Diffie-Hellman Protocol: Prime Numbers as an Early Tool for Enhanced Data Encryption

Raoul Friedemann

Occidental College

April 26, 2016

Abstract

The Diffie-Hellman Protocol (DHP) was one of the earlier methods for encrypting data transmitted between two private computers through a public media inundated with potential eavesdroppers. DHP was an early contributor to other equally powerful encryption tools such as RSA encryption. DHP introduced the discrete logarithm problem as well as the solution through exponential primes and the modulo function. I will substantiate the assertion of exponential time complexity via the properties of prime numbers and the Fundamental Theorem of Arithmetic.

Outline

- Conceptual background on DHP in the classical key-exchange depicting Arya transmitting an encrypted message to Bran through a public medium exposed to an eavesdropper, Cersei.
- Discuss the application of this protocal through prime number exponentiation and modulo functions thereby introducing the discrete logarithm problem as well as the formula

$$(x^a)^b mod(p) \equiv (x^b)^a mod(p)$$

- Provide a simple mathematical example illustrating how numerical data could be securely transferred without the need to send a key.Use this example to illustrate the questions that are raised about potential flaws with the operation.
- Introduce the time-complexity effects stemmed from prime factorization problems requiring exponential time.
- Explain the impacts that carried and compare to the RSA encryption method which utilizes a similarly effective method of public-key encryption.

References

Tao, T. (2007, January 17). Lecture on Structure and Randomness in the prime numbers. University of California Los Angeles. Los Angeles.

-

Terr, D. (n.d.). Diffie-Hellman Protocal. Retrieved from MathWorld–A Wolfram Web Resource: http://mathworld.wolfram.com/Diffie-HellmanProtocol.html

-

Weisstein, E. W. (n.d.). Discrete Logarithm. Retrieved from MathWorld–A Wolfram Web Resource: http://mathworld.wolfram.com/DiscreteLogarithm.html