Project 3

Honya Elfayoumy
helfayoumy3@gatech.edu

TASK 2

Since a lot of people like to use common passwords, a suggestion I could implement to improve password security would be to require multifactor authentication. Many applications use this nowadays to increase security measures for their users. It helps protect the user's account by requiring the user to verify their identity through another method instead of just using a password. Passwords are generally "easier" to hack whereas multifactor is more complex to hack. An example of a common multifactor authentication is verification code via SMS. Other methods that can be implemented are biometric scanners (such as fingerprint). Georgia Tech uses Duo to send a one-time token that allows for a second method of verification - this would also be a viable method.

TASK 3

Proof of work is a consensus algorithm that is used in kernelcoin blockchain. An alternative to the consensus mechanism is proof of capacity. This system requires more hard drive space typically since it generates plots from datasets stored on the hard drive. As the number of plots increases, there is a higher chance for the algorithm to find the next block in the chain. Whereas with proof of work, the transactions are secured by validating each block every second. Proof of work requires powerful hardware such as CPUs and GPUs.

Strengths (compared to proof of work)

Greener option

More energy efficient

No special hardware needed

Low entry barrier

Weaknesses (compared to proof of work)

Not as popular

Can be infected by malware

Finding Consensus 4/4: Alternative Consensus Mechanisms | by Till Antonio Mahler | blockwhat? | Medium

Proof of Capacity (Cryptocurrency) Definition (investopedia.com)

TASK 4

Your answer here..

TASK 5

It is known that n = p * q and it is assumed that p and q are prime numbers. In this function, p <= q. If you can divide by 2 evenly into n, then it is not prime so I will use p = 2 to check if n % 2 = 0. I check through all odd numbers to find the value for p. Once I find the value for p, I can find q by doing n / p. Once I find p and q, I can find the private key by following the steps of RSA as follows:

d * e = 1 (mod phi(p * q))

d = inv(e) (mod phi(p * q))

TASK 6

The public key used in this task is vulnerable because n1 and n2 share a common factor other than 1. Given that scenario, it is easy to find the common factor. The steps taken to derive the private key in this task was to find the common factor for n1 and n2. If the greatest common factor is not 1, then the private key is discovered.

TASK 7

According to the RSA broadcast attack, if a message is encrypted by different public keys with the same exponent, it would look like this:

C1 = $m^3 mod\ n_1$

C2 = $m^3 mod\ n_2$

… etc.

course-paper-5600-rsa.pdf (utc.edu)

I am able to use the Chinese Remainder Theorem to obtain the number before the mod operation was performed to get pow(m,3). Then I calculated the

Chinese remainder theorem - Wikipedia