Cryptanalysis of Book-Caesar-RSA Cipher

Samanvitha Basole and Shubham Pachpute

CS 265 Cryptography and Computer Security

San Jose State University

March 8, 2018

1 Problem Statement

...

2 Approach

In this paper, we solve the BCR cipher consisting of a three-stage cascade: Altered book, Caesar, and RSA. Each stage uses the output of the previous one as input as shown in Figure 1. We discuss the high-level algorithm design of Book, Caesar, and RSA ciphers, then we

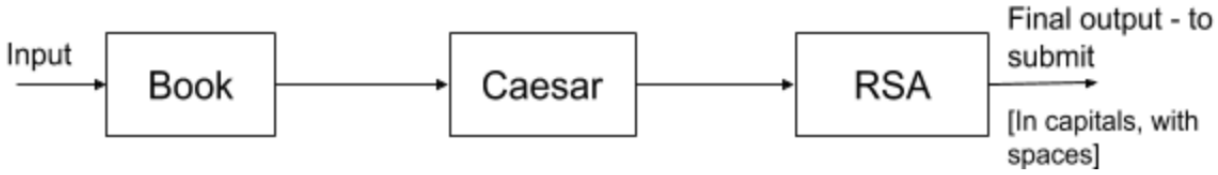

Figure 1: General Architecture

present the algorithm pseudocode and part of the implementation. Next, we explain our decryption process and analysis achieved through computational experiments. Finally, we provide screenshots of our solution and submission.

3 Algorithms Discussion

3.1 Book Cipher

3.2 Caesar Cipher

Caesar cipher is a simple substitution cipher in which the alphabet is shifted a certain number of characters based on the key. It is a symmetric key algorithm, that is, the same key is used

for encryption and decryption [1].
We show the following example to demonstrate encryption and decryption using Caesar cipher: Given a Caesar cipher with a left shift of 3, we first convert letters to numbers:

Letters:	A	B	C	D	E	F	...	X	Y	Z
Numbers:	0	1	2	3	4	5	...	23	24	25

To encrypt the plaintext 'ATTACK AT DAWN', we

- Transfom each letter in the plaintext into a number using the above scheme
- Apply the rule: (number + key) mod 26 to each transformed number
- Tranform each number back to its corresponding letter using the same scheme above

The result is the following ciphertext XQQXZH XQ AXTK.
Decryption is done in a similar way except the following rule is applied in the second step: (number - key) mod 26.

3.3 RSA

4 Algorithms Pseudocode

...

5 Decryption and Analysis

...

6 Solution Submission

...

References

[1] Bruce Busta. Encryption in theory and practice. *The CPA Journal*, 72(11):42, 2002.