AES Encryption and AccessApp

Brandi Coon

Abstract - With the usage amount of technology and social media being at an all time high, there is always a need for usernames and passwords (i.e. login credentials/“virtual keys”). The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data [1]. That being said, AES gives us a nice, secure way to keep login credential information extremely safe, private, and therefore, harder to steal or tamper with. In this paper, I describe the way in which AES encryption will be implemented in the application “AccessApp”. AccessApp is a nice way in which all of ones Entertainment and Social Media apps can be stored in one place, along with all necessary credential information to login and use these apps from one singular place.

1. Introduction

In our current generation, our society essentially revolves around technology and social media. Whether you are in your teens, 20s, 30s, or even older, the chance that you use some piece of technology or have some kind of social media profile is very high, it’s no surprise. Not only is it expected that a person has at least one social media profile, but if they have at least one profile, then it is quite likely that they have many.

Think about all of the different entertainment and social media apps you use on your cellphones: Instagram, Facebook, Snapchat, Twitter, Netflix, Hulu, Spotify, etc. Now think about the hassle of having to open each application separately and type in your username and password to log in to each app separately. Why not avoid this hassle and make a safe and easy way to access and use these apps all in one place?

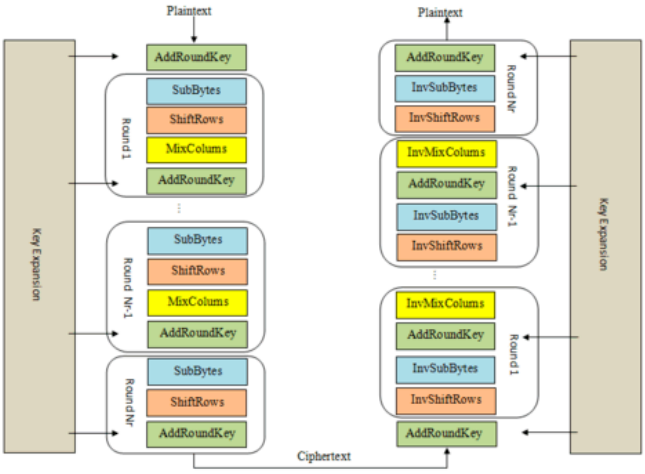
AccessApp serves as this "Entertainment/ Social Media" consolidation app. This one application basically "interfaces" with all of those other previously mentioned apps, serving as a single point where you can log in and get to ANY of those other entertainment/ social media apps mentioned, without having to separately open and close a bunch of different ones.

This application is also a safe one in terms of data privacy. AccessApp essentially keeps a "credentials" manager for all of your accounts in the listed apps, so that you can just open up/access the intended app from the main consolidation app. In other words, it keeps your log-in credentials saved in one place so AccessApp can log you in to whatever app it is you want to use. Now that we have all of this private and sensitive information saved in one vulnerable place, how is it that we keep it safe? This is where AES comes into play.

2. Methodology

The intended implementation of AES in this application is to be used to keep login credential information safe and secure. When users initially enter their usernames and

passwords into the system, AES will be used to encrypt this information and store it safely within the application.



As seen in the diagram above, the program code will take in the user's username, for example, as plaintext, and perform the necessary steps following it in order to fully encrypt the sensitive information. Once the information is encrypted, it can now be saved in the system without worrying that someone can easily hack in and access and/or tamper with this information. It's hard to do anything productive (as a hacker) with gibberish login credentials; it would virtually be meaningless information to them.

3. Experiments/Progress

Currently, I have made progress in laying out my code in which the program will take in the user's credentials, encrypt them, and save them somewhere in the system. I am currently in the middle of making sure I can decrypt the AES encrypted information so that it can be sent into the intended social media app, and from there I still have to write the code that actually produces the app itself, and I have to find a social media app that allows me to access it from within the AccessApp and automatically fill in the login information so that it can log in itself. After previously speaking with Professor Pablo Rivas, for this project I will only select one social media app to interface with, make sure it is fully working, and then from there, depending on what social media apps allow me to interface with them and depending on the amount of time we have to work with other apps, I will continue to add more and more social media platforms into AccessApp.

4. Conclusion

In this paper I described the new application AccessApp and its intentions to use AES for encrypting credentials. I further explained my progress and what else needs to be implemented for my project. I believe that using AES to encrypt this type of login credential information is a safe and secure way to make sure it is not stolen or tampered with.

5. References

[1] M. Rouse, M. Cobb, GEM100, and B. Pawliw, "Advanced Encryption Standard (AES)", https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

DES vs AES

	DES	AES
Date	1976	1999
Block size	64	128
Key length	56	128, 192, 256
Number of rounds	16	9,11,13
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM, enhanced by NSA	Independent cryptographers