Conference in Numerical Analysis 2014 (NumAn 2014)
September 2-5, 2014
Chania,Greece

Symmetric Key Cryptography Algorithms Based on Numerical Methods

Youssef Hassoun[a] **and Hiba Othman**[b]

[a,b]Department of Mathematics, American University of Science and Technology, Beirut, Lebanon

yhassoun@aust.edu.lb,hothman@aust.edu.lb

Abstract

Cryptography is used to protect information content communicated over a network from being accessed by adversaries. This is achieved by transforming (encrypting) plaintext before transmission in such a way that its contents can only be disclosed upon application of a reverse transformation (decryption). Both transformations involve a secret component which can be either the transformations themselves or some key used in the process. This paper focuses on implementing symmetric-key cryptography algorithms based on numerical methods. An empirical study is performed investigating the correlation of encryption and decryption efficiency of different root-finding numerical methods to the size of the plaintext and to key parameters.

There are two categories of key-based cryptographic algorithms[1], symmetric-key and asymmetric-key or public-key algorithms [1, 2, 3]. In the first category, sender and recipient share a private key known only to both; the same key is used for encryption and decryption. By contrast, in public-key cryptography two keys are used, one key is made publicly available to senders for encrypting plaintexts while a second key is kept secret and is used by the recipient for decrypting ciphered texts.

Depending on the plaintext chunks on which an algorithm operates, symmetirc encryption algorithms are classified as stream and block ciphers. Stream ciphers operate on individual characters one at a time using time-varying encryption transformation. Block ciphers, on the other hand, operate on blocks of characters ($n \geq 64$ bits) using fixed encryption transformation.

Menzes et. al [3] defines a block cipher as an encryption function which maps n-bit plaintext block into an n-bit ciphertext block, where n represents the *blocklength*- a substitution cipher with a large character size. The function is bijective and is parametrized by a k-bit key. DES is an example of a 64-bit block cipher with a 56-bit key. Caesar cipher can be classified as a block cipher with one character block and a shift of k characters as key.

We propose a symmmetric-key encryption algorithm based on solving a system of linear equations. It is a block cipher that maps n-characters of plaintext into n-characters of ciphertext. The

[1]Hash functions are one-way and do not fall into these categories, since there is no decryption

key consists of $(n \times 1)$ vector b_j and an $(n \times n)$ matrix (a_{ij}). Encrypting a block of n characters, represented by $(n \times 1)$ vector (c_j), is achieved by solving the systems of linear equations:

$$\sum_{i=1}^{n} a_{ij} x_j = b_j - c_j \qquad (I)$$

Provided that $det(a_{ij}) \neq 0$, the solution vector (x_j^*) exists; it represents the cipher text and is of dimension $(n \times 1)$. The condition on (a_{ij}) guarantees that encryption function is bijective and, consequently, has an inverse- the decryption function. Decrypting the ciphered text is achieved by substituting solution vectors into equation (I) giving rise to $c_j = \sum_{i=1}^{n} a_{ij} x_j^* - b_j$.

Another algorithm proposed in [4] and based on solving non-linear equations can also be classified as a 1-character block cipher. Any non-linear function with one variable can be defined as a key[2]. The encryption function is defined as finding the solution of the equation:

$$f(x) - c_i = 0 \qquad (II)$$

Here, (c_i) represents the numerical code of the i^{th} character in the plaintext, e.g., the ascii-code, and $f(x)$ is an arbitrary non-linear function, polynomial or otherwise. To guarantee that encryption function has an inverse, numerical encoding of plaintext together with $f(x)$ must be chosen in such a way that equation (II) has at least one real root. The set of resulting roots $\{x_i^*\}$ represents the ciphertext. On the recipient side, each entry (x_i^*) in the ciphered text is decrypted by substituting it into $f(x)$ giving rise to $c_i = f(x_i^*)$.

To conclude, we propose symmetric encryption algorithms based on solving a system of linear equations as well as solving non-linear equations using numerical methods [5]. The proposed cryptosystems are block ciphers with matrices and non-linear functions as private keys. To make encryption functions invertible, and thereby guarantee decryption, the keys are constrained to satisfy some conditions. We implement the algorithms and perform an empirical study investigating the efficiency of encryption and decryption functions in terms of the functions' parameters and in terms of plaintext message size.

References

[1] N. Ferguson, B. Schneier and T. Kohno (2010). Cryptography Engineering. John Wiley & Sons. ISBN: 9780470474242

[2] B. Schneier (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons. ISBN: 0471117099

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone (1996). Handbook of Applied Cryptography. CRC Press. ISBN: 0849385237

[4] A. Ghosh and A. Saha (2013). A Numerical Method Based Encryption Algorithm with Steganography. R. Bhattacharyya et al. (Eds) : ACER 2013, pp. 149157. CS & IT-CSCP

[5] R. L. Burden and J. D. Faires(2010). Numerical Analysis, 9^{th} Edition. Cengage Learning. ISBN-13: 9780538733519

Key words: Cryptography, Encryption, Numerical Methods, Symmetric-Key.

[2]The authors in [4] proposed a polynomial function of degree 3 as a key