In-Class Activity

We are only going to focus on block ciphers and utilize various strategies to securely store our sensitive data. A common approach when designing a new feature for an existing product is to find ways to leverage the product's current behavior in order to lower the cost to implement (build) and maintain this security feature. In a real-world environment the security feature will always need to evolve to meet industry standards, therefore maintainability is important. We also want to try and minimize data leakage or data loss if possible.

Scenario

You were recently hired as a software security engineer working on a product that runs similar to an IDE (e.g. NetBeans, PyCharm, Visual Studio). You don't know much about this product other than it reads in project files, and the user can edit them and save their changes.

During a planning meeting, the security architect decides that, in order to meet certain industry standards in security, these project files need to be encrypted due to sensitive data stored within the files (e.g. user data, sensitive code or some other ridiculously sensitive logic like raw SQL queries, keys, company-based Intellectual Property, etc. You're not really sure what.). As part of the Agile Framework lifecycle, this work is passed down and assigned to your team in the form of a *Feature*, and you are working on a *Spike story* to design the encryption/decryption mechanism.

For the sake of time, we will only focus on the encryption mechanism while taking into consideration how a decryption mechanism would be able to support the design. The last thing you want is to encrypt something so well that it's impossible to decrypt it. But hey! The best kind of encryption is the one where no one can decrypt it, right?

Assumptions

1. The software that reads in the file has access to a public/private key pair used for asymmetric encryption.
2. The list of cryptographic algorithms you can use in this design are the following:
    a. 128-bit (min) AES Encryption with any of the following cipher block modes
        i. AES-CBC
        ii. AES-CTR
        iii. AES-GCM
    b. 2048-bit (min) RSA Encryption
    c. SHA-256 Hashing Algorithm (If needed)
3. A sample project file has been provided to you.