Encrypt password

This use case provides password security for the user with the implementation of an encryption algorithm. The algorithm developer actor creates an algorithm which would encrypt the user inputted password when they try to login or signup. During sign up, the password gets encrypted by the developer and then stored into the database by the administrator actor. During login, the password input is encrypted by the developer and then verified with the password in the database to see if they match by the administrator.

Alternate Flow: An alternate flow would be that if the encryption algorithm is changed, the passwords inputted by the user would not match the ones stored in the database, so the algorithm would also have to be applied to the stored passwords.
Exception Flow: An exception flow would be if the user entered an incorrect password, which would prevent them from logging in since their password would get encrypted but it would not match the one in the database.

Information

Rank	Medium
ID	
Status	Unspecified
Justification	
Primary Actors	Algorithm Developer, Database, Administrator
Suppporting Actors	User

Details

Level	User
Complexity	Medium
Use Case Status	Initial
Implementation Status	Scheduled
Preconditions	A precondition is that there is a pre-existing database and encryption algorithm set in place by the algorithm developer and administrator.
Post-conditions	The post condition is a successful or unsuccessful login/sign up.
Author	N/A
Assumptions	An assumption is that the user is attempting to sign up or login to the system.