WRITEUP - ASGN4

Viveka Agrawal

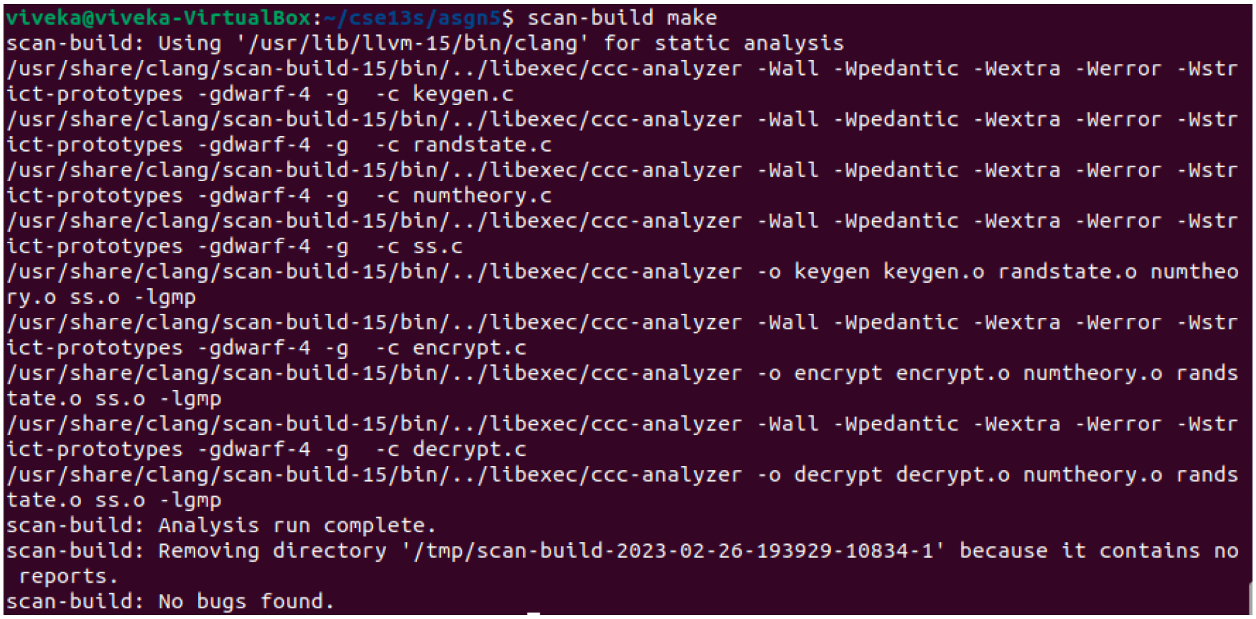
CSE13S, Winter 2023

In this assignment, I learned how to implement a cryptographic program. The program is used for encrypting messages using a public key and decrypting the coded message using private keys. We are implementing the Schmidt-Samoa Algorithm to test the primality of a number to determine if it is a prime or a composite number. The program is implemented in 3 parts: a key generator, an encryptor, and a decryptor. The key generator generates 2 keys - a public key n and 2 private keys d and pq. The key generator first generates 2 large random numbers p and q such that p does not divide q - 1 and q does not divide p - 1. The program tests if these large numbers are prime numbers using the Schmidt-Samoa Algorithm. Once p and q are determined to be prime, a public key is generated from these numbers using the formula n = p squared times q. Private keys pq and d are also calculated as follows: pq is calculated from lcm(p - 1, q - 1) and d is calculated from the inverse of n modulo pq. The encryptor then encodes the message m using public key n and produces the coded message c. The decryptor reads in the coded message c and decrypts it using the private keys d and pq to produce the original decoded message m.

Before this assignment, I was not aware of how cryptography works. Now, I understand that cryptography is important for encrypting secure transactions, such as online banking, so when I access my online bank account, my data is encrypted and decrypted using cryptographic algorithms.

Cryptogrophy enables secure communication between 2 parties on the internet, so the data sent by the sender is encrypted using the public key which is known to everyone, but only the receiver can decrypt the message using their private key which is only known to the receiver.

The autograder on git shows a ?? for me for scan-build even though there are no bugs reported in my program. Here is the proof:



```
viveka@viveka-VirtualBox:~/cse13s/asgn5$ scan-build make
scan-build: Using '/usr/lib/llvm-15/bin/clang' for static analysis
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c keygen.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c randstate.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c numtheory.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c ss.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -o keygen keygen.o randstate.o numtheo
ry.o ss.o -lgmp
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c encrypt.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -o encrypt encrypt.o numtheory.o rands
tate.o ss.o -lgmp
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -Wall -Wpedantic -Wextra -Werror -Wstr
ict-prototypes -gdwarf-4 -g  -c decrypt.c
/usr/share/clang/scan-build-15/bin/../libexec/ccc-analyzer -o decrypt decrypt.o numtheory.o rands
tate.o ss.o -lgmp
scan-build: Analysis run complete.
scan-build: Removing directory '/tmp/scan-build-2023-02-26-193929-10834-1' because it contains no
 reports.
scan-build: No bugs found.
```