Journal of Applied Artificial Intelligence
https://jaai.sabapub.com
ISSN: 2709-5908

2024 Volume 5, Issue 2: 71-83
DOI: https://doi.org/10.48185/jaai.v5i2.1053

Secret key generation based Short Tandem Repeat DNA

Sadoon Hussein[1, *], Ahmed Sami Nori[2]

[1] Physic Department, College of Science, University of Mosul University, Iraq.
[2] Cyber Security Department, College of Computer Science and Mathematics, University of Mosul University, Iraq.

Received: 11.07.2024 • Accepted: 10.09.2024 • Published: 12.09.2024 • Final Version: 27.09.2024

Abstract: In a daily basis, scientists seek to develop more advanced security solutions to be applied into IoT environment using in-hand technologies. Indeed, many approaches have been proposed to respond to this scarcity, and many other exertions have been spent. One promising consequence is DNA computing, which has significantly promising capabilities over traditional electronic computers. As biological characteristics have always been a source of inspiration for scientists in developing complex computing systems and technologies. DNA is a molecule in organism`s cells. All organisms' DNA are similar in about 99.9%. In this paper, a new data encryption technique has been inspired by DNA characteristics in which the encryption key transmission is based on STR DNA fingerprint. The proposed technique will be applied in a healthcare environment. The STR-DNA based key generation and transmission technique will be used to encrypt the message before being transmitted over the IoT environment. The experimental results showed that the proposed technique has similar characteristics as the RSA algorithm added the feature of applying the mechanism on biological environments.

Keywords: DNA. RSA. STR, Encryption, Key Transmission.

1. Introduction

In the routine of our everyday lives, with an increased use of smart devices connected, protecting the transmitted critical data against potential attacks is necessary [1,2]. In this paper, a comprehensive system has been designed with a sophisticated security to transmit secret keys between the IoT Devices with lightweight capability to be able to applicable on an IoT devices. In addition to its capabilities to development and upgrade. The research objectives can be summed up in four main points:

-Create an authentication technique inherited from biological environment to be applied to IoT environment. Also, to encrypt biological data in a way that makes it secure, as any approach will offer encrypting biological data by first encoding it will make it vulnerable to attacks in the encoding phase. So, the researchers aim to encrypt biological data without the need of adding any extra layer of encoding to ensure security. It is essential to demonstrate that it is possible to construct such a complicated system on the basis of DNA, which is the primary goal of adapting existing encryption algorithms. The purpose of this modification is to make it a candidate that is

* Corresponding Author: Sadoon Hussei, email: sadosbio113@uomosul.edu.iq

suited for application in biological environments in order to accommodate the genes-based computers that have recently evolved. As the future of computing, we are working toward the goal of subrogating traditional calculations into biologically based systems in order to take advantage of the features that were discussed earlier.

- To produce an encryption technique based on DNA computing in which the encryption technique is inherited from DNA and biological processes to be applicable on biosensors

2. Background

Just as scientists have always drawn inspiration from biological features to create intricate computer systems and technology. The suggested method was motivated by features found in DNA. The DNA of all species is similar in 99.9% of cases. Every living thing has distinct surviving components [3]. Thus, each and every living thing has a distinct DNA feature. One individual can be distinguished from another using these characteristics. Since children receive half of their DNA from each parent, it can also be used to determine a person's relationship to another person. Less than 1 to 19 billion duplication chances exist in a DNA characteristic, according to statistical evidence supporting DNA fingerprint duplication probability statistics. which suggests that the DNA properties are highly reliable. DNA profiling is based on a distinct feature known as STR found in the DNA sequence [4]. The amount of repeats that are present in a particular area of the DNA sequence, which is referred to as a STR, differs from individual to individual. in a structure of the DNA. Short Tandem Repeat is an abbreviation that pertains to a certain kind of repeated DNA sequence that can be found in the genome. often, these sequences are made up of small motifs that are repeated numerous times in a row. These motifs often consist of two to six base pairs. Because STRs are highly polymorphic, which means that the amount of repeats can differ from person to person, they are valuable for a wide variety of applications[5,6].

2.1. DNA

Within an organism's body is a molecule called DNA that contains the genetic instructions necessary for growth and function. It functions as a genetic information storage medium. Every living cell uses DNA as its fundamental store medium, and its main job is to receive and deliver biological instructions [7]. The branch of computing known as DNA computing is a relatively new one that utilizes molecular biology, biochemistry, and DNA as an alternative to the conventional silicon-based computer technology commonly used. The theory, experiments, and applications of DNA computing in a DNA characteristic are the primary focuses of the research and development that is being conducted in this topic[8]. DNA serves as the fundamental storing medium for all living cells. Its primary job is to take in and send life's info back across billions of years. A marble-sized characteristic may contain about 10 trillion DNA molecules. [9,10].

2.2 DNA Fingerprint

DNA fingerprinting, sometimes referred to as DNA profiling, is a method for identifying people according to their distinct genetic composition. The idea behind DNA profiling is to use an individual's DNA traits to identify them. The DNA of all species shares 99.9% of the same characteristics [11].Every living thing has distinct surviving components. Accordingly, each living thing has a distinct DNA characteristic, as seen in figure 1. The trait that sets each person distinctly is known as short tandem repeats (STR). STRs is a repetition on number of nucleotides (typically from 3 to 7 base pairs) in the chromosome. The number of repetitions varies from person to person (up to thirty repetitions), and this is the factor that distinguishes one individual from another based on their performance. Twenty distinct loci are utilized as genetic markers in the process of DNA profiling. Additionally, one locus, known as the amylogenic locus, is utilized to verify the gender

of the individual who provides the DNA sample. A locus is the precise physical place on a chromosome where a gene or other DNA sequence is located. It can be thought of as a genetic equivalent of a street address. In modern times, scientists only employ thirteen loci [12,13].

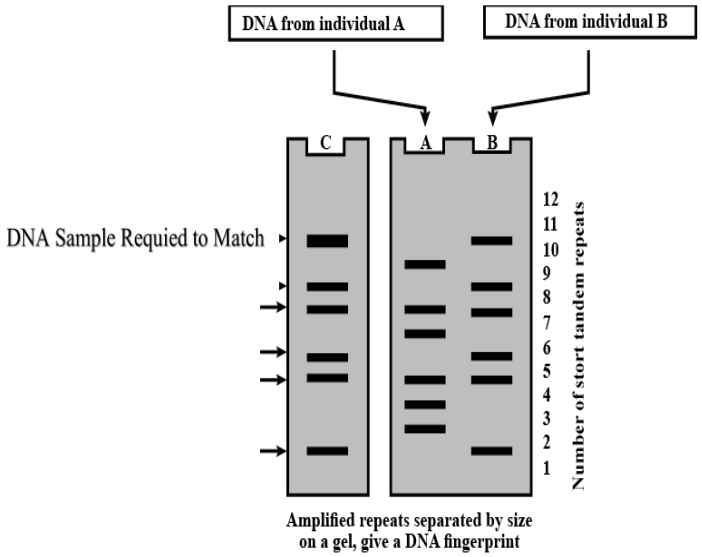

Figure 1: DNA Fingerprinting [14]

The implementation of the DNA profiling process is to collect a sample then extract the DNA portion of the sample. Then, use amplification technique to amplify specific regions of the DNA using PCR technique [15]. These regions are called STR, which are a repetitive sequence in the DNA with a unique characteristic that differs from one person to another as shown in figure 2.

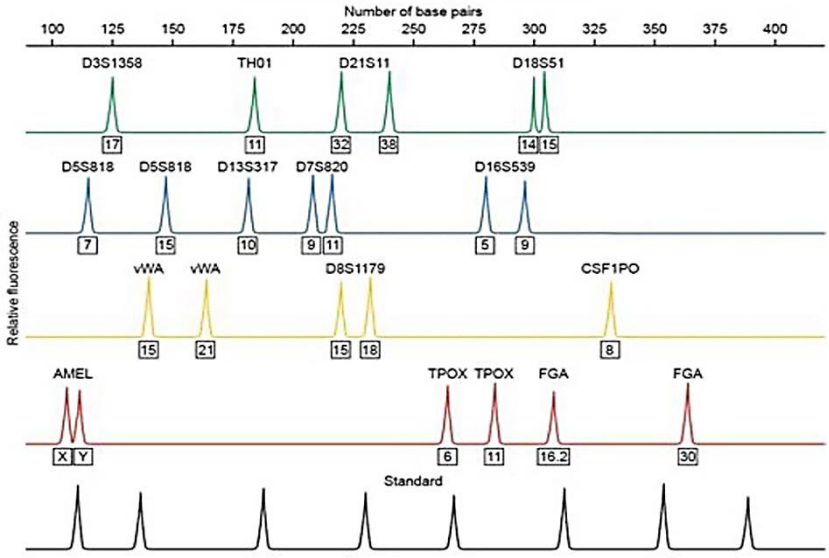

Figure 2: DNA STR Matching process [16]

2.3 AVISPA Tool

The process of automating the validation of internet security protocols and applications is typically referred to by this word. The Automated Validation of Internet Security Protocols and Applications (AVISPA) is a tool that may be launched by pushing. This ensures that the validation process is carried out quickly and accurately. A formal language that is both modular and expressive is provided, which enables the specification of protocols as well as the security characteristics that are associated with those protocols. In addition to integrating a number of back-ends that implement a wide range of cutting-edge automatic analysis techniques, it also provides a formal language that is modular. Based on the findings of experiments conducted on a

comprehensive collection of Internet security protocols, it can be concluded that the AVISPA tool represents the most advanced form of automatic security protocols now available. The same level of performance and scalability, along with the same level of scope and resilience, are not found in any other tool. The tool used to ensure the robustness of the authentication protocol using several attacks [17]. The GUI of the AVISPA tool simulation is represented in Figure 3

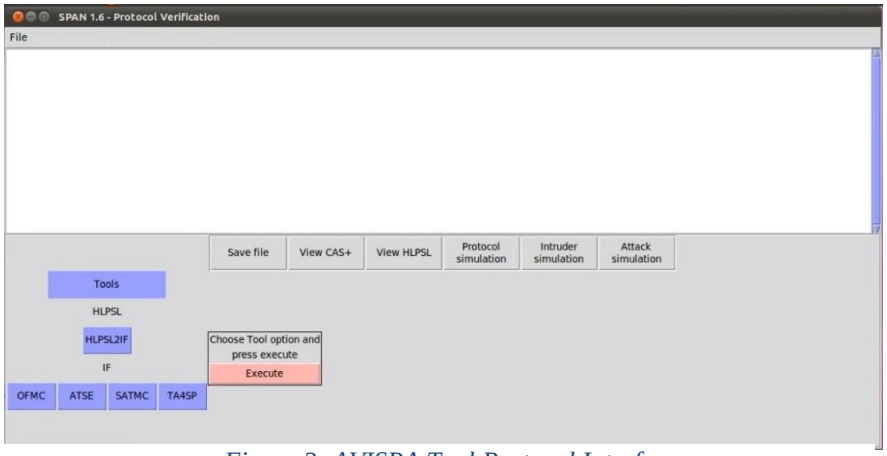

Figure 3: AVISPA Tool Protocol Interface

As shown AVISPA Architecture in figure 3. The CAS+ definition of the protocol is sent to SPAN as input when it is written in the Alice Bob notation. After that, SPAN will transform it into a script that uses the HLPSL specification. Those responsible for the specification are Saillard and his coworkers. It is then converted to IF by the translator that transforms HLPSL to IF and analyzes it by employing the backends built by AVISPA. The HLPSL script is sent to the IF translator as an input, and the IF translator then converts it to IF.

3. Literature Review

Key generation is the process of generating keys used in the encryption process. DNA cryptography is utilized for expanding the effectiveness and security of encryption methodologies. DNA is utilized as the data transporter, and it utilizes modern biological technology to procure encryption. In recent years, many image encryption algorithms utilize chaos and DNA cryptography. Table 1 summarizes the literature review.

Table 1:Literature Review

No.	Study	Year	Methodology	Results
1	Kumar and Sharma [18]	2023	A proposed technique for generating ECC-keys via a genetic algorithm consists of multiple stages: chromosome initialization, fitness evaluation, selection, uniform crossover, and mutation.	Further investigation in novel key-generation techniques for contemporary cryptographic applications is facilitated by the proposed ECC-GA strategy.
2	Xue Wei and Dola Saha [19]	2022	Propose a new key Generation using Neural Networks from Wireless Channels, which extracts the implicit features of channel in a compressed form to derive keys with high agreement rate.	Results demonstrate that the latent vectors of the legitimate parties are highly correlated yielding high KGR (≈ 64 bits per measurement) and low KDR (<0.05 in most cases)
3	Shargabi and Al-Husainy [20]	2021	Proposed a new lightweight key transmission and encryption algorithm based on the DNA sequence to be adequate for IoT device's resources	the experimental results show outstanding results regarding key size, encryption time

4	Patel and Doshi [21]	2021	A reliable and efficient lightweight key exchange system with a safe RUA was proposed by the Authors for the user-gateway model. In order to develop a lightweight RUA method, the work employed elliptic curve cryptography (ECC).	The research used publisher-subscriber-based lightweight Message Queuing Telemetry Transport (MQTT) protocol to propose a highly secure and efficient RUA scheme for the sensor-based environment with the formal security analysis and real-time implementation.
5	Gao et al. [22]	2020	Proposed a lightweight and efficient physical layer key generation scheme, which extract shared secret keys from channel state information (CSI)	Several experiments in various real environments are conducted. The experimental results show that the proposed scheme can efficiently generate shared secret keys for nodes and protect their communication
6	Reddy et al. [23]	2020	Proposed hybrid key generation approach consists of adequate encoding based on DNA	The proposed approach is evaluated against conventional cryptographic methods, resulting in a reduction of processing time by 55% and 67% respectively.
7	Jacovic et al. [24]	2019	A novel approach is proposed for creating secret keys at the Physical layer to enhance IoT security, using a low-complexity mechanism. We provide an effective method by utilizing the carrier frequency offset (CFO) and channel estimate components of Orthogonal Frequency Division Multiplexing (OFDM) receivers.	Enhances the capacity of targeted nodes to generate corresponding secret keys, effectively impeding the risk posed by an eavesdropper, and proves valuable in safeguarding forthcoming IoT devices.
8	Yuliana et al[25]	2019	Recommendation of a signal strength exchange (SSE) system as a very effective mechanism for generating keys, together with a synchronized quantization (SQ) technique within the SSE system to synchronize data blocks throughout the quantization phase.	The test results obtained from IoT devices equipped with IEEE 802.11 radio demonstrate that the SSE system exhibits superior efficiency in terms of both processing time and communication overhead compared to current systems.
9	B. R.Pushpa [26]	2017	Hiding encryption key in a DNA sequence form to make it more secure after applying a complementary rule, then assigning it an index according to a fixed table.	The modified technique is strengthened by hiding the key in a DNA sequence form.
10	Wattar et al. [27]	2015	Generating key-dependent shift rows transformation by using reverse complement process inspired from DNA process.	The proposed enhanced approach is inspired by DNA process and applied on the classical AES.

A literature review of the state-of-the-art research work of key generation has been summarized as shown in the recent table. Based on the conducted review, it is obvious of the lack of IoT, Lightweight and healthcare based key generation algorithms, which stimulates the authors to concentrate on these environments due to its` special requirements. Moreover, it would appear that there is no appropriate approach that has been created to address the security requirements of the Internet of Things in order to deal with the various assaults. The conclusion that can be drawn from this is that the Internet of Things (IoT) still needs an adequate model in order to mitigate the technical gap in terms of security modeling, data gathering, and robust countermeasure methods.

So, the upcoming proposal gives countermeasure methodologies for the secured IoT for healthcare data transmission.

4. Proposed STR fingerprint Key algorithm

In this paper, a new encryption key transmission technique has been proposed in which the encryption key is inspired from DNA characteristics revealing a promising future of bio-inspired cryptographic techniques. The proposed technique will be used to generate the key required to encrypt patient's sensor information in a complete design of a healthcare system.

A comprehensive healthcare system design will be used to illustrate the suggested methodology. First, the medical data will be taken from "nodes," or patient prospects, that are being watched over by biosensors. Using an internal router, the gathered data will be sent over the internet to a Raspberry Pi device with an integrated broker, where it will be processed, and then to a dedicated candidate physician application based on the patient's medical condition. Every piece of information gathered from doctors and patients will be safely kept on a Firebase cloud. Ensuring the privacy of medical data and the security of the healthcare system provide a security problem.

The presented mechanism provides the ability to implement the RSA algorithm to a promising biological environment, such as a molecular computer or biosensors. The experimental analysis shows the same security level as the original RSA Theoretically. In our scenario, the key generation process will be used to encrypt the information transmitted from the physician to the patient. It provides a secure and trustworthy environment between healthcare network candidates using certain operations and each participant.

In this study a new key generation and transmission technique has been proposed in which the encryption key is inspired from DNA characteristics revealing a promising future of bio-inspired cryptographic techniques.

The proposed technique has been inspired by the simulation of DNA fingerprinting in which the individual's DNA can be differentiated from another by the number of STR [28]. The proposed key generation technique supposes that by giving organism`s DNA, the number of STRs will be unique and related only for this organism. If the organism changed, the number of STR will change, and this will be the private key. One DNA sequence comes from the sender, and the other comes from the receiver, who wishes to communicate in a secure manner. The primary goal is to combine the two DNA sequences in order to make a DNA sequence that is completely unique. There will be a backbone for the generation of the private key, which will be the key for encrypting the message. This backbone will consist of the sender's and the receiver's STR. A decryption of the data is not possible without the DNA sequence of the offspring that was originated. If the attacker does not have the person's STR (private key), they will not be able to access the key sequence that is used for encryption. The implementation of the proposed technique is shown in figure 4.

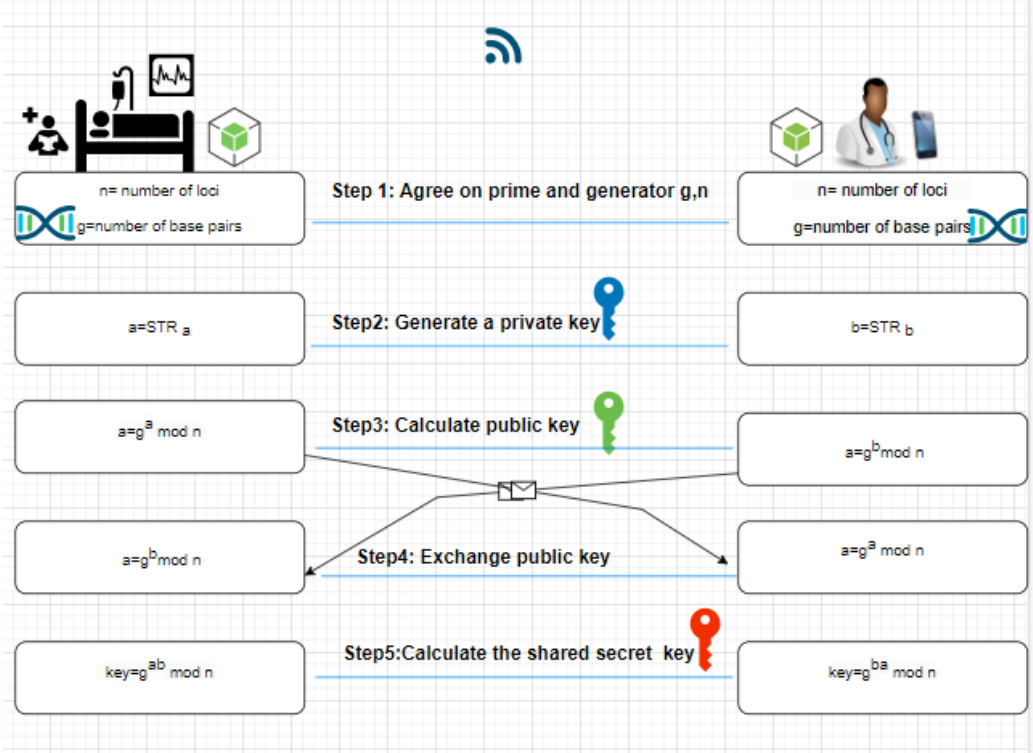

Figure 4: STR key generation block diagram

The proposed key generation technique supposes that giving organism`s DNA, the number of STRs will be unique and related only for this organism. If the organism changed, the number of STR will change, and this will be the private key.

One DNA sequence comes from the sender, and the other comes from the receiver, who wishes to communicate in a secure manner. The primary goal is to combine the two DNA sequences in order to make a DNA sequence that is completely unique. There will be a backbone for the generation of the private key, which will be the key for encrypting the message. This backbone will consist of the sender's and the receiver's STR. A decryption of the data is not possible without the DNA sequence of the offspring that was originated. If the attacker does not have the person's STR (private key), they will not be able to access the key sequence that is used for encryption. Figure 3 illustrates the process by which the encryption key will be formed in the form of a DNA sequence by utilizing STRs that are collected from both the sender and the receiver. The figure depicts a block diagram that illustrates how the encryption key will be constructed in the form of a DNA sequence by utilizing STRs that are collected from the sender (Doctor's) and the recipient. In this equation, the generator (g) represents the number of loci, which are the locations of STRs, and the prime number *"n"* represents the DNA sequence that is repeated. Each party then extracts their STRs and stores it in a variable “a” and “b” respectively. Each party will then use a formula to generate their own public key using the formula in step 3. The next part is to exchange the recently generated public key with each other. The final step is to generate the shared key using the formula in step 5. The public key that is generated by the two parties is a one-way function, which means that it cannot be reversed in order to produce the encryption key without either party having the private key.

5. Implementation

5.1. Formal security verification using AVISPA tool

The Automated Validation of Internet Security Protocols and Applications (AVISPA) mechanism is the name given to this particular piece of technology [29] serves the purpose of formally verifying the security of the cryptographic protocol that is being proposed. A demonstration of the security protocol is offered by AVISPA through the application of the High-Level Protocol Specification Language (HLPSL). This language also enables us to express the security properties of the protocol that are to be validated. In the following graphic, the format security verification that was performed with the AVISPA tool is detailed (figure 5)

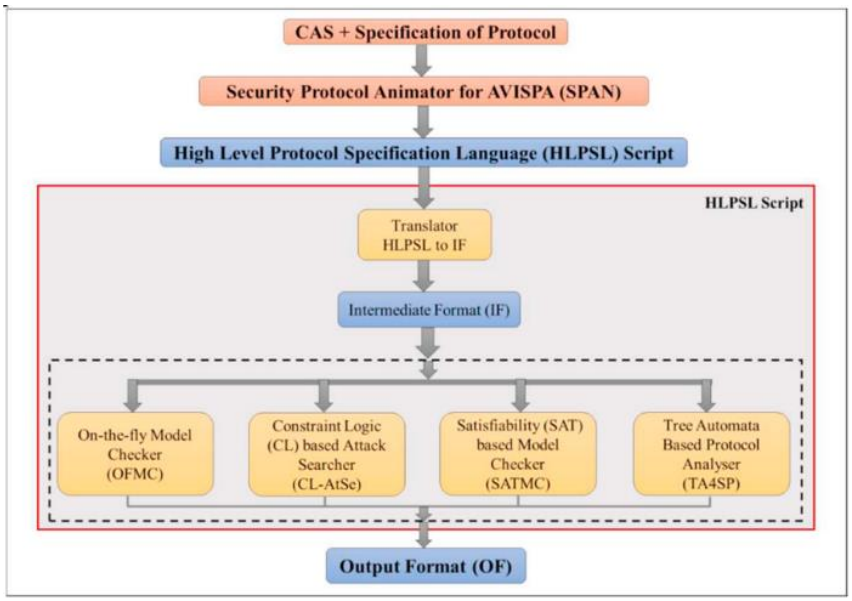

Figure 5: AVISPA security Architecture [29]

As shown in figure 5, the CAS+ specification of the protocol, which is written in Alice Bob notation, is entered into SPAN, which then turns it into an HLPSL specification script from the original format. Following the entry of the HLPSL script into the IF translator, the AVISPA backends are employed in order to perform an analysis on the script and execute the translation from HLPSL to IF. On-the-fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CLAtSe), Satisfiability-based Model-Checker (SATMC), and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP) are the four backends that AVISPA employs in order to determine whether or not the objectives that are outlined in the HLPSL goal section have been accomplished. It is essential to make certain that the objectives that were described in the HLPSL's aim section have been successfully completed. A number of restricted rounds will be carried out by the backend in order to continue executing the protocol until either it is decided that the protocol is safe for the number of sessions or an attack is discovered. The protocol is modeled as states in the HLPSL. Every state contains a variable, and when that variable's value varies, the state transition occurs when certain conditions are met [29].

5.2. Implementing Key Exchange Protocol using AVISPA Tool

The study used AVISPA tool to validate the authentication robustness of the key transmission process.

The STR key generation algorithm implementation is represented in algorithm 1 which represents AVISPA Code and Syntax for the Key generation algorithm.

```
Role sender(Sender, Receiver: agent, SND, RCV: channel(dy))
played_by Sender def= local State: nat, g, n, a, A, Na: text, K: symmetric_key
init State := 0
transition
State = 0 /\ RCV(start) =|> State' := 1 /\ SND(Receiver, {g, n, Na}_K)  // Start the key exchange by sending prime (g), generator (n), and a nonce (Na)
State = 1 /\ RCV(Receiver, {B: text, Nb: text}_K) =|> State' := 2 /\ SND(Receiver, {A, Nb}_K)  // Receive B and Nb, send A and Nb to complete key exchangerole environment() def=sender, receiver: agent,
SND, RCV: channel(dy)
intruder_knowledge = {sender, receiver}
composition
sender(sender, receiver, SND, RCV) /\ receiver(sender, receiver, SND, RCV)
end role
role receiver(Sender, Receiver: agent, SND, RCV: channel(dy)) played_by Receiver def=
local State: nat, g, n, b, B, Nb: text, K: symmetric_key
init State := 0
transition
State = 0 /\ RCV(Sender, {g', n', Na': text}_K) =|> State' := 1 /\ SND(Sender, {B, Na'}_K)  // Receive prime, generator, and nonce, send B and received nonce
State = 1 /\ RCV(Sender, {A: text, Nb': text}_K) =|> State' := 2
end role
role environment() def=
const sender, receiver: agent,
SND, RCV: channel(dy)
intruder_knowledge = {sender, receiver}
composition
sender(sender, receiver, SND, RCV)/\ receiver(sender, receiver, SND, RCV)
end role
goal
secrecy_of K  // Ensure secrecy of the shared secret key
authentication_on SND, RCV  // Ensure authentication during message exchanges
end goal
```

5.3. Results

To evaluate the security of the proposed algorithm, the study used many tools and standards, among them AVISPA tool to evaluate the authentication protocol. The AVISPA tool generates an output that indicates the robustness of the key generation process and its robustness against many types of attacks. The figure 6 shows the output results of the implementation of the AVISPA tool to ensure the robustness of the STR algorithm.

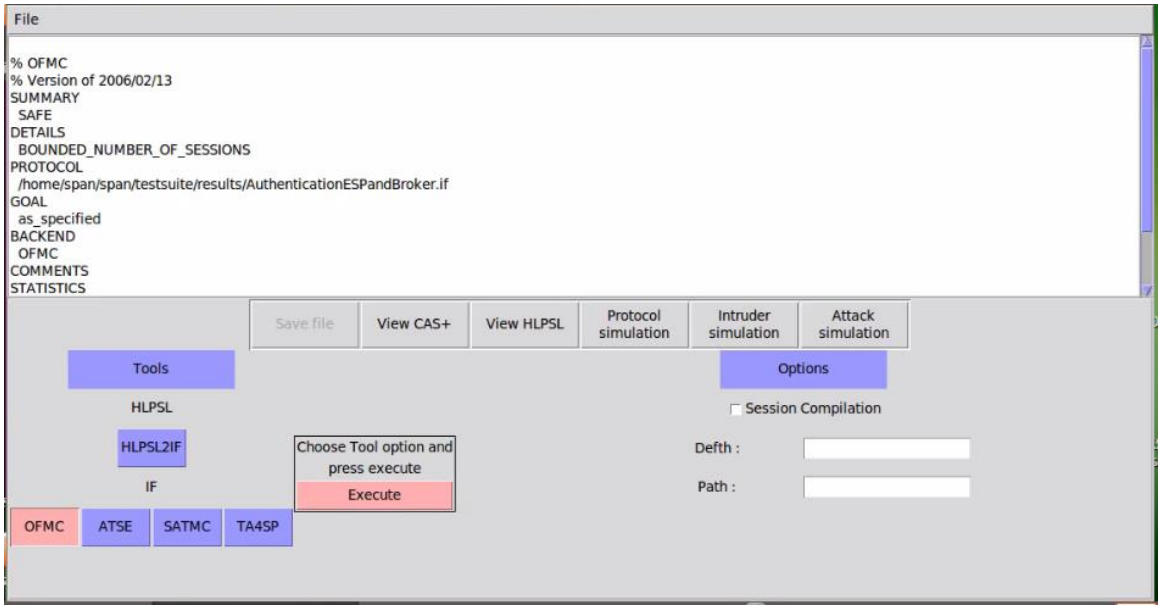

Figure 6: AVISPA results

As shown in the figure 6 a method that is proposed to be used for the generation of keys that makes use of AVISPA. On-the-fly Model-Checker (OFMC), which is one of AVISPA's four backends, is utilized to ascertain whether or not the objectives that are defined in the HLPSL's goal section are being accomplished. The backend is responsible for carrying out the protocol through a series of iterations that are limited in number. This process continues until either the protocol is judged secure for the specified number of sessions or an attack is detected. States are used as a model for the protocol in the HLPSL. In every state, there is a variable, and the transition from one state to another occurs whenever the value of the variable changes. The summary of the results indicates safe key generation environment after execution of the key generation and transmission process using OFMC and the related configurations.

5.4. Comparison

The study presents multiple comparisons that indicate the advance of the proposed key generation technique in many aspects including time complexity. The STR algorithm is similar to the idea of RSA algorithm then Comparisons have been done between them. The performance characteristics of the proposed algorithm are represented as follows in table 2.

Table 2: Comparison criteria for the proposed STR Key generation with RSA Key generation algorithm

Properties	STR	RSA [30]
Key Generation	Utilizes the unique properties of DNA sequences, particularly STRs, to generate encryption keys. The process involves combining DNA sequences from both the sender and receiver to form a unique key. This biological basis aims to ensure high uniqueness and security due to the low probability of DNA sequence duplication.	Relies on the mathematical properties of large prime numbers. The key generation involves selecting two large prime numbers, computing their product (the modulus), and deriving the public and private keys through modular arithmetic.
Key time	0.11ms	8.17s
Key size	32 or 64 bit	1,024 or 2,048 or 4,096 bits
Security	The security relies on the uniqueness of individual DNA sequences and the difficulty in reversing the DNA combination process. The experimental analysis suggests it offers the same level of	Its security is based on the difficulty of factoring the product of two large prime numbers. As of now, no efficient algorithm exists to factorize such numbers in a feasible

	security as RSA theoretically	time frame, making RSA secure against current computational capabilities.
Key Length and Complexity	The key length and complexity are tied to the DNA sequence data, which may vary in length but generally can be very large, offering a high level of security.	The key length typically ranges from 1024 to 4096 bits, with larger keys providing higher security. The complexity increases with the length of the key, making it computationally more intensive.
Practicality and Implementation	While innovative, practical implementation might be challenging due to the need for accurate DNA sequencing and processing capabilities. It also requires secure transmission of biological data.	Widely implemented and supported in various applications, RSA is practical and well-understood, with established protocols and hardware support.
Use Cases	Potentially useful in bioinformatics, secure communication in biological research, and areas requiring high-security authentication tied to biological identities.	Commonly used in secure communications over the internet, digital signatures, and encryption of sensitive data in various sectors.
Code size	3byte	46.4mbyte

As shown, the study compared the proposed algorithm with the RSA algorithm to illustrate that the proposed mechanism has characteristics identical to the RSA algorithm with the added ability to implement in biological environment.

6. Conclusion and Future Work

The proposed technique showed the key generating using the STR sequences, which is characterized by a unique fingerprint for each person. It is a method similar to the method of generating the key in the RSA. This resulted in an increase in the strength of the encryption and the time it takes to hack it, knowing that this method was not approved previously. The verification of mutual authentication between nodes is accomplished by the application of security verification based on AVISPA. An unofficial security study is presented in order to demonstrate how the proposed system is capable of withstanding any and all kinds of assaults.

Future work may include of implementation of the proposed system on a remote manner in order to provide the capability of using, controlling and managing the system in a wider range environment. Also, the use of Biosensors devices which have the capability to read STR sequence as an additional security feature and add biometric factors as a mutual authentication feature.

References

[1] Gamil R. S. Qaid and Nadhem Sultan Ebrahim (2023) “A Lightweight Cryptographic Algorithm Based on DNA Computing for IoT Devices”

[2] Jinwei Yu, Wei Xie, Zhenyu Zhong, Huan Wang,(2022) “Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation, Chaos, Solitons & Fractals”, Volume 162.

[3] Kairi, A., & Bhadra, T. (2023). "Decoding the future using a novel DNA-based cryptosystem". Journal of European Chemical Bulletin, 12, 3597-3609.

[4] Bahig, H. Nassr, D. (2019)” DNA-Based AES with Silent Mutations”. Arabian Journal for Science and Engineering, vol 44, pp. 3389-3403

[5] George, A. Singh, H. , (2017)”Design of Computing Circuits using Spatially Localized DNA Majority Logic Gates”. IEEE International Conference on Rebooting Computing (ICRC), Washington, DC, pp. 1-7

[6] Jian-Jun; Wang, Q.-W.; Yong, K.-Y.; Shao, F.; Lee, K.J. (2015). “Programmable DNA-mediated multitasking processor”. Journal of Physical Chemistry B. 119 (17): 5639–5644.
[7] Suyel Namasudra, , (2022) “A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure, Computers and Electrical Engineering”, Computers and Electrical Engineering. 104. 108426. 10.1016/j.compeleceng.2022.108426.
[8] Rajni, A. , (2017) “DNA Computing. International Journal Of Engineering And Computer Science”, India, vol 6 issue 1.
[9] Church, G. Gao, Y. Kosuri, S,(2012)”Next-Generation Digital Information Storage in DNA”, Science, New York
[10] Pan,C., Tabatabaei, S.K., Tabatabaei Yazdi, S.M.H. et al. (2022). “Rewritable two-dimensional DNA-based data storage with machine learning reconstruction”. Nat Commun 13, 2984
[11] Ahgue, A. O., De Nkapkop, J. D., Effa, J. Y., Franz, S., Adelis, P., & Borda, M. (2018(“ A DNA-based chaos algorithm for an efficient image encryption application”. In 2018 International Symposium on Electronics and Telecommunications (ISETC) (pp. 1-4). IEEE.
[12] B.Akiwate and L. Parthiban,(2018), “A Dynamic DNA for Key-based Cryptography,” International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India.
[13] Ali A.Yassin , Abdullah Mohammed Rashid , Abdulla J. Yassin , Hamid Alasadi,(2021),” A novel image encryption scheme based on DCT transform and DNA sequence”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 21, No. 3, March 2021, pp. 1455~1464
[14] Casey-Tyler Berezin, Samuel Peccoud, Diptendu M. Kar, Jean Peccoud, Cryptographic approaches to authenticating synthetic DNA sequences, Trends in Biotechnology,Volume 42, Issue 8, 2024.
[15] Sabry, Mona & Hashem, Mohammed & Nazmy, Taymoor & Khalifa, M.Essam. (2015)."Design of DNA-based Advanced Encryption Standard (AES)". 10.1109/IntelCIS.2015.7397250.
[16] Sherif H. El-Alfy, Ahmed F. Abd El-Hafez,Paternity testing and forensic DNA typing by multiplex STR analysis using ABI PRISM 310 Genetic Analyzer, Journal of Genetic Engineering and Biotechnology, Volume 10, Issue 1,2012.
[17] Sherif H. El-Alfy, Ahmed F. Abd El-Hafez, Paternity testing and forensic DNA typing by multiplex STR analysis using ABI PRISM 310 Genetic Analyzer, Journal of Genetic Engineering and Biotechnology, Volume 10, Issue 1, 2012
[18] Kumar, Sanjay, and Deepmala Sharma. 2023. "Key Generation in Cryptography Using Elliptic-Curve Cryptography and Genetic Algorithm" *Engineering Proceedings* 59, no. 1: 59.
[19] Xue Wei and Dola Saha. 2022. KNEW: Key Generation using NEural Networks from Wireless Channels. In Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning (WiseML '22). Association for Computing Machinery, New York, NY, USA, 45–50.
[20] Al-Shargabi, B., Al-Husainy, M.A.F. (2021). A New DNA Based Encryption Algorithm for Internet of Things. In: Saeed, F., Mohammed, F., Al-Nahari, A. (eds) Innovative Systems for Intelligent Health Informatics. IRICT 2020. Lecture Notes on Data Engineering and Communications Technologies, vol 72. Springer, Cham
[21] C. Patel and N. Doshi, "Secure Lightweight Key Exchange Using ECC for User-Gateway Paradigm," in *IEEE Transactions on Computers*, vol. 70, no. 11, pp. 1789-1803, 1 Nov. 2021.
[22] X. Gao, W. Du, W. Liu, R. Wu and F. Zhan, "A Lightweight and Efficient Physical Layer Key Generation Mechanism for MANETs," *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2020
[23] M. Indrasena Reddy, A.P. Siva Kumar, K. Subba Reddy, A secured cryptographic system based on DNA and a hybrid key generation approach, Biosystems, Volume 197, 2020.
[24] M. Jacovic, M. Kraus, G. Mainland and K. R. Dandekar, "Evaluation of Physical Layer Secret Key Generation for IoT Devices," *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*, Cocoa Beach, FL, USA, 2019, pp. 1-6, doi: 10.1109/WAMICON.2019.8765465.
[25] Yuliana, Mike & Wirawan, Iwan & Suwadi, Suwadi. (2019). An Efficient Key Generation for the Internet of Things Based Synchronized Quantization. Sensors. 19. 2674. 10.3390/s19122674.
[26] B.R.Pushpa, (2017) “A new technique for data encryption using DNA sequence,” International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017

[27] Wattar, Auday & Mahmod, Ramlan & Zukarnain, Zuriati & Udzir, Nur. (2015). "A New DNA-Based Approach of Generating Key-dependent ShiftRows Transformation". International Journal of Network Security & Its Applications. 7. 10.5121/ijnsa.2015.7107.

[28] O. F. Rashid, Z. A. Othman, S. Zainudin and N. A. Samsudin, "DNA Encoding and STR Extraction for Anomaly Intrusion Detection Systems," in *IEEE Access*, vol. 9, pp. 31892-31907, 2021.\

[29] Patil Rachana Yogesh, Devane Satish R, Formal Verification of Secure Evidence Collection Protocol using BAN Logic and AVISPA, Procedia Computer Science, Volume 167, 2020.

[30] Vishwakarma, Seema & Gupta, Neetesh. (2021). "An Efficient Color Image Security Technique for IOT using Fast RSA Encryption Technique". 717-722. 10.1109/CSNT51715.2021.9509697.