Chapter 4
Towards Parameterized Shared Key for AVK Approach

Shaligram Prajapat
Maulana Azad National Institute of Technology, India & Devi Ahilya University, India

Ramjeevan Singh Thakur
Maulana Azad National Institute of Technology, India

ABSTRACT

"Key" plays a vital role in every symmetric key cryptosystem. The obvious way of enhancing security of any cryptosystem is to keep the key as large as possible. But it may not be suitable for low power devices since higher computation will be done for longer keys and that will increase the power requirement which decreases the device's performance. In order to resolve the former specified problem an alternative approach can be used in which the length of key is fixed and its value varies in every session. This is Time Variant Key approach or Automatic Variable Key (AVK) approach. The Security of AVK based cryptosystem is enhanced by exchanging some parameters instead of keys between the communicating parties, then these parameters will be used to generate required keys at the receiver end. This chapter presents implementation of the above specified Mechanism. A model has been demonstrated with parameterized scheme and issues in AVK approach. Further, it has been analyzed from different users' perspectives. This chapter also highlights the benefits of AVK model to ensure two levels of security with characterization of methods for AVK and Estimation of key computation based on parameters only. The characteristic components of recent styles of key design with consideration of key size, life time of key and breaking threshold has also been pointed out. These characteristics are essential in the design of efficient symmetric key cryptosystem. The novel approach of AVK based cryptosystem is suitable for low power devices and useful for exchanging very large objects or files. This scheme has been demonstrated with Fibonacci-Q matrix and sparse matrix based diffused key information exchange procedures. These models have been further tested from perspective of hackers and cryptanalyst, to exploit any weakness with fixed size dynamic keys.

DOI: 10.4018/978-1-5225-0536-5.ch004

INTRODUCTION

"Sending and receiving information securely" is the sole objective of every communication system. The medium on which information is propagated has been transformed drastically due to growth in communication technology. As the transmission over public network takes places between unknown entities, ensuring security of information is a challenging task due to vulnerability of the public systems (Diffe & Hellman, 1977). Hence, ensuring security of information between participating entities is essential. Similarly, protection of data of interconnected machines within networked system from malicious damage is also desirable aspect of a successful cryptosystem. Since, the cryptosystem is exposed publicly in networked system. All of its components like plaintext, cipher text, key, enciphering algorithm and deciphering algorithms are available on the network either in hidden formats or exposed in some other way(depending upon mechanism) (Chakrabarti, et. al., 2008). Except the original text i.e. the plain text before leaving sender's machine, all other information is available in encrypted or hidden format. Among these components of symmetric key based cryptosystem, secrecy of key is important because if key is compromised, then rest other components are of no use. Using brute force attacks mechanism, weakness of these cryptosystems can be exploited, where cryptanalyst or attacker tries each possible key until the right key is found to decrypt the message (Prajapat & Thakur, *2015*). According to Moore's law, the power of personal computers has historically doubled approximately every 18 months. In addition, well equipped attackers often develop new techniques and algorithms to improve the efficacy of key search attacks. Therefore, estimate of the time required for successful key search attacks must be revised downward as the computing power and resources which are available to attacker's increases. Most of the time they are successful due to: availability and accessibility of fast computing resources, capability to use power of AI enabled algorithms, availability of sender/receiver's personal information to prune the search space making task of cryptanalyst and hacker's job easier (A. Nadeem et. al., 2005). With the growth of multi course processing, availability of CPU-GPU pairs parallel and grid based computing algorithms, the search time can be reduced to polynomial time from exponential (infeasible) in near future. Presently, to enhance the success rate of brute force attack best alternatives are:

- Reduce the life time of key.
- Increase the key length. In former approach by choosing the shorter key lifetime, one can reduce the possible potential damage even if one of the keys is known.

In later approach, choosing longer key length one can decrease the probability of successful attacks by increasing the number of combinations that are possible (Prajapat & Thakur, *2015*). The state of art symmetric key based cryptosystem trends towards increasing length of key for enhancing security, but it has certain side effects. It increases processing, resource utilization, and time consumption. In the next section of this chapter, we will learn the model of AVK, as a solution to the above problem. And subsequently we will learn to add extra security provision for this model of key exchange using exchange parameters only mechanism. The chapter also highlights novel methods for generating keys using parameterized key based cryptosystem.