A Cryptographic Simulator for Enhancing Undergraduates' Learning Experience in Cybersecurity Education

This work is supported by NSF Target Infusion Project (Award ID: 1714261)

Ayodeji, Ogundiran, Jie Yan Department of Computer Science, Bowie State University
Chaobin Liu, Department of Mathematics, Bowie State University
Weifeng Xu, College of Public Affairs, University of Baltimore

Introduction

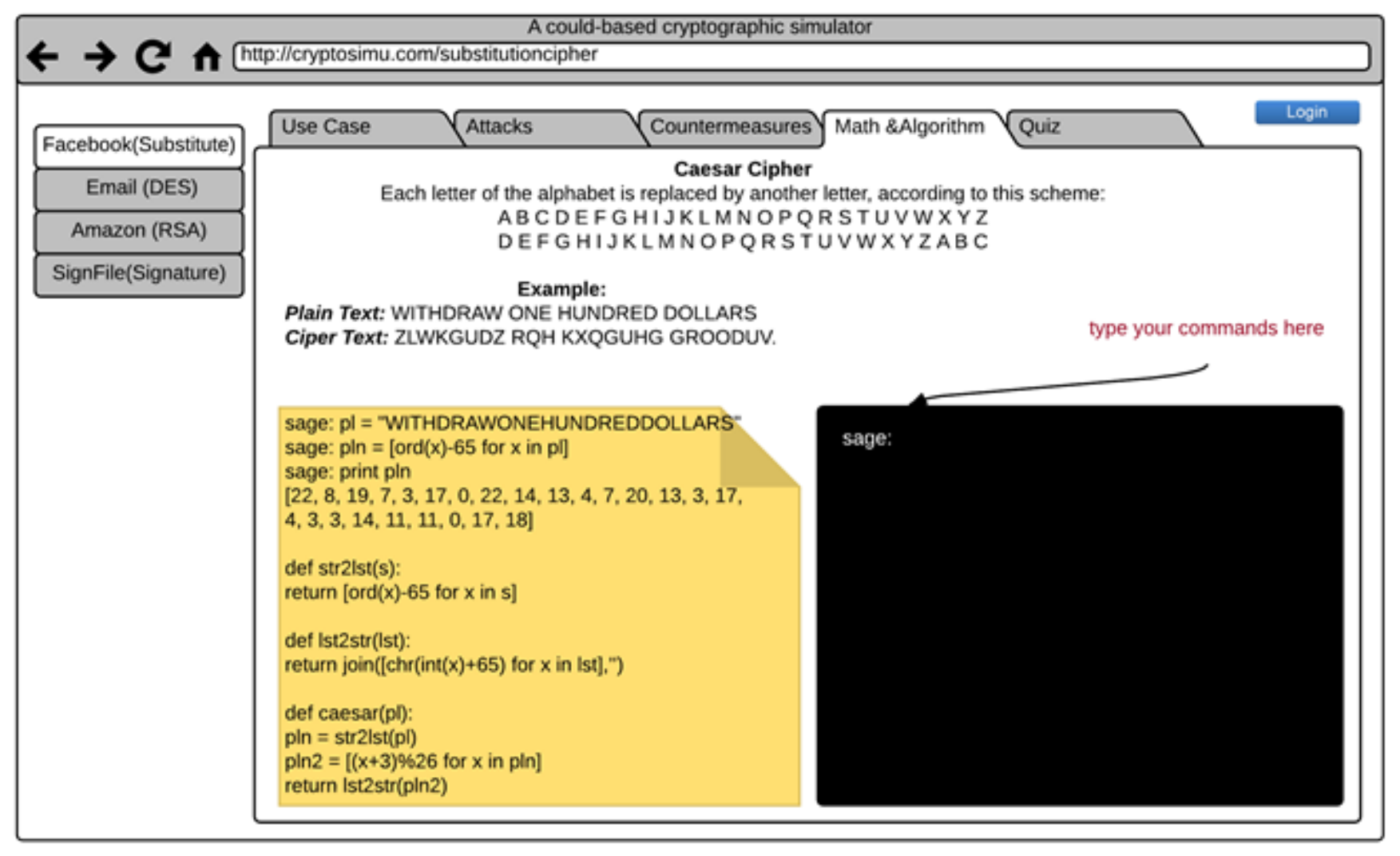
- Cryptography is one of the most important tools for building secure systems. It can be used to achieve several goals of information security. Through the proper use of cryptography, one can ensure the confidentiality of data, protect data from unauthorized modification, and authenticate the source of data. In cyber security, cryptography is a very important and necessary tool that covers encryption and decryption algorithms, cryptographic protocols, and cryptanalysis. Due to the importance of cryptography, National Centers of Academic Excellence (CAE) guidelines have included cryptography as the core knowledge for information assurance and cybersecurity education accreditation. These guidelines have been incorporated into the syllabi and curriculum of colleges offering computer science and information security as majors. However, there are still a few major barriers for students at HBCU institutions to comprehend the core concepts of the cryptography.

Project Goals

With this project, we aim at implementing a cloud-based cryptographic simulator with a contextualized learning approach to help students comprehend the fundamental concepts of cryptography, including protocols and cryptanalysis, and studying to what extent that the simulator can enhance undergraduates' learning experience.

Approach/Methodology

- Pick the Undergraduate Cryptography course (COSC 445 - Fundamentals of Cryptography & Applications) at Bowie State University for the empirical study.
- Students in the classes will be divided into groups.
- Each lab is designed for two-and-a-half hours to be consistent with the length of the current lectures.
- At the completion each lab, all students will take post-lab quizzes and turn in lab reports. Faculty will use the same rubrics for grading.

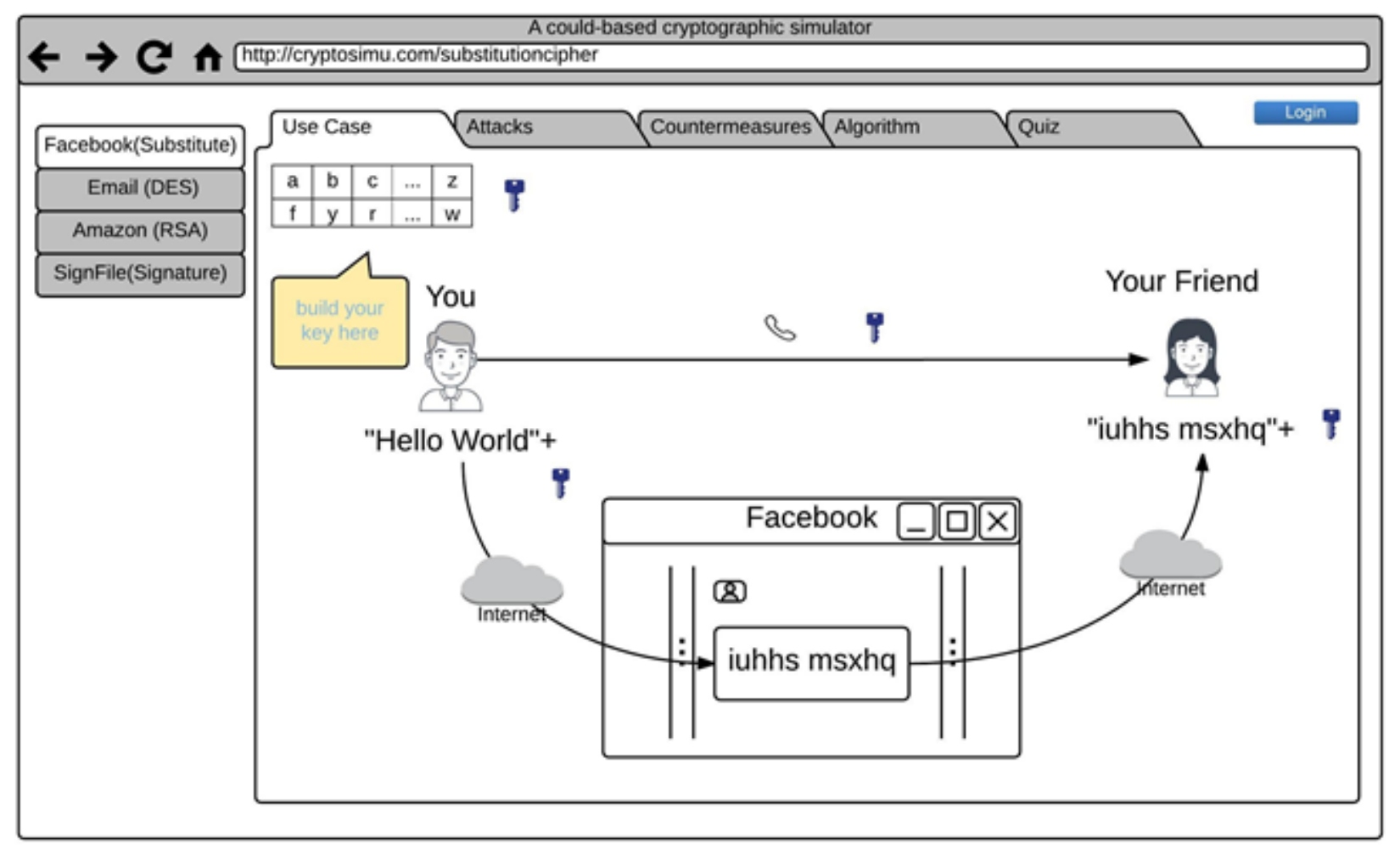


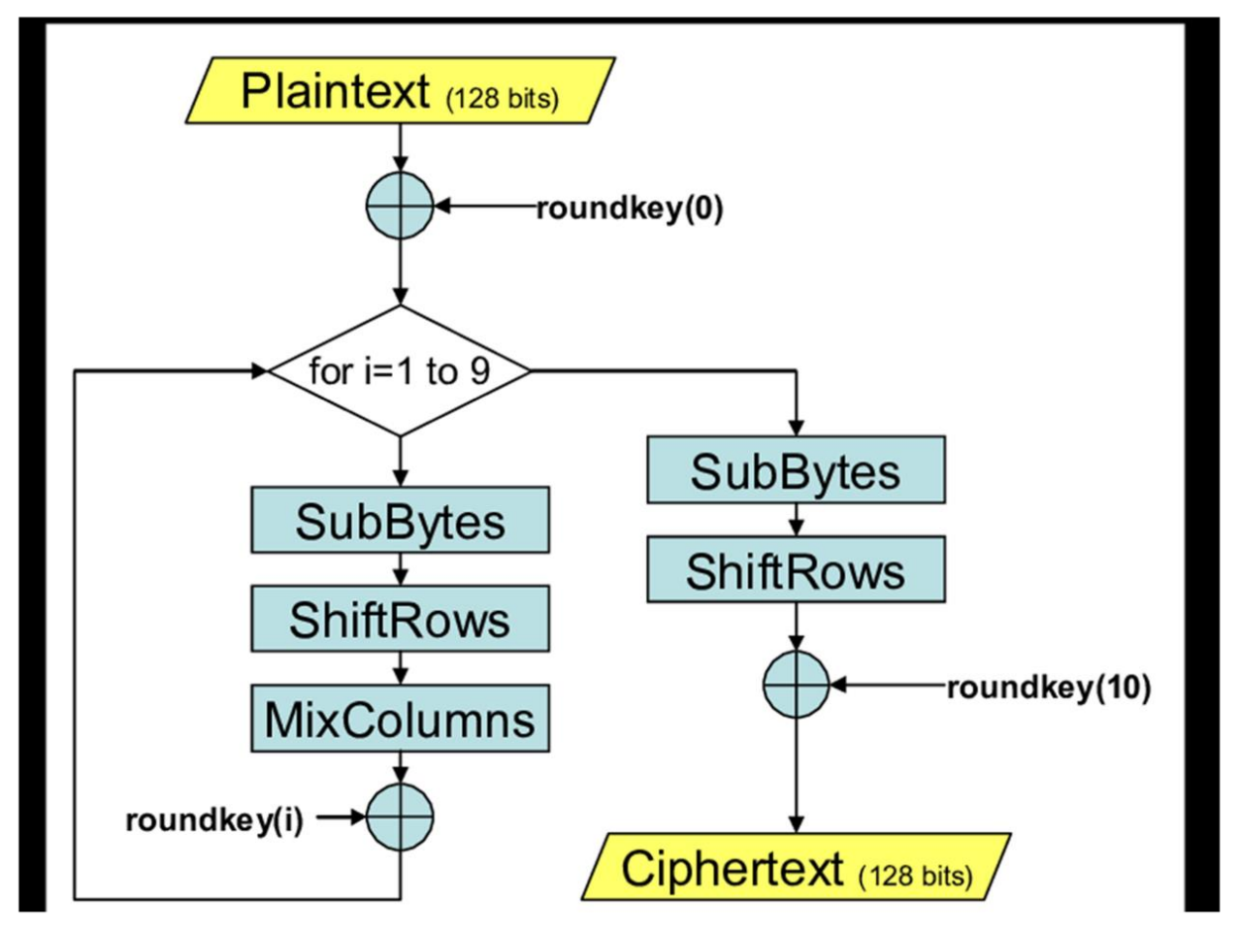
Caesar Cipher
Each letter of the alphabet is replaced by another letter, according to this scheme:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

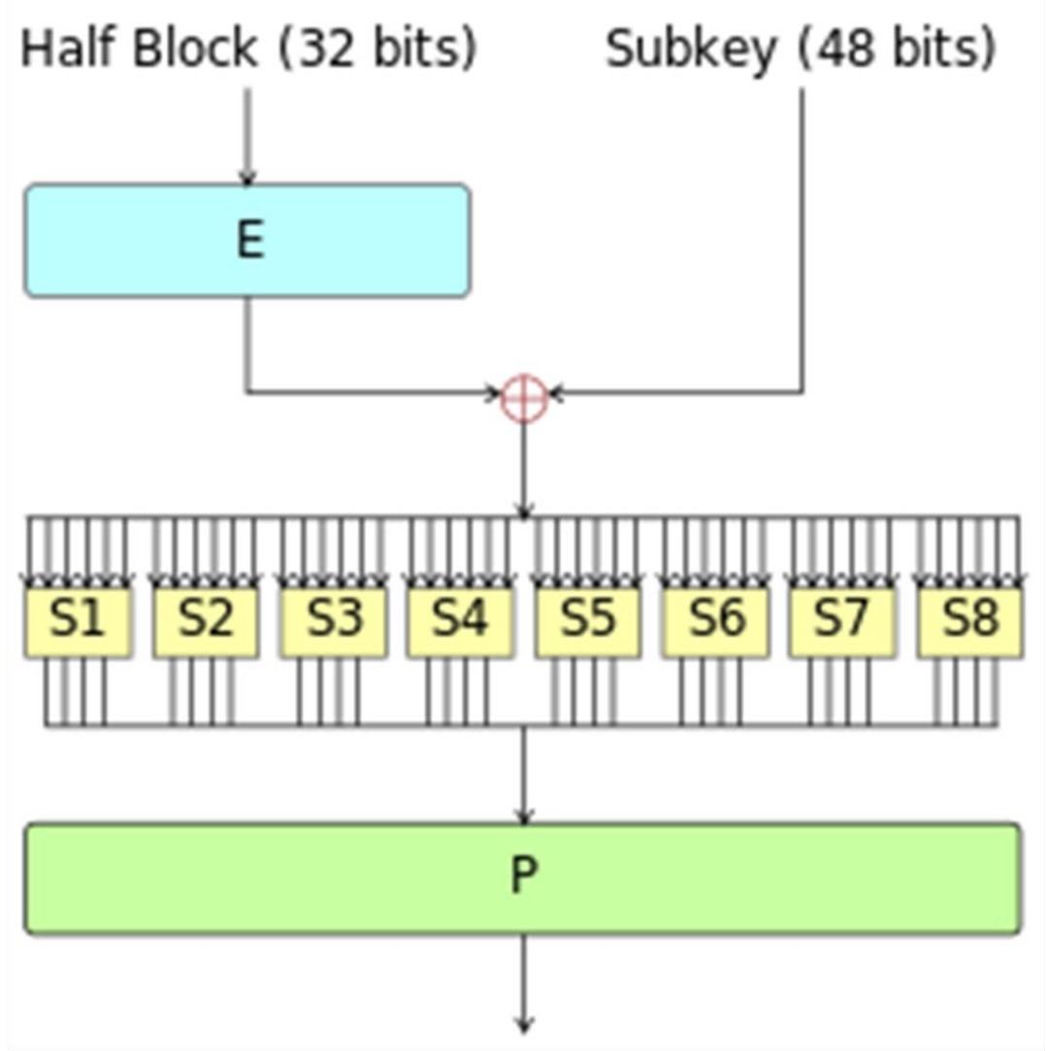
Example:
Plain Text: WITHDRAW ONE HUNDRED DOLLARS
Ciper Text: ZLWKGUDZ RQH KXQGUHG GROODUV.

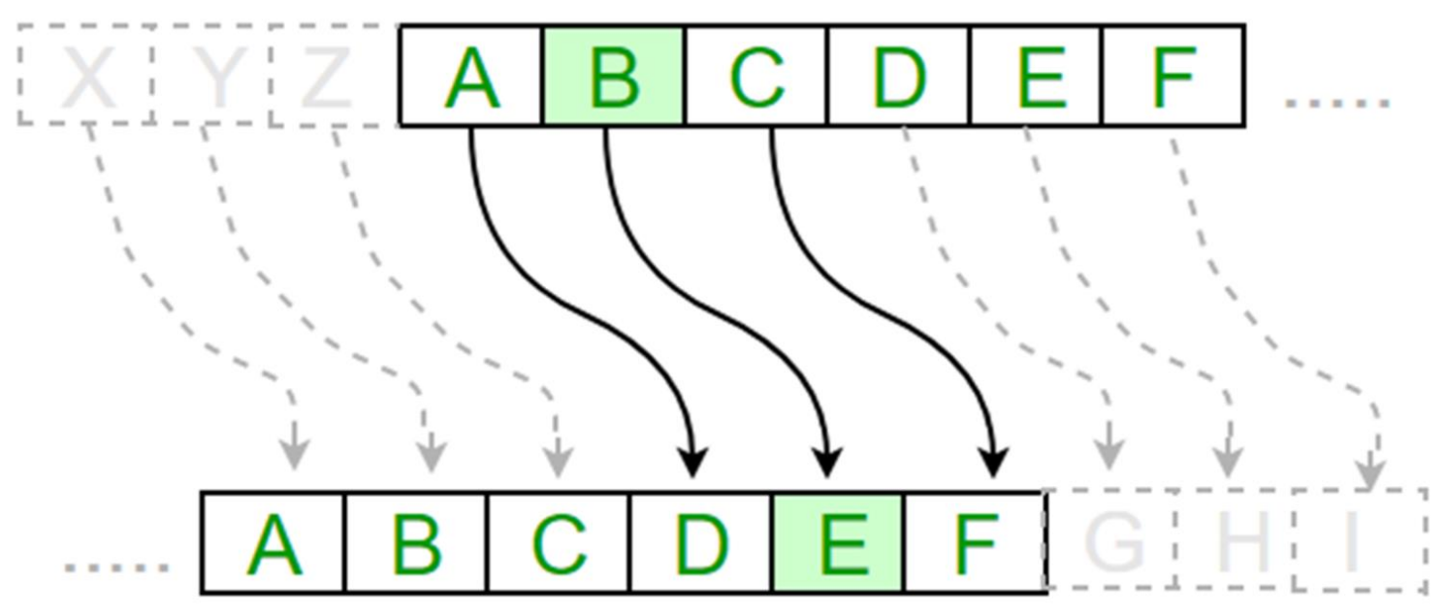
```
sage: pl = "WITHDRAWONEHUNDREDDOLLARS"
sage: pln = [ord(x)-65 for x in pl]
sage: print pln
[22, 8, 19, 7, 3, 17, 0, 22, 14, 13, 4, 7, 20, 13, 3, 17,
4, 3, 3, 14, 11, 11, 0, 17, 18]

def str2lst(s):
return [ord(x)-65 for x in s]

def lst2str(lst):
return join([chr(int(x)+65) for x in lst],'')

def caesar(pl):
pln = str2lst(pl)
pln2 = [(x+3)%26 for x in pln]
return lst2str(pln2)
```

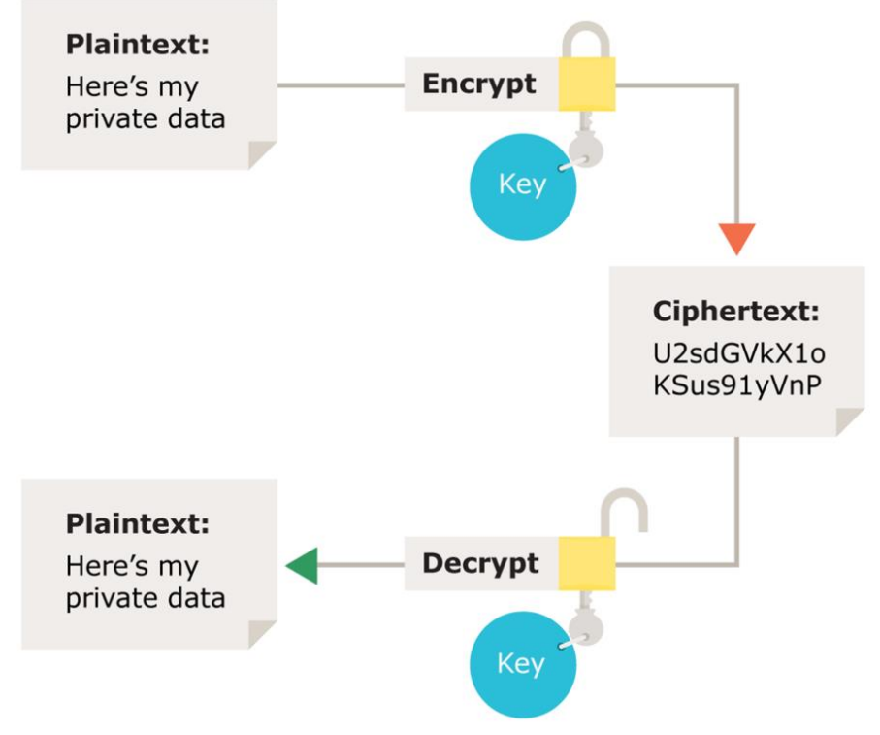
```
sage:
```











Project Evaluation

Project Outcome	Evaluation Method	Explanations/Benchmarks
Students performing contextualized learning	Document the rationales to proposal real-world use cases related to cryptography	Results will cover major cryptography topics, including symmetric and asymmetric ciphers
	Document the rationales and steps to real-world misuse cases from the attackers' and adversaries' perspectives	Results will indicate the importance of cryptography from different perspectives
	Perform student learning outcome assessment for proposed course; Survey students for degree of satisfaction with the contextualized learning	Outcome assessment and surveys will collect student and instructor perceptions of effectiveness in achieving the teaching and learning objectives
Students exploring the cryptographic content knowledge	Document and trace the cryptographic content knowledge units covered by use/misuse cases	Documents will be used to show knowledge units covers CAE criteria
	Implement the cryptographic simulator with knowledge units	The implemented simulator includes the proposed use/misuse cases covering the knowledge units
	Perform student learning outcome assessment for proposed course; Survey students for degree of satisfaction with knowledge units	Outcome assessment and surveys will collect student and instructor perceptions of effectiveness in achieving the teaching and learning objectives
Maintain the CAE accreditation	Document all empirical study activates, such as pre-/post-surveys and quizzes	The results will be used for maintaining CAE accreditation in 2021
	Document feedback from faculty workshops	

Future Work

- The primary goal is to have a workshop for cybersecurity faculty on how to properly integrate this research into their curriculum.
- Implement this approach in the classroom and gather student data for analysis.