CS 333 - Algorithm Analysis

Spring 2020

Research Project

Group members: Arman Hasanzade, Güneş Büyükgönenç, Ahmet Yıldırım, Cem Denizsel

Title: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems by R.L. Rivest, A.Shamir, and L. Adleman

The article talks about the privacy and the ownership of messages or mails sent online and how to encrypt the messages such that only the intended receiver can read it.
The writers describe the Diffie, Hellman [1] algorithm and propose their own idea and method of encryption, which is inspired by Diffie, Hellman algorithm of encryption.
The algorithm of the authors uses similar mathematical functions as the original algorithm, however the authors utilize "Prime number factorization" for an easy to encrypt but hard to break / decrypt algorithm. They call their algorithm a "trap-door one-way permutation", because using the prime numbers, it is easy to encrypt the message such that anyone who is eavesdropping receives garbage, but also easy to decrypt the message when you have the key (trap-door).
The article also talks about "signing" the messages such that the sender cannot deny the fact that s/he did not send the message. This is important for online business transactions and important mails.

We are planning to implement the algorithm described in the paper. For additional resources, the authors suggest readings from Diffie, Hellman [1][2] before reading the algorithm described in the paper.

References:

- *[1] Diffie, W., and Hellman, M. New directions in cryptography. IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654.*
- *[2] Diffie, W., and Hellman, M. Exhaustive cryptanalysis of the NBS data encryption standard. Computer 10 (June 1977), 74-84.*