Open Access Journal

Journal of Sustainable Research in Engineering Vol. 4 (2) 2018, 69-75

Journal homepage: http://sri.jkuat.ac.ke/ojs/index.php/sri

The use of RC4 Encryption to Provide Privacy for Smart Meters

Lincoln Kamau[1*], Kibet Langat[1] and Christopher Muriithi[2]

[1]*Jomo Kenyatta University of Agriculture &Technology, School of Electrical, Electronics and Information Engineering, Department of Telecommunication and Information Engineering, P.O. Box 62000 - 00200 Nairobi, Kenya*

[2]*Murang'a University of Technology, School of Engineering and Technology, Department of Electrical and Electronic Engineering, P.O. Box 75 – 10200 Muranga, Kenya*

[*]*Corresponding Author - E-mail: kamaulincoln@jkuat.ac.ke*

Abstract The electrical power grid is undergoing improvements and is being transformed to the Smart Grid. Smart Grid uses two-way power and information flow to better monitor, plan and control the electrical power grid. Advanced communications allow better service delivery, faster problem detection and correction, and more efficient distribution. However, the same heavy reliance on data that makes Smart Grid possible is the same source of its vulnerability: cyber attacks and privacy leakages. By accessing information on monitoring such as a household's power usage, it is possible to deduce when the owners of a home are present and even what electrical equipment they have. Such privacy leakages could be used in planning a break-in. To overcome this, we examine the use of encryption on smart meter data. This work uses a popular stream cipher known as RC4 (Rivest Cipher 4). We show that due to its low computational requirements, RC4 is a suitable candidate for encryption.

Keywords Cyber security, Encryption, Privacy, Smart meter, Smart Grid.

1. Introduction

The traditional electrical grid is being upgraded to a better system known as the Smart Grid. This new approach integrates modern telecommunication to run operations more effectively. It involves various players working together, communicating and cooperating with each other, as shown in Fig. 1**[**1**].**

A number of benefits result from this. Planning of power delivery is enhanced, because the supplier is rapidly updated on changes in demand and can make better decisions.

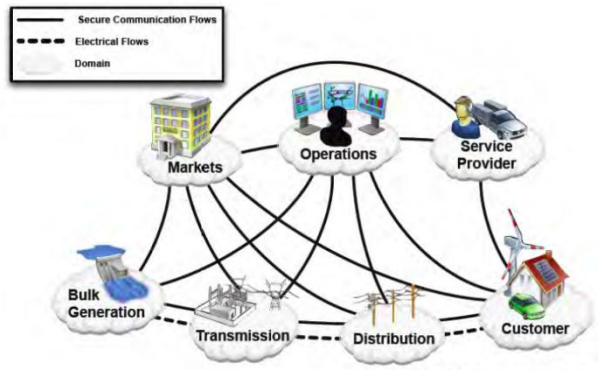

Fig. 1. Interaction of Actors in different Smart Grid domains through Secure Communication Flows

Monitoring is superior with more fine-grained information collected, yet with less manpower needed to collect it. Fault detection and correction is also

more automated. Demand Side Management (DSM) is also made possible. DSM is a technique that allows electrical loads to be shifted from peak to off-peak periods, thus reducing the cost of generating power **[**2**]**.

As a result, Smart Grid is able to better serve both the supplier and the consumer. There are less power outages, transmission losses, undetected faults and lower greenhouse gas emissions. It also allows for distributed power sources, more customer choices, and can increase the capacity of the existing electric power networks **[**3**]**.

However, the same enhanced communication that gives Smart Grid its strength is also one of its greatest sources of vulnerability. Taking up advanced communications brings with it not only the benefits in that field, but the difficulties as well. With more data being sent, there is a greater threat in terms of cyber threats and privacy leakage. When data consists of control and monitoring information of a system, and there are large numbers of users involved, then its protection becomes more very crucial.

If control information is corrupted by a hacker, it can cause the system to respond in unexpected ways – including power outages and damage of equipment. Fault response data could be delayed leading to system failure. Billing information can be modified, making a consumer's usage seem much less. If done on a large scale, this would result in massive energy theft. Such problems are the cyber threats that Smart Grid faces.

Monitoring information may fall into the wrong hands. A robber, a spy or an enthusiastic marketer can get a lot of information about a household by analyzing how power is consumed over time. Smart meters collect more data than traditional electrical meters. Such detailed consumption data would facilitate the creation of users' lifestyle profiles, with information such as when they arrive home, when they eat, etc **[**4**]**. Electrical devices within a household can also be identified, based on the pattern of how they consume power using a technique called Non-intrusive Load Monitoring (NILM) **[**5**]**. Fig. 2 illustrates the power of this technique to extract information from a household's electrical consumption data [6]. This derived information can be used to plan a break in, with the robbers not only being able to determine the best time to attack, but also the electrical devices they can expect to steal.Marketers could hound customers to buy their products based on studing their habits. Massive survelance is also possible. All this would be happening to unsuspecting victims who are in the safety of their homes.These are the privacy threats facing Smart Grid.

For Smart Grid adoption to be successful in the long term, cyber security and privacy concerns must be addressed. The intuitive solution of adopting standard methods used in computer securitywould fail for two reasons. First, Smart Grid devices use embedded systems, which have limited processing power and memory capacity. Second, some applications, such as fault detection, have very small time allowances (i.e. latency). This paper seeks to examine RC4 encryption algorithm as a possible technique to enhance privacy.

The rest of the paper is organized as follows: Section 2 looks at recommended security objectives for Smart Grid. Section 3 highlights cyber threats and privacy leakage. Section 4 briefly discusses encryption. The methodology is given in Section 5, followed by a discussion of the results in Section 6 and Section 7 concludes the paper.

2. Security Objectives

Before solving the security problems in any system, it is important to have clear objectives to aim for. Without these, one would not have an objective standard with which to determine if a system is secure. Three cyber security objectives are given for Smart Grid by the National Institute of Science and Technology (NIST) **[**1**]**: Availability, integrity and confidentiality.

Availability – Timely and reliable access to information. Loss of availability means that information is not delivered and could lead to power disruption.

Integrity – Delivery of information without improper modification or alteration. Loss of integrity could cause incorrect decision making resulting from using wrong or incomplete data.

Confidentiality – Protection of personal privacy and proprietary information from unauthorized access. Loss of confidentiality could expose crucial information to malicious parties.

This paper focuses on reaching the goal of confidentiality.

3. Cyber Threats and Privacy Leakage

Cyber attacks can have severe consequences on the Smart Grid. An attacker could change control signals, leading to massive blackouts and damage of equipment. Other attacks could simply involve inefficiency due to slowing down of communication in

and energy theft, through altering the billing or pricing information.

Attacks can be classified based on which security objective they hinder, giving us three categories **[**6**]**:

Attacks targeting availability, also called denial-of-service (DoS) attacks, attempt to delay, block or corrupt the communication in the Smart Grid.

Attacks targeting integrity aim at changing the data illegally or disrupting data exchange.

Attacks targeting confidentiality aim at acquiring unauthorized information from network resources in the Smart Grid. Wire tappers and traffic analyzers are in this group.

Encryption, which has potential to mitigate attacks on confidentiality, is examined in the next section.

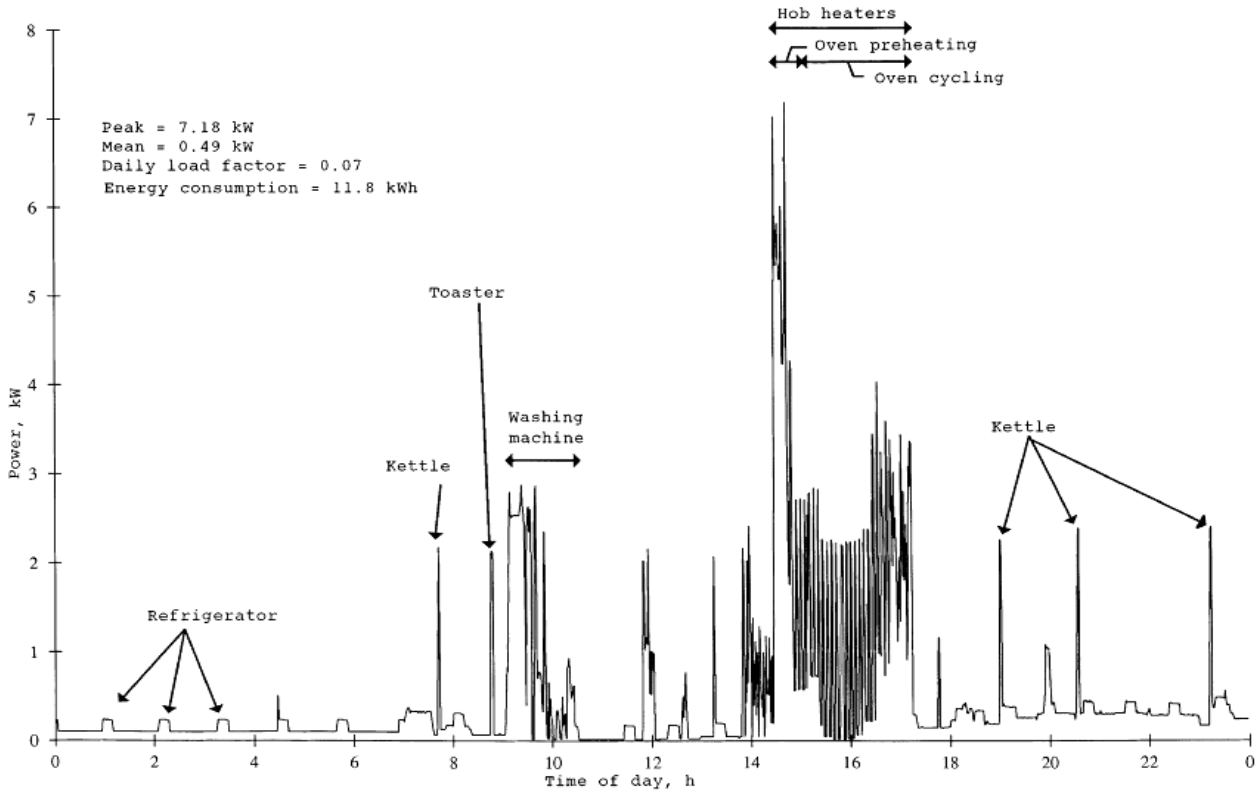

Fig. 2. Household profile with devices identified

4. Encryption

Encryption is a cryptographic technique used to provide secure communication and information protection. It makes it difficult for a third party to access information without permission. Encryption involves taking a message (known as the *plaintext*) and using a *key* to convert it to *ciphertext*, (which appears as illegible data).

The recipient of the message then uses the key to convert the ciphertext back to the legible plaintext. The harder it is for another party to obtain the plaintext from the ciphertext, the better the encryption technique.

Encryption techniques can be divided into two major categories, depending on how the key is used. Fig. 3 summarizes the classification.

Asymmetric key cryptography uses two different keys, a public and a private key, one for encryption and the other for decryption.

In *symmetric key* cryptography, the same key is used for both encryption and decryption. Asymmetric key cryptography generally requires more computation resources than symmetric key cryptography. For the same *security level*, a longer key is needed for asymmetric key encryption [8]. Thus, the use of asymmetric key encryption may be unsuitable in embedded computing systems.

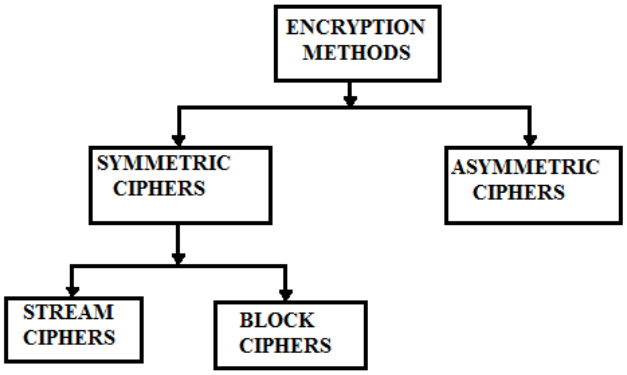

Fig. 3. Classification of Encryption

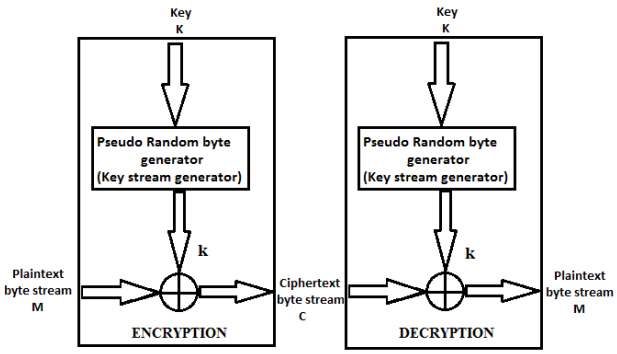

Fig. 4. Block diagram for a stream cipher

Symmetric key cryptography requires approximately constant computational resources regardless of the key size [7]. It is thus a preferred option for Smart Grid, which relies on embedded systems and has time critical operations.

Symmetric encryption can further be divided into two groups: block and stream cipher. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. A stream cipher encrypts plaintext one bit or byte at a time.

Stream ciphers are typically faster and use far less code than block ciphers [9]. This is an important advantage in smart meters.

The RC4 stream cipher algorithm is an efficient stream cipher. In it, plaintext is encrypted by taking its bitwise exclusive-OR (XOR) with a stream of bytes. If the plaintext stream is 01010101 and the key stream is 11011101, then the ciphertext is

plaintext 01010101
keystream 11011101 ⊕
ciphertext 10001000

Decryption does the same to retrieve the message:

ciphertext 10001000
keystream 11011101 ⊕
plaintext 01010101

Fig. 4 shows how RC4 stream cipher operates. A key is used to generate a stream of bits using a key stream generator. Using XOR, this stream is then used to convert the plaintext stream into ciphertext. The details for the RC4 algorithm, especially the key stream generator, are given in the appendix.

5. Methodology

To illustrate the impact of encryption using RC4 on consumption data, graphs were plotted before and after encryption. Plots of encryption data demonstrate that patterns used to monitor a household are no longer present. Without the key, it is very difficult to determine the original consumption and usage patterns. This difficulty is similar to the complexity one would meet when attacking the encryption scheme RC4. In addition, timing requirements are examined.

The pattern for the consumption at different times needs to be hidden from an eavesdropper who may have malicious intentions.

RC4 encryption was applied to the data. Different keys were used. Decryption was performed on one to see if the original result would be found. A wrong key was also tried to see if the original data can be retrieved without the right key. Finally, the time for encryption was determined.

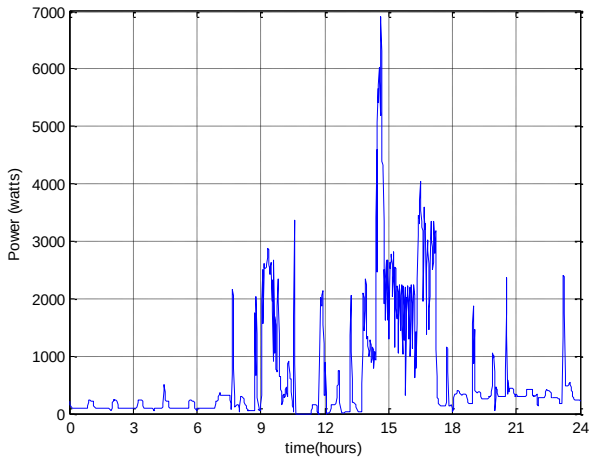

Fig. 5. Plot of estimated household consumption

The steps followed were:

1. The values of the graph in Fig. 2 were captured through image processing to produce Fig. 5.

2. Each value of demand was rounded off to the nearest integer and converted to binary. 10 bits were sufficient for all the values involved.
3. A stream of random bits (key stream) was generated using RC4 algorithm. A key of *[14, 10, 57, 34, 15, 7]* was used for the encryption. This key will be henceforth referred to as Key1.
4. XOR operation was applied to each 10 bit representation of energy demanded using 10 successive bits from the key stream.
5. The encrypted value was converted from binary to decimal representation and the resulting graph was plotted as shown in Fig. 6.
6. Decryption was performed to confirm that the results would be the same as the original. This is shown in Fig. 7.
7. Different keys were used on the same data of Fig. 5 to give Fig. 8 and 9. The keys used were *[2, 21, 200, 63, 0, 0, 7]* and *[2, 21, 200, 63, 0, 0, 6]*.These keys will be henceforth referred to as Key2 and Key3 respectively.
8. To demonstrate the effect of using a wrong key, Key2 was used to decrypt data that had been encrypted using Key3 (NB: These two keys differ by only one bit/digit). The results were as shown in Fig. 10.
9. For all encrypted graphs, the points x = 6 and x = 18 (i.e. 6am and 6pm respectively) were marked using a data cursor to distinguish the random looking graphs.
10. Time taken to perform the encryption was determined using Matlab's tool for examining computation, known as Profiler. Five (5) runs were performed to get average computation time.

6. Results

From the graphs of the encrypted data, privacy is created. Without the key, a person snooping would not be able to obtain power usage data. Once encryption is done, power usage patterns are concealed as shown in Fig. 6. Non-intrusive load monitoring (NILM) would not be able extract usage patterns from such random looking data.

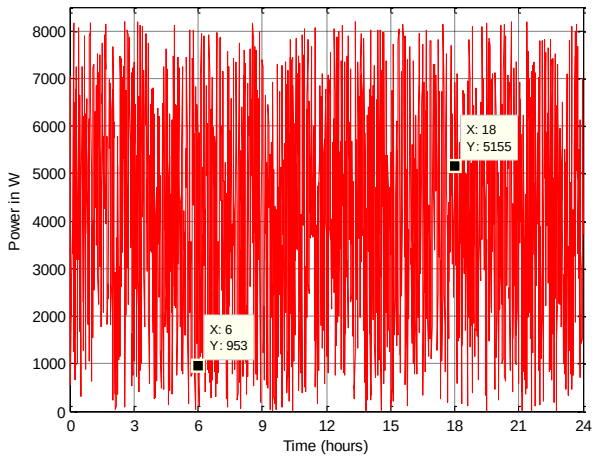

Fig. 6. Encrypted power demand.

Decryption of the above result gave the same results as the original curve. The resulting graph is shown in Fig. 7 and it matches Fig. 5.

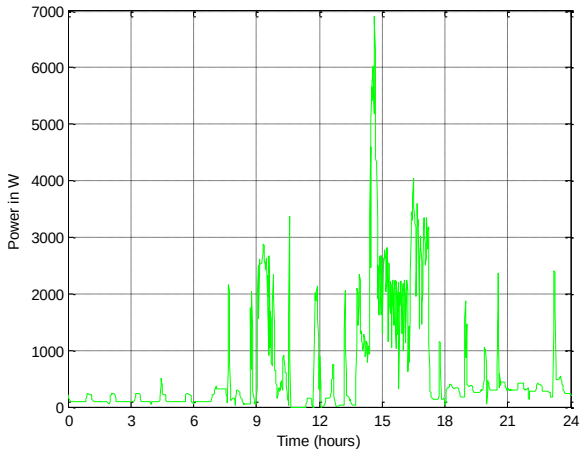

Fig. 7: Results after decryption

Different keys gave different results. For Key2 (i.e. [2, 21, 200, 63, 0, 0, 7]), the graph of Fig. 8 was obtained.

The different encrypted graphs can be distinguished by the data cursors at x = 6 (6am) and x = 18 (6pm). From Figures 6, 8 and 9, the values were different for each key as tabulated on Table 1.

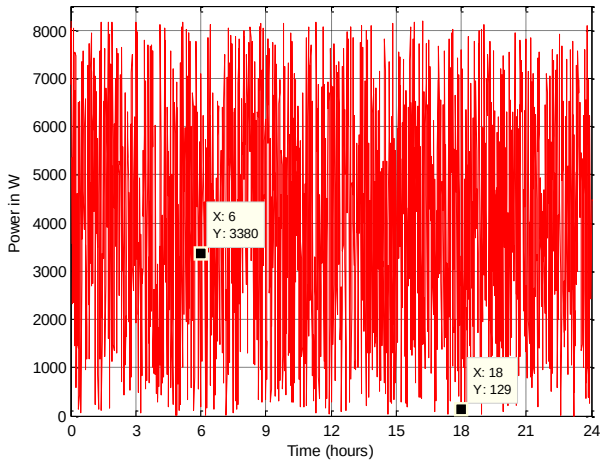

Fig. 8. Encryption using a Key2

Fig. 8 and 9 shows the result after encryption using Key2 and Key3 respectively. The goal of hiding the information on user data is thus met using different keys.

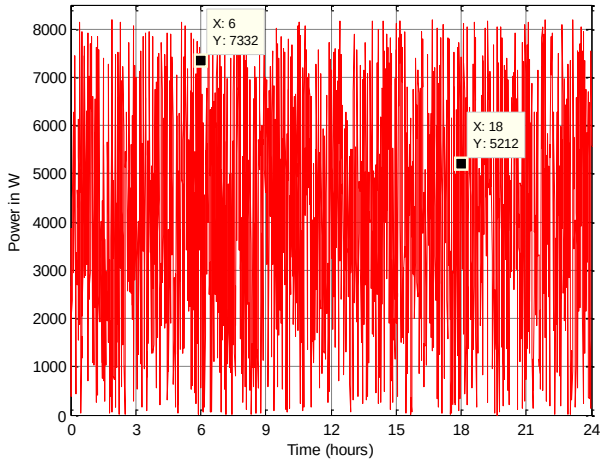

Fig. 9. Encryption using a Key3

If the wrong key is used, the results will be unintelligible. To demonstrate this, decryption of fig. 9 was attempted using the Key2. The result was as shown in fig. 10.

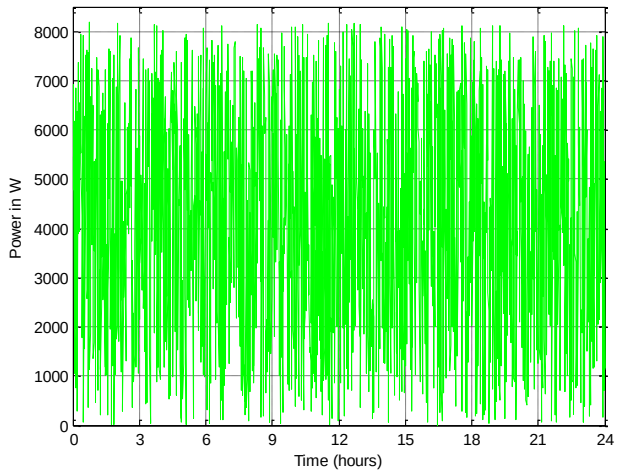

Fig. 10. Decryption using the wrong key.

A key concern in Smart Grid communication is the time taken to complete encryption. Delays in some applications can be costly. Most devices also have low capacity.

The encryption operations in this paper were done on Matlab 7.10. A laptop with 2.6 GHz processor and 4.0GB RAM. The time taken was 0.761 seconds (taking an average of 5 runs). Using Matlab's Profiler, a tool used to determine how much time is spent executing sections of code, over 80% of this time was used in plotting and binary and decimal conversions. In an embedded system, these two operations would be unnecessary. Thus, about 0.15 seconds (20% of total run time) went into encryption of all the data. The data being used is based on a 24 hour period, taking samples each minute – a total of 1440 samples. Thus each sample would take 0.104 milliseconds. Such a delay would be negligible in a metering operation and would not affect system operation.

Table 1. Sample values distinguishing the different keys

Key	Value at x = 6 (i.e. 6am)	Value at x = 18 (i.e. 6pm)
Key1	953	5155
Key2	3380	129
Key3	7332	5212

7. Conclusions

The importance of privacy cannot be ignored in the deployment of Smart Grid. Too much would be at stake considering the modern age's dependence on electricity. In a time when cyber crimes are on the rise, ignoring these threats would hinder Smart Grid

adoption. Improving privacy would go a long way in building customer confidence in Smart Grid.

The use of RC4 encryption was found to be an effective way of providing privacy involving electrical power usage. Due to the simplicity of the algorithm, the time required to perform encryption would not affect system performance.

Further work would involve implementing this algorithm on a microchip that can be installed in a smart meter. The chip would have fewer overheads than simulation, but also slower processing. An examination of its performance would provide the final verdict on its effectiveness for smart meters.

Appendix

The RC4, key generation algorithm is as follows [9]:

A variable length key is used to initialize a state vector S, which contains a permutation of the numbers between 0 and 255 in its elements S[0], S[1],…S[255]. Encryption/decryption is done by systematically picking a byte from S and finding its XOR with a plaintext/ciphertext byte. The pseudocode below describes the procedure.

S is first initialized with values from 0 to 255. The key is expanded into a temporary vector T which is the same length as S (i.e. 256 bytes).

```
/* Initialization */
for i = 0 to 255 do
    S[i] = i;
    T[i] = K[i mod keylen];
```

T is then used to form an initial permutation of S by going through all elements of S swapping each using a scheme dictated by T[i]:

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
   j = (j + S[i] + T[i]) mod 256;
   Swap (S[i], S[j]);
```

S is then permuted repeatedly while a byte k is chosen from it systematically:

```
/* Stream Generation */
i, j = 0;
while (true)
   i = (i + 1) mod 256;
   j = (j + S[i]) mod 256;
   Swap (S[i], S[j]);
   t = (S[i] + S[j]) mod 256;
   k = S[t];
```

This key, k, is then used to generate the ciphertext, c, by using bitwise XOR with the plaintext, p, i.e. c = k XOR p.

Acknowledgement

The authors would like to acknowledge Jomo Kenyatta University of Agriculture and Technology for facilitating the study.

References

[1] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for smart grid cyber security," National Institute of Science and Technology, 2010.

[2] Z. Fan et al., "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities," *Communications Surveys & Tutorials, IEEE*, vol. PP, no. 99, pp. 1-18, 2011.

[3] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," *Communications Surveys & Tutorials, IEEE*, vol. PP, no. no.99, pp. pp.1-37, Sept 2011.

[4] Alfredo Rial and George Danezis, "Privacy-Preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, Chicago, USA, 2011, pp. 49-60.

[5] George W. Hart, "Nonintrusive Appliance Load Monitoring," in *PROCEEDINGS OF THE IEEE*, 1992, pp. 1871– 72.

[6] Elias Leake Quinn, "Privacy and the New Energy Infrastructure," *Social Science Research Network (SSRN)*, Feb 2009.

[7] Wenye Wang and Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, April 2013.

[8] Christof Paar and Jan Pelzl, *Understanding Cryptography*.: Springer, 2010.

[9] William Stallings, *Cryptography and Network Security: Principles and Practive*, 5th ed. USA: Prentice Hall, 2011.

[10] G. Strbac, "Demand side management: Benefits and challenges. , 36(12)," *Energy Policy*, vol. 36, no. 12, pp. 4419-4426, 2008.