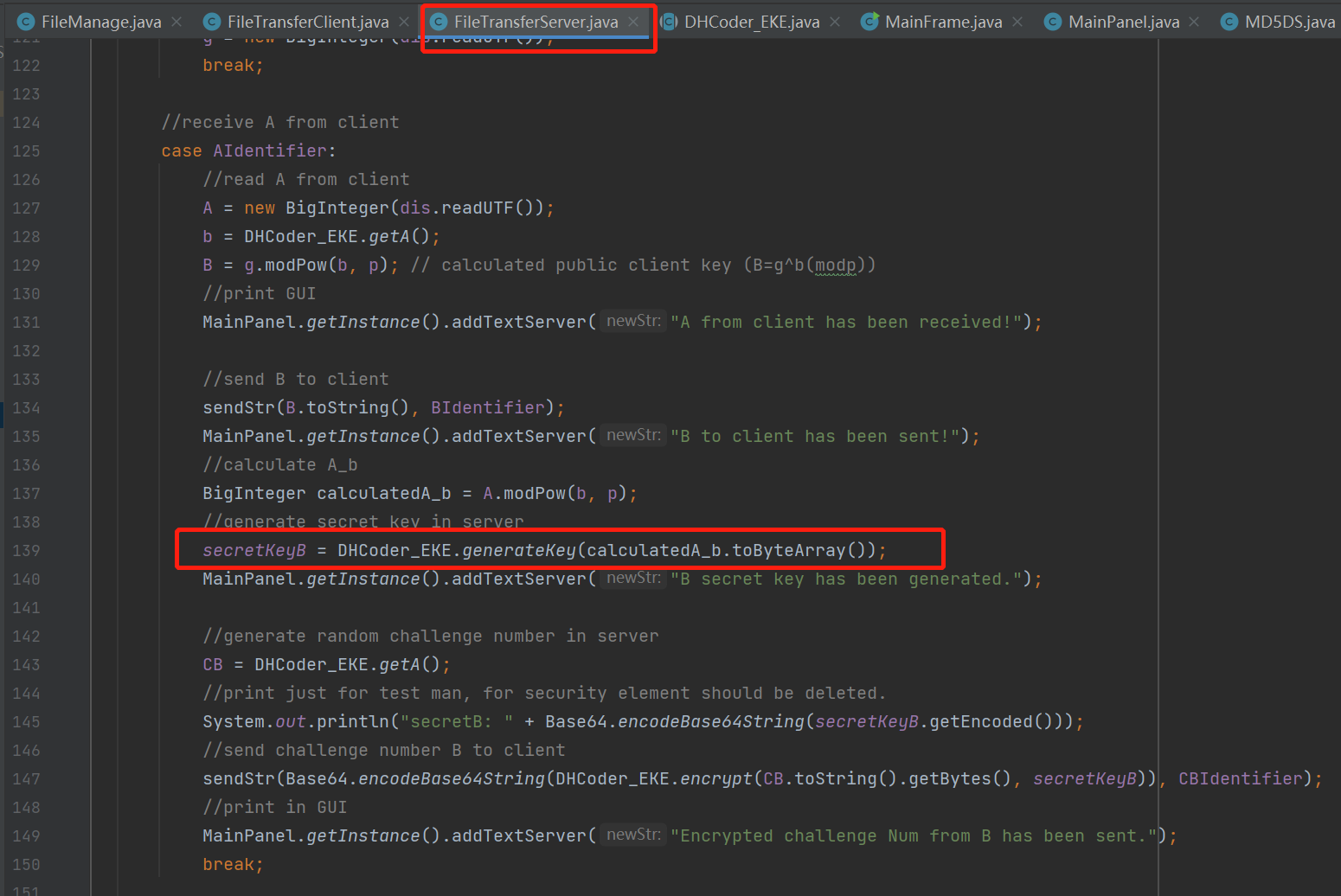
1. **Client**: receive and decrypt CA, do the check. If check pass, do the file transition.

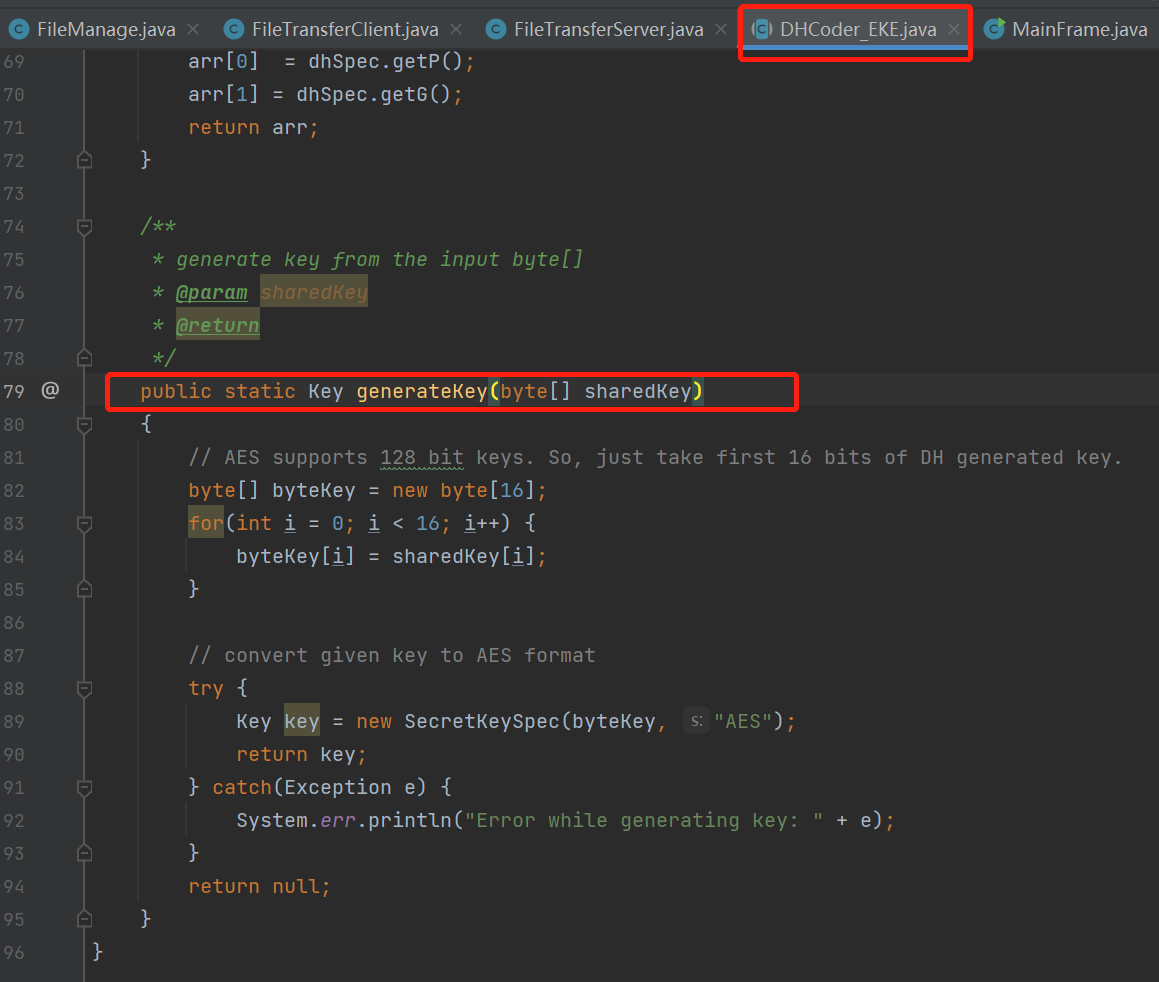


**Symmetric Encryption: AES**

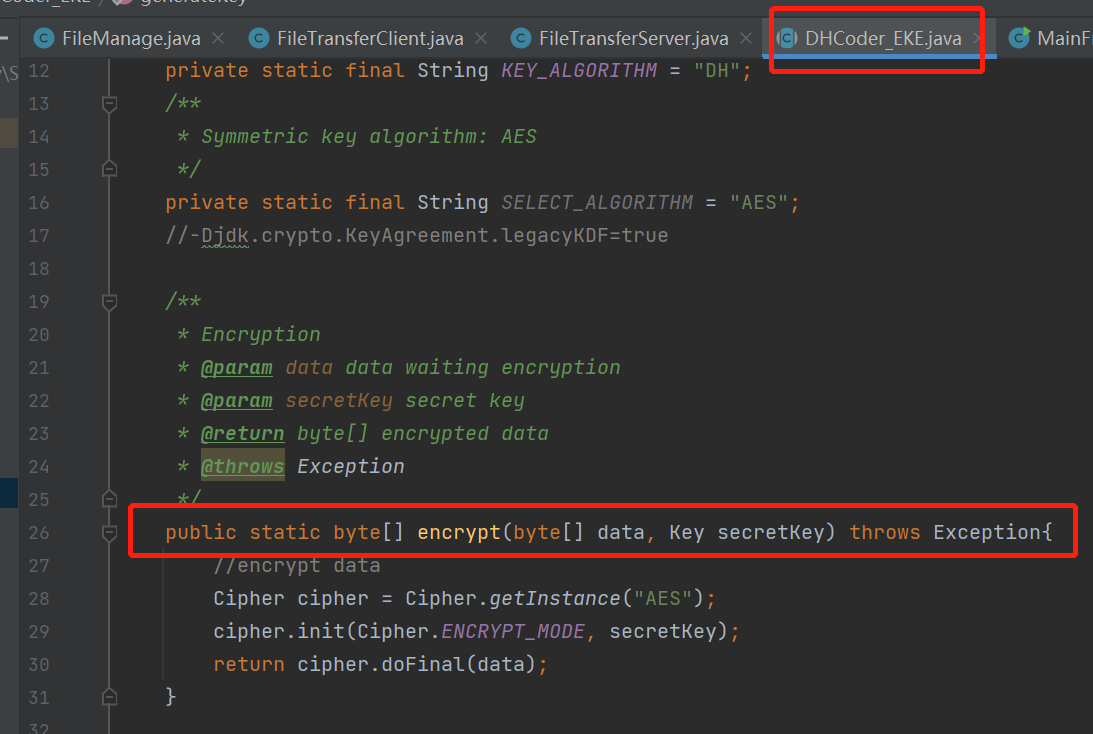
1. **Generate key** for client and server in authentication progress:



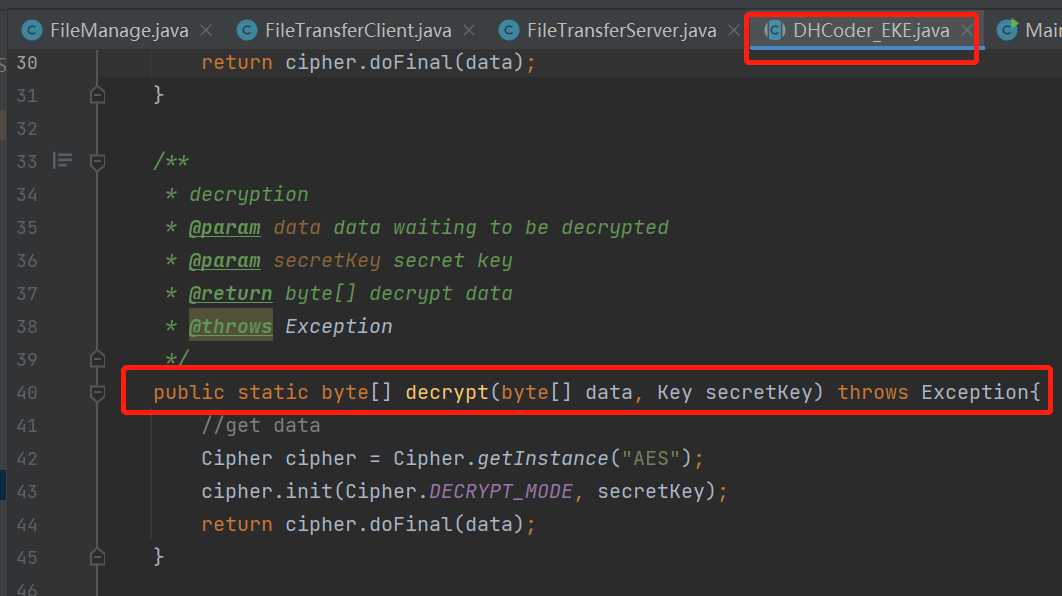




1. The **encryption**

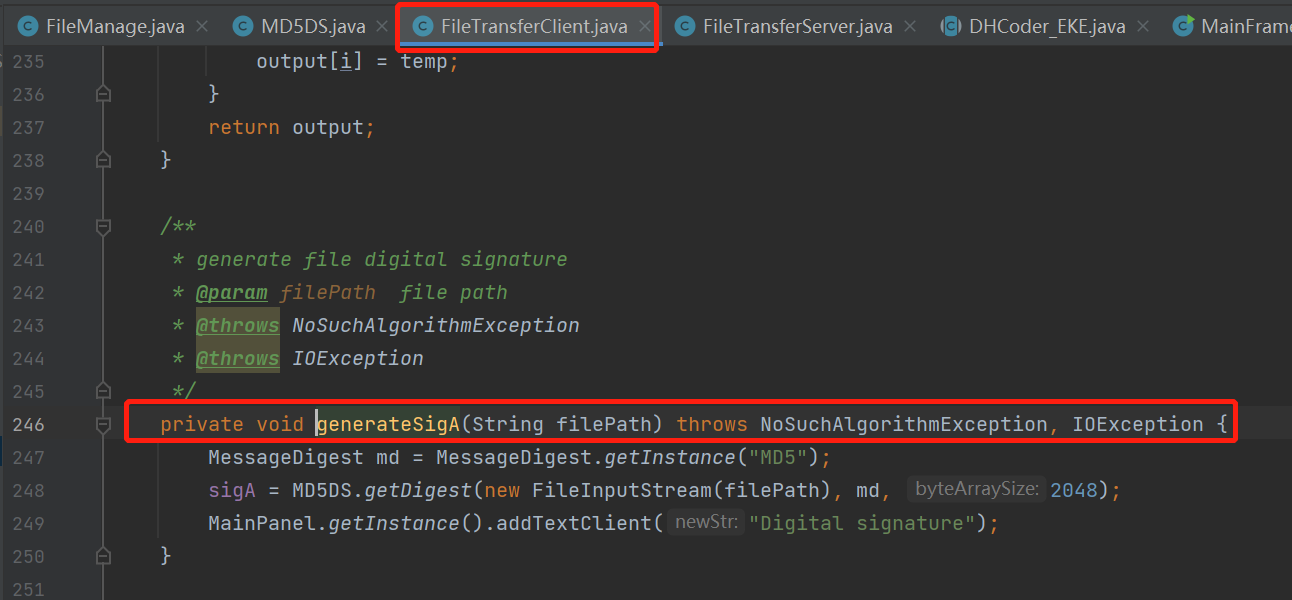


1. The **decryption**

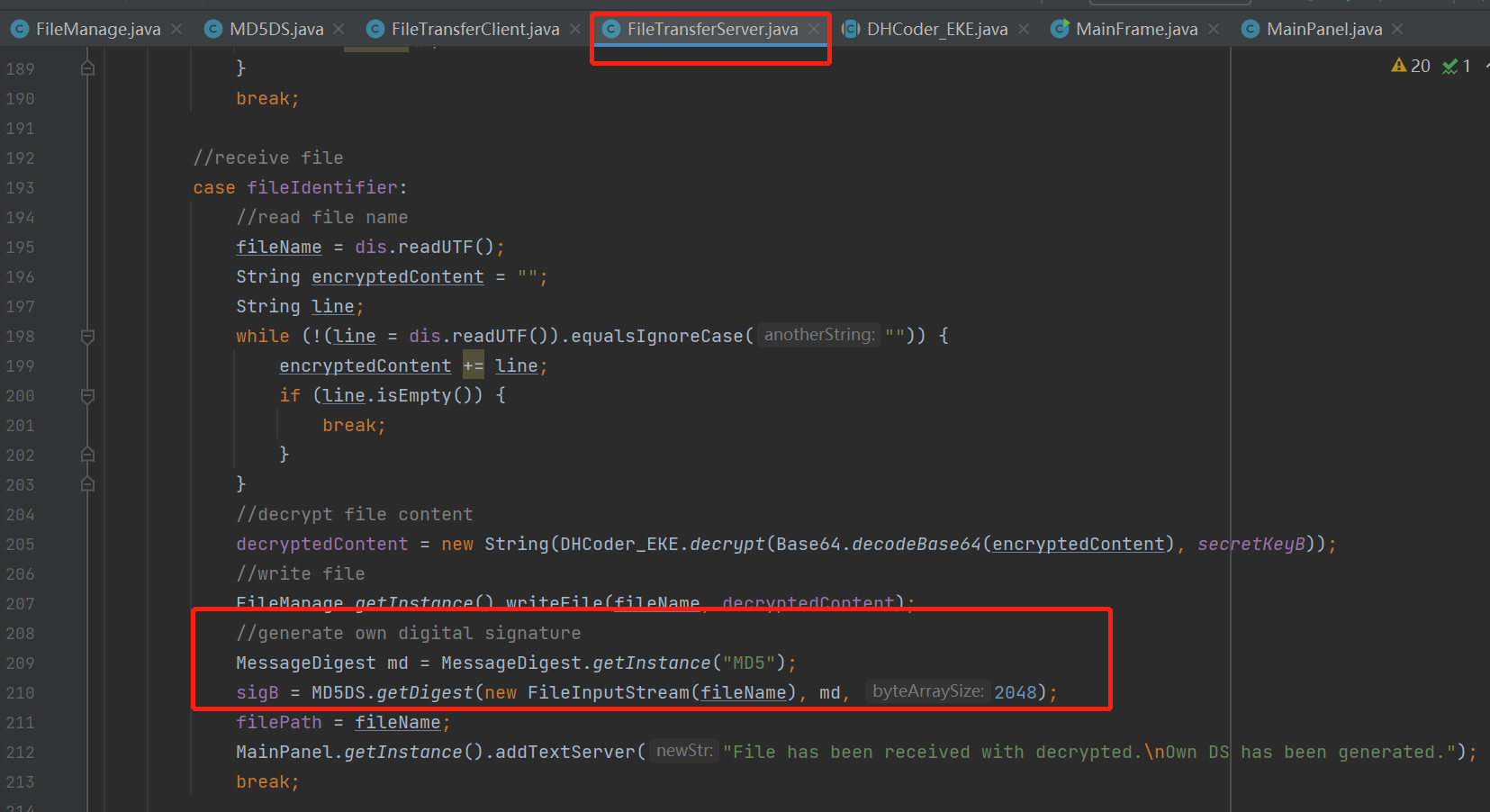


**Digital Signature: MD5**

1. Generate DS in client:



1. Generate DS in server:



1. MD5DS class

