International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 10 Issue 8 August - 2026, Pages: 1-7

Encryption Techniques in Protecting Renewable Energy Systems

Dalael Saad Abdul-Zahra

Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babylon, Iraq
dalael20175@gmail.com

Abstract. *Renewable energy systems, from solar and wind power plants to smart distributed energy grids, are an integral part of biological neurons. However, these complex, internet-connected robots make them vulnerable to cyber-attacks. Therefore, a robust cybersecurity application is essential to control these eyes and protect the electrical grid. The world is witnessing major transformations in the field of energy, as attention is being drawn to energy sources as an alternative to traditional energy. This source is characterized by being environmentally friendly and renewable, and contributes to reducing dependence on fossil fuels. Renewable energy contributes to reducing greenhouse gas emissions that contribute to climate change. Reliance on a single source of energy reduces the risk of power outages, and renewable energy is also a long-term investment that ensures a sustainable future. In this work the aim is to link two different concepts: renewable energy (represented by solar cells) and cybernetic interpretation (represented by the RSA algorithm). This link can be useful in understanding how different technologies can integrate to serve a common purpose. In this paper, the intersection between renewable energy, especially solar cells, and cybernetic interpretation will be studied through the RSA algorithm. By examining how these two distinct concepts are linked, we aim to highlight the potential for technological integration that serves a common purpose. This exploration not only highlights the functionality of solar energy systems, but also underscores the importance of secure communications in the digital age, and demonstrates how these technologies can complement each other.*

Keywords. RSA Algorithm; Renewable Energy; Encryption; Decryption.

1. Introduction.

Technologies for information and communication (ICTs) have had a significant impact on the world. With the pinnacle of digitization nearing, over half of the world's population is currently online. Regardless of the format—image, text, sensor data, control program, program output, etc.—all information is transformed into binary data and saved for later processing and retrieval. Around the world, data centers offer the space needed to do all of these tasks. Currently, 13% of the world's primary energy supply comes from renewable sources [2], however the growth of this percentage varies significantly among nations, particularly within the European Union. While renewable energy only made up a small percentage of total energy in other nations like the USA and the Netherlands in 2009, it contributed 47% and 30% of total final energy in Sweden and Finland, respectively [3]. Geographical factors, power system designs, and political colors all contribute to these disparities. Energy security has been defined from a number of perspectives by numerous researchers. The term "energy security," which encompasses ideas like supply security, infrastructural dependability, affordability, and environmental friendliness [25], is contentious and complicated [24]. Depending on a country's geographic location, natural resource endowment, economic nature [26], status as a producer/exporter, consumer importer, or transitor [27], vulnerability to disruptions in the energy supply, political system, ideological beliefs and perceptions [28], and international relations status, energy security can mean different things to different countries. For instance, reliance on Russian gas is dependent on historical experiences during the Cold War [29], as cited in [27]. One of the public key cryptosystems was developed by Rivest, Shamir, and Adleman and was first proposed in 1978. Since then, the most widely used and recognized general-purpose encryption method has been the RSA approach. The plaintext and ciphertext of the RSA [1] encryption technique is both integers. In 2015, Gafitoiu proposed a polynomial RSA by using polynomials instead of integers by taking $\mathcal{Z}_{\mathbb{p}}[\mathcal{X}] = \{z_0 + z_1 x + z_2 x^2 + \cdots + z_k x^k | k \geq 0 , z_i \in \mathcal{Z}_{\mathbb{p}}\}$ both compute modulo a prime number p and a polynomial as a ring with two operations [2]. Hamza suggested a public key in 2022 called PQ-RSA, which uses quaternion polynomial algebra in place of polynomial RSA and has the same parameter [3]. In 2024, Abbas and Yassein present TPRSA, a modified RSA substitute that has a new mathematical structure and is based on Tri-Cartesian algebra and polynomials [4, 5]. In order to achieve great security, Abo-Alsood et al. also offer a new public key, HH-RSA, using the five-dimensions HH-Real algebra [6, 7]. By combining polynomial RSA and NTRU using a hexadecnion polynomial rather than polynomial RSA, Abbas and Yassein present a novel public key hexadecnion polynomial RSA(PH-RSA) [8, 9]. In this paper we explain who keep this networks from vandalism or malfunction by creating a secure encryption system that protects renewable energy centers from exposure to these attacks and maintaining their internal programming by retrieving the public and private key between the devices inside those centers and the designers of those devices, especially in places that operate on solar energy such as solar cells in energy centers and protecting them, which leads to a large percentage of energy storage that is safe and effective and can be used and reused using some important encryption algorithms such as RSA algorithm.

2. Methodology

A) Renewable Energy Networks. The method of this research is to study the importance of security in renewable energy networks. The security of renewable energy networks is critical for several reasons:

- Protection of Sensitive Data**:** Renewable energy systems generate and transmit vast amounts of data, including operational metrics and user information. Protecting this data from unauthorized access is crucial.
- Operational Integrity**:** Cyberattacks can disrupt the operation of energy networks, leading to power outages and financial losses. Ensuring the integrity of these systems is vital for maintaining service continuity.
- Public Trust**:** As more consumers adopt renewable energy solutions, maintaining public trust in these systems is essential. Security breaches can undermine confidence in renewable energy technologies.

B) Encryption Algorithms in Renewable Energy Networks. Encryption algorithms play a key role in securing data transmitted across renewable energy networks. Here are some commonly used encryption techniques in figure 1:

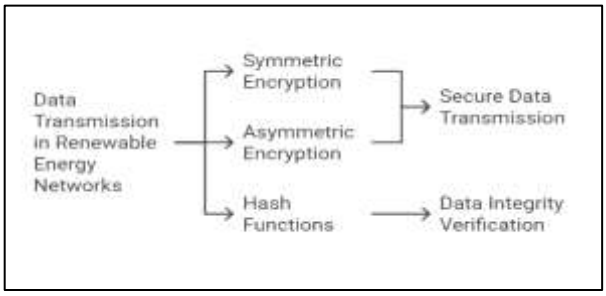

Figure 1. Method of encryption Algorithms in Renewable Energy Networks.

We can summarize the method of work in Figure 2.

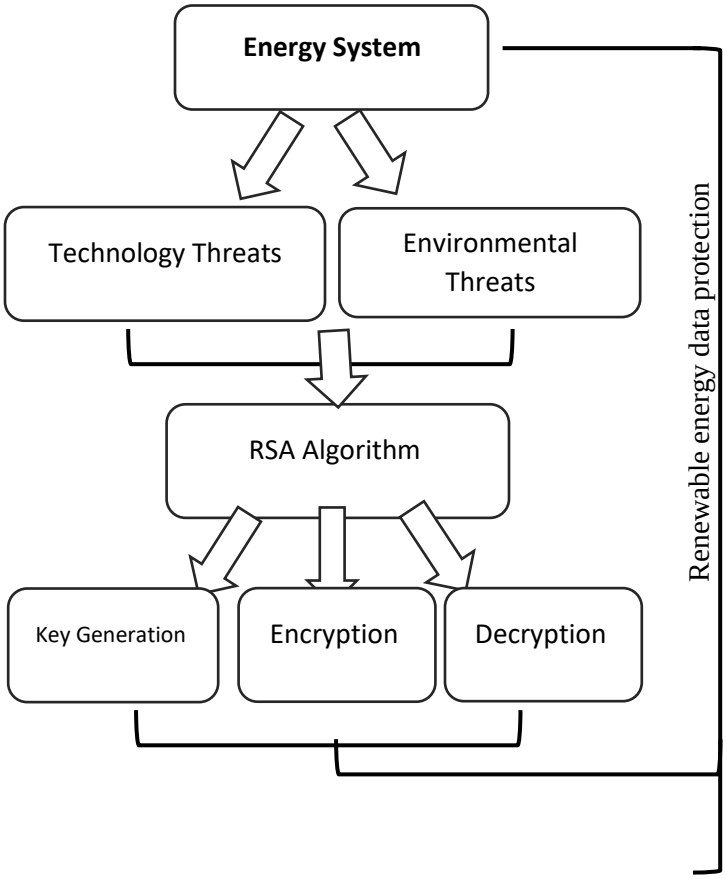

Figure 2. summarize the method SREN

3. Cryptography Overview:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. It is concerned with developing and analyzing protocols that prevent third parties or the public from reading private messages, as well as various services such as digital signatures, which provide data integrity and authentication. Modern cryptography is heavily based on mathematical theory and computer science. Cryptography is Important:

- Privacy: Protects sensitive information from unauthorized access.
- Data Integrity: Ensures data has not been altered.
- Authentication: Verifies the identity of the sender and receiver.
- Non-repudiation: Prevents senders from denying they sent a message.

3.1. Types of Cryptography:

- Symmetric-key cryptography: Uses a single key for both encryption and decryption.
- Public-key cryptography: Uses a pair of keys: a public key for encryption and a private key for decryption. In fig 1:
- Hash functions: Creates a fixed -size string of characters (hash) from any data input.

3.2. The RSA Algorithm:

The RSA algorithm is a widely used public-key cryptographic system that enables secure data transmission. It relies on the mathematical properties of prime numbers and modular arithmetic. The security of RSA is based on the difficulty of factoring large composite numbers, making it a robust choice for protecting sensitive information. As digital communication continues to grow, the importance of secure algorithms like RSA cannot be overstated.

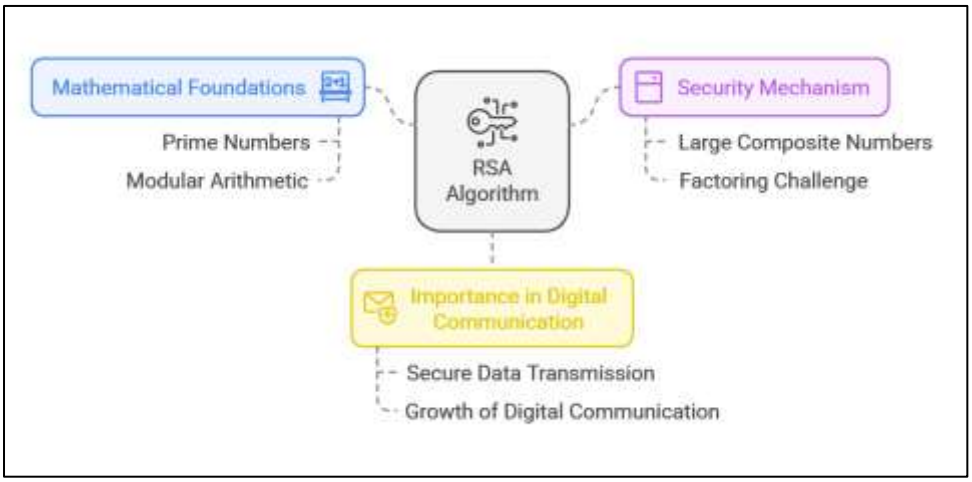

Figure 3. RSA algorithm.

- Prime Generation**:** The code generates large prime numbers using random bit generation and checks for primality.
- Key Generation**:** It computes the public and private keys based on the generated primes.
- Encryption**:** The plaintext message is converted to an integer and encrypted using the public key.
- Decryption**:** The ciphertext is decrypted back to plaintext using the private key use:

3.2.1. RSA Algorithm Implementation

```
1. import random
2. from sympy import isprime, mod_inverse
3. def generate_prime_candidate(length): """Generate an odd integer randomly."""
4.     p = random.getrandbits(length)
   return p | (1 << length - 1) | 1
    # Ensure it's odd and has the correct length
5. def generate_prime_number(length): """Generate a prime number of specified bit length."""
```

```
    p = 4
    while not isprime(p):
        p = generate_prime_candidate(length)
    return p
def gcd(a, b):
    """Compute the greatest common divisor using Euclidean algorithm."""
    while b!= 0:
        a, b = b, a % b
    return a
def generate_keypair(bits):"""Generate a public and private key pair."""
    p = generate_prime_number(bits)
    q = generate_prime_number(bits)
    n = p * q*r
    phi = (p - 1) * (q - 1)
    e = 65537  # Common choice for e
    while gcd(e, phi) != 1:
        e = random.randrange(2, phi)
    d = mod_inverse(e, phi)
    return ((e, n), (d, n))  # Public and private key
def encrypt(public_key, plaintext):"""Encrypt the plaintext using the public key."""
    e, n = public_key
    plaintext_bytes = plaintext.encode('utf-8')
    plaintext_int = int.from_bytes(plaintext_bytes, byteorder='big')
    ciphertext_int = pow(plaintext_int, e, n)
    return ciphertext_int
def decrypt(private_key, ciphertext):
    """Decrypt the ciphertext using the private key."""
    d, n = private_key
    plaintext_int = pow(ciphertext, d, n)
    plaintext_bytes = plaintext_int.to_bytes((plaintext_int.bit_length() + 7) // 8, byteorder='big')
    return plaintext_bytes.decode('utf-8')
if name == "main":
bits = 16  # For demonstration, use a small key size
public_key, private_key = generate_keypair(bits)
message = "Hello, RSA!"
print(f"Original Message: {message}")
encrypted_msg = encrypt(public_key, message)
print(f"Encrypted Message: {encrypted_msg}")
decrypted_msg = decrypt(private_key, encrypted_msg)
print(f"Decrypted Message: {decrypted_msg}")
```

3.2.2. *Advanced Encryption Standard (AES)*

AES is one of the most widely used symmetric encryption algorithms. It operates on fixed block sizes and supports key sizes of 128, 192, and 256 bits. Its efficiency and security make it suitable for protecting data in renewable energy networks.

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
import os
def encrypt_aes(key, data):
cipher = AES.new(key, AES.MODE_CBC)
ct_bytes = cipher.encrypt(pad(data.encode(), AES.block_size))
return cipher.iv, ct_bytes
def decrypt_aes(key, iv, ct):
cipher = AES.new(key, AES.MODE_CBC, iv)
pt = unpad(cipher.decrypt(ct), AES.block_size)
```

```
11. return pt.decode()
```

3.2.3. Data Encryption Standard (DES)

Although DES is considered less secure than AES, it can still be used in scenarios where performance is prioritized over security. It operates on 64-bit blocks and uses a 56-bit key.

```
1. from Crypto.Cipher import DES
2. from Crypto.Util.Padding import pad, unpad
3. def encrypt_des(key, data):
4. cipher = DES.new(key, DES.MODE_CBC)
5. ct_bytes = cipher.encrypt(pad(data.encode(), DES.block_size))
6. return cipher.iv, ct_bytes
7. def decrypt_des(key, iv, ct):
8. cipher = DES.new(key, DES.MODE_CBC, iv)
9. pt = unpad(cipher.decrypt(ct), DES.block_size)
10. return pt.decode()
```

4. Results and Discussion

In the rapidly evolving field of renewable energy, ensuring the security of data transmitted across networks is paramount. This document explores various code encryption algorithms that can be effectively utilized within renewable energy networks. By employing these algorithms, we can safeguard sensitive information, enhance communication integrity, and protect against potential cyber threats. The following table summarizes key encryption algorithms, their characteristics, and their applicability in renewable energy systems in Table 1.

Algorithm	Type	Length	Strength	Reenable Energy
RSA	Asymmetric	1024, 2048, 4096 bits	High	Secure key exchange for IoT devices in renewable systems
AES	Symmetric	128, 192, 256 bits	Very high	Data encryption for smart grid communications
DES	Symmetric	56 bits	Low	legacy systems in older renewable energy infrastructures

We can summarize the method of work in Figure 4.

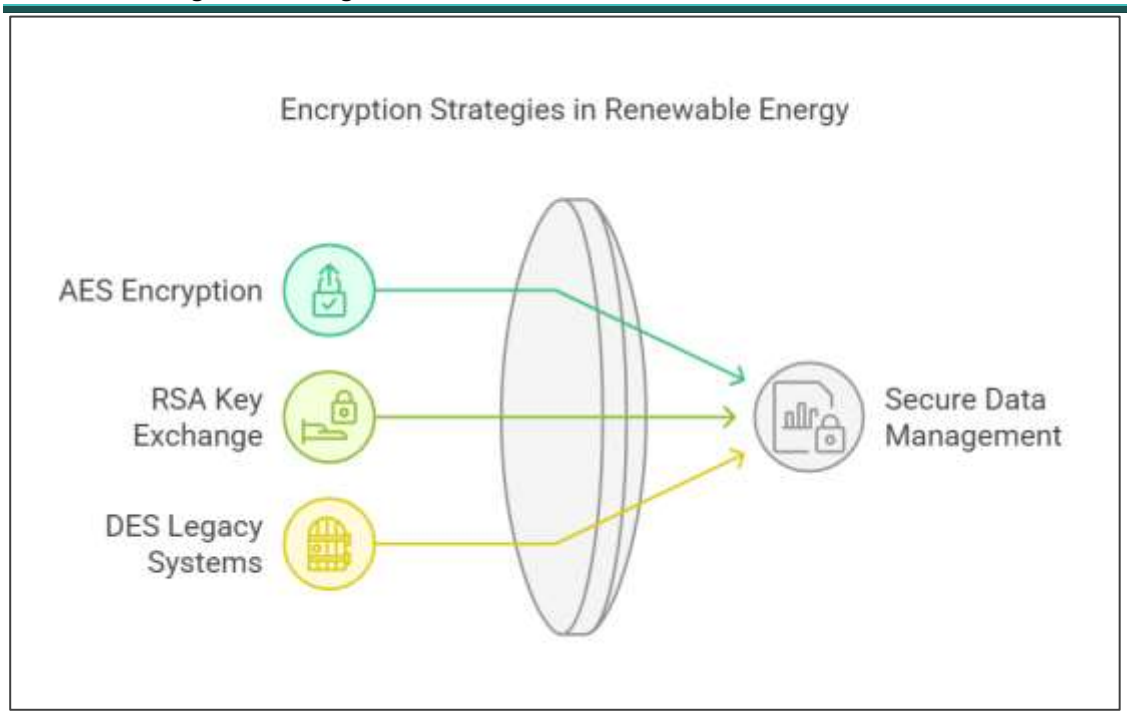

Figure 4. (SREN) Encryption Algorithm.

5. Conclusion

The intersection of renewable energy, represented by solar cells, and cybernetic interpretation, exemplified by the RSA algorithm, presents a promising avenue for technological integration. By understanding how these two concepts can work together, we can foster innovations that not only enhance energy efficiency but also ensure the security of data in our increasingly digital world. This synergy highlights the importance of interdisciplinary approaches in addressing contemporary challenges and advancing sustainable solutions.

Reference

1. IEA. World energy outlook 2012. Paris: IEA/OECD; 2012.
2. European Commission. EU, energy in figures, statistical pocketbook 2012. Brussels: Publications Office of the European Union; 2012.
3. Valentine SV. The fuzzy nature of energy security. Sovacool BK. The Routledge Handbook of Energy Security. New York: Routledge; 2011. p. 56–73. ISBN 13: 9780415591171
4. García-Gusano D, Iribarren D, Garraín D. Prospective analysis of energy security: A practical life-cycle approach focused on renewable power generation and oriented towards policymakers. Applied Energy. 2017;190: 891-901. DOI: 10.1016/j.apenergy.2017. 01.011
5. Luft G, Korin A. Energy security: In the eyes of the beholder. In: Luft G, Korin A, editors. Energy Security Challenges for the 21st Century: A Reference Handbook. Santa Barbara, California, USA: Praeger Security International; 2009. pp. 1-17. ISBN: 978-0-275-99998-8
6. Johansson B. A broadened typology on energy and security. Energy. 2013;53: 199-205. DOI: 10.1016/j.energy.2013.
7. Marquina A. The southeast– southwest European energy corridor. In: Marguina A, editor. Energy Security: Visions from Asia and Europe. UK: Palgrave Macmillan; 2008. pp. 54-68. ISBN: 978-0230595002
8. Leonard M, Popescu N. A Power Audit of the EU-Russia Relations. Policy Paper. London: European Council on Foreign Relations; 2007. Available from: https://www.ecfr.eu/page/-/ECFR-02_ A_POWER_AUDIT_OF_EU-RUSSIA_ RELATIONS.pdf [Accessed: 12 March 2020]
9. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signature and public key cryptosystems”, Communications of the ACM, vol. 21, no.2, pp.120-126, 1978.

I. B. Gafitoiu "Polynomial based RSA", Linnaeus University, B. Sc Thesis, 2015, pp. 7-19.

10. M. H. Hamza, "Designing an Efficient and Secure Cryptosystems Similar to MaTRU and RSA", M. Sc. Thesis, University of Al-Qadisiyah, Iraq, 2022.
11. H. R. Yassein and N. M. G. Al-Saidi, "BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly Multidimensional Algebra", Proc. the 6th International Cryptology and Information Security Conference, Negeri Sembilan, Malaysia, pp. 1–11, 2018.
12. B. N. Abbas and H. R. Yassein, "Design of an Alternative to Polynomial Modified RSA Algorithm", International Journal of Mathematics and Computer Science, vol. 19. No. 3, pp. 693-696, 2024.
13. H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed and W. I. El-Sobky, "QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra", Appl. Math. Inf. Sci. vol.17, No. 1, pp.49-53 (2023).
14. Hadeel Hadi Abo-Alsood, Mohammed Hassan Hamza, Sukaina Abdullah Al-Bairmani, Hassan Rashed Yassein, "International Journal of Mathematics and Computer Science, vol. 19, no. 4, pp. 177–1182, 2024.
15. H. R. Yassein and N. M. G. Al-Saidi, "HXDTRU Cryptosystem Based on Hexadecnion Algebra", Proc. 6th International Cryptology and Information Security Conference, Sabah, Malaysia, pp. 1–10, 2016.
16. B. N. Abbas and H. R. Yassein, " A High-Security Encryption Based on Hexadecnion Polynomials", International Journal of Mathematics and Computer Science, vol. 19. No. 1, pp. 37-40, 2024.