RSA and Pseudoprimes

Aslihan Okur
Ataollah Hosseinzadeh Fard
Berkay Baris Turan
Mustafa Yagiz Kilicarslan

Historical Context

People have been using different types of approaches to hide their individual information. A common approaches implementing private key algorithms in which both receiver and addresser must have access to the algorithm so as to exchange the private information. However, sharing private keys decreases the security of the system. Hence, computer scientists came up with a different approach which is public key cryptography. Public key is a communication type that transforms information into an indecipherable format, making communications more secured. RSA being one of the first encryption (deciphered) systems, it is still one of the most common systems used for secured information.

Mathematics

Euler's Totient Function

Euler's totient function determine the number of positive integers which are smaller than a given number n and relatively prime with n. If n = p q where p and q are two prime numbers, then "ϕ(n) = (p - 1) (q - 1)". This relation provides the main mathematical component in RSA.

Fermat's Little Theorem

Fermat's Little Theorem states that if p is a prime number, then $a^p \equiv a \ (mod\ p)$. Therefore, it was used as a criterion to test integers for primality. Nonetheless, there are integers which are not primes, yet they satisfy Fermat's Little Theorem. The aforementioned numbers behave like primes in the sense of Fermat's Little Theorem whereas they are not primes. These numbers are called pseudoprimes. We use this theorem to generate suitable numbers for our purpose.

Computer Science

How Does It Work ?

In RSA system, usually two large primes are chosen using Fermat's Little Theorem, which almost always produces a prime with some exceptions of pseudoprimes. These numbers, which are represented by 'p' and 'q', are crucial since they make code harder or easier to 'hack' regarding their properties.

Totient Function basically tries to calculate the numbers that are relatively prime to the given number, in this case 'n = p . q', p and q being the 'probable primes' determined by Fermat's Little Theorem, as explained above.

Steps:
1- Two Large 'Probable Primes' are determined, 'p' and q'.
2- Compute 'n = p * q' and 'ϕ(n) = (p - 1) (q - 1)'.
3- Choose an encryption key 'e' relatively prime to ϕ(n)
4- Calculate the decryption key 'd' such that ed = 1 (mod φ(n)).
5- Publish e and n, and keep d, p, and q secret.
Al being a public-key algorithm, after the message is cyphered by public-key, one who wants to decipher it must know the private key, if not they must factorize two very large primes. Since computers must compute each possibility one-by-one, it takes years to solve this overwhelming problem.

How to Hack It ?

In Unix based operating systems, programs can be found that can be used to crack RSA systems. These programs employ "Brute-force attacks" which consecutively try every possible configurations, to find these prime or pseudoprimes, until they findthe right configuration. The time exhausted by such programs is the time complexity needed to crack an RSA system. In nowadays, when RSA is used, there are three cases. These cases correspond to using: "Two Primes", "A prime and a Pseudoprime", or " Two Pseudoprimes". Analyzing time Complexity, RSA is more secure, i.e., takes longer time to be cracked, when "Two Pseudoprimes" are used. It is worth mentioning that nowadays standard RSA systems are based on "Two Primes" in general.

Time complexity of different cases for using RSA

SCAN ME

Demo Program

Conclusion

The objective of this study is to observe the possible outcomes when we use pseudoprimes instead of primes in RSA systems. According to data we collected from research and the code we wrote, our conclusion is that using pseudoprimes instead of primes increases time complexity; in other words, it enhances the security of RSA system. This is conditional on using relatively large pseudoprimes in the algorithm.

References

- Cook, J. D. (2018, December 12). RSA encryption exponents are mostly all the same. Retrieved March 5, 2020, from https://www.johndcook.com/blog/2018/12/12/rsa-exponent/Weisstein, Eric W.
- Frankenfield, J. (2020, January 29). Private Key. Retrieved March 5, 2020, from https://www.investopedia.com/terms/p/private-key.asp
- "Fermat's Little Theorem." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/FermatsLittleTheorem.html
- Private key generation from on-line handwritten signatures. (2002, October 1). Retrieved March 5, 2020, from https://www.emerald.com/insight/content/doi/10.1108/09685220210436949/full/html
- Rouse, M. (2019, May 8). What is a Private Key? - Definition from WhatIs.com. Retrieved March 5, 2020, from https://searchsecurity.techtarget.com/definition/private-key
-The History of Cryptography. (n.d.). Retrieved August 2020, from https://cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/history.html
- What is a Public Key? - Definition from Techopedia. (2012, November 19). Retrieved March 5, 2020, from https://www.techopedia.com/definition/16139/public-key