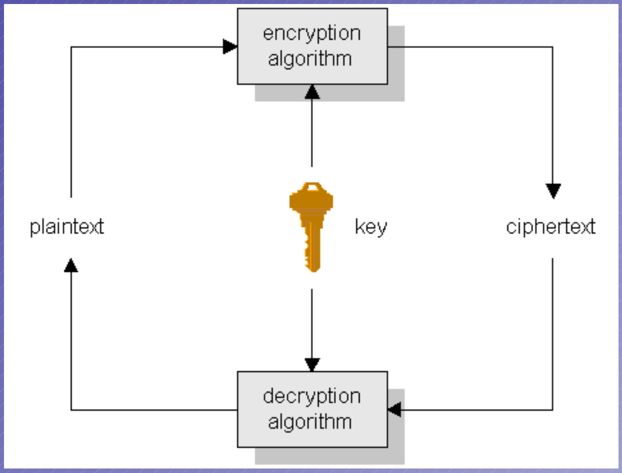
Benchmarking of Cryptographic Algorithms

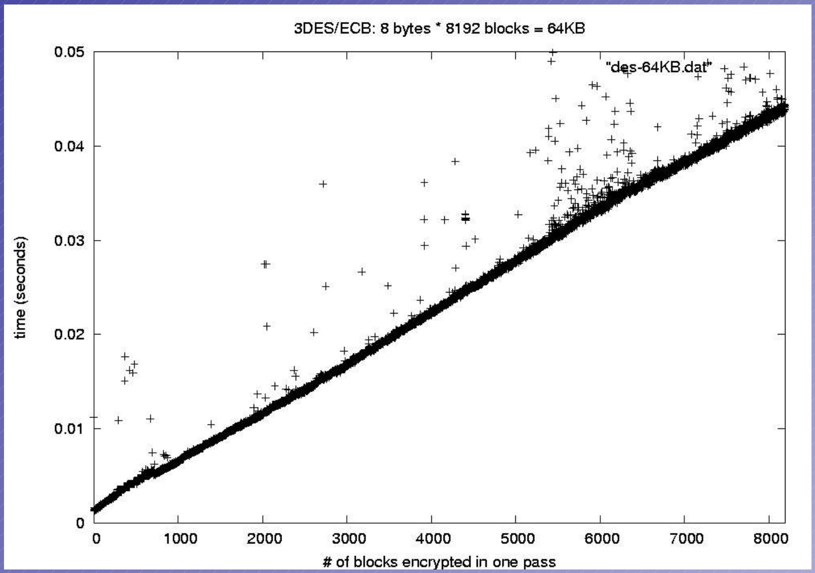
Alex Volkovitsky
February 2, 2005

Abstract

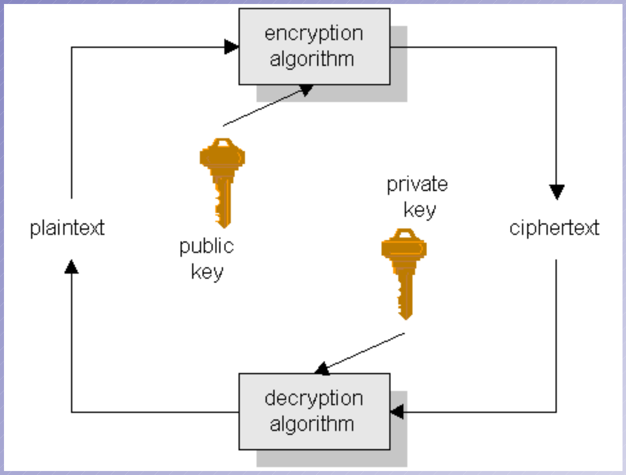
The author intends to validate theoretical numbers by constructing empirical sets of data on cryptographic algorithms. This data will then be used to give factual predictions on the security and efficiency of cryptography as it applies to modern day applications.



Symmetric key algorithms, such as DES, use the same key to encrypt and decrypt. Pro: speed, Con: key needs to be shared over a previously established secure connection



A graph showing the relationship between the amount of plaintext and the time taken to encrypt it, using a 3DES algorithm in ECB mode. Due to the nature of ECB, the progression is clearly linear. The slope of the line can be interpreted as the time taken to encrypt one 64Kb block, and the y-intercept is assumed to be the overhead of the program.



Due to the insecure nature of the Internet, public key algorithms, such as RSA, have become widely popular. These algorithms rely on NP-hard mathematical problems (those without an easily derivable solution, such as factoring) to exchange data without having to divulge the private key. Pro: easily established over any connection. Con: not suitable for large chunks of data due to high amounts of computation.