Iraqi Journal of Computers, Communications, Control and Systems Engineering

Volume 26 | Issue 1 Article 10

4-4-2026

Secret Key Generation from Real-Time Audio in Communication Apps

Rasha M. Mohsin
College of Computer Science, University of Technology-iraq, Baghdad, Iraq,
rasha.m.mohsin@uotechnology.edu.iq

IJCCCE 2026;26(1):134–144

RESEARCH ARTICLE

Secret Key Generation from Real-Time Audio in Communication Apps

Rasha M. Mohsin

College of Computer Science, University of Technology-iraq, Baghdad, Iraq

ABSTRACT

Social media platforms security growing challenge of Security vulerabilities, underscoring for secure communication channels and robust user privacy safeguards. Althought key exchange protocol of the Diffie-Hellman (DH) widely adopted, remains various attacks of susceptible asnumber_theoretic exploits, Discrete Logarithm Attacks (DLAs) and Man_in_the_Middle Attacks (MITMAs). This study aim to generate cryptographic key depend on WAV audio files. By operating the entropy and distinctiveness of speech and ambient sound. Audio features has extracting by system to generat secure keys compatible with the DH protocol. The facilitate of these keys is strong encryption and decryption processes, thereby that enhancing the security of communication. Method's effectiveness, highlighting its suitability for real-time deployment and its potential to enhance data protection across various applications which experimental validation has confirmed.

Keywords: Security attacks, Diffie-Hellman protocol, Cryptography, Wav file

Highlights

1. Novel key generation by using WAV.
2. Supports real-time implementation with low latency.
3. Increased entropy in the key generation process.
4. Simple integration with the existing DH protocol.

1. Introduction

Internet and advanced technologies, nowadays, such as mobile phones and computers had become essential factors in daily life, many devices connected together and data exchange between interconnected parties arise the need to provide protection means to these transmitted files; since some of these files contains important or sensitive information. Many techniques have had been invented to achieve this goal, such as information hiding, watermarking and data encryption and firewalls, these techniques aim to provde

Received 22 July 2025; revised 29 October 2025; accepted 23 November 2025.
Available online 4 April 2026

E-mail address: rasha.m.mohsin@uotechnology.edu.iq (R. M. Mohsin).

https://doi.org/xx.xxxxx/2617-3352.1522

the security for data against different types of threats [1]. Most traditional cryptographic systems employ complex mathematics to generate secure keys, but even these methods can be vulnerable to advanced hacking techniques [2].

In secure communication, the Diffie-Hellman key exchange is a key method used to let two parties safely share a secret over an untrusted network. The security of the protocol fundamentally relies on the generation of strong, unpredictable cryptographic keys. A large prime number and intricate mathematical operations are the main key features for keys generated [3]. The Diffie-Hellman key exchange protocol (DH) is one of many protocols that basic for applying these features, it is an asymmetric cryptography system protocol, it uses two keys public and private key, private key must exchange over an protected channel, but it has numerous security flaws, including number theory-based attacks, Discrete Logarithm Attacks (DLA) and Man-in-the-Middle attacks (MIM) [4].

Recent research in cryptography has focused on methods for generating alternative keys to protect keys from attacks using unexpected tools, including the utilization of multimedia data such as audio recordings. Today, it has become common to use unique methods to generate keys to ensure their protection; however, a problem has emerged: when data for cryptographic key generation or difficulty in regenerating keys is a primary concern, it poses a significant challenge to encryption methods or key exchange protocols.

There has been a growing trend of using distinct, naturally occurring data to generate cryptographic keys [5]. Different soarces have been employed in the process of key generation such as image, video files and audio files, audi files such as wav files have several propertiessuch as large amount od data since the wav file is not compressed that make them an efficeien source for generating exchange keys [6].

This research propose a method for secret keys generation from wav files, the generated keys have specific properties and can be employed in Diggie-Hellman key exchange protocol.

Through experimental analysis, the demonstrate the effectiveness and security of an approach, highlighting its potential applications in various fields, including secure communication, digital rights management, and authentication systems. The rest of an article is divided into five sections. Section 2 presents a discussion of related works on improvements to the Diffie-Hellman algorithm. Section 3 explains the theoretical background for security attacks and the Diffie-Hellman protocol. Section 4 describes the proposed technique for extracting the keys. Section 5 shows the results of the proposed technique. Finally, Section 6 will conclude the research.

2. Related works

In the following section, several techniques adopted by authors who relied on multimedia files to generate private and public keys for the key exchange process are reviewed, along with other related methods. The key features identified in these studies are summarized as follows:

- Murali P and Palraj R in 2011, provided an approach that depended on an image sent from source to destination to generate the key exchange. The true random number generator generated the private key on a Monochrome image, which has a size of 25×25 pixels. The approach was considered cost-effective and easy to apply; however, an attacker could easily guess it due to the low entropy of the image [7].
- Sharma P, Naga R. Lakshman Dileep et al. in 2018, the researchers proposed a method to extract the secret and public keys of the Diffine-Hellman protocol by applying the XOR function to specific rows and columns within an image. The number of columns

are multiples of eight in an image. The suggest way is easy for keys genration but also louded opportunity to discovery of keys by an attacker [8].

- Mohsin R. M. et al. [2019], the researchers proposed a method to improve the security of Diffine-Hellman protocol by two steps for each cryptography process firstly, generate a color image randommly that utilized to key genration process. The keys generation is second step made by XOR function applied on the generated image values. The limitation of suhhested method is the generated image, as it raises the attacker's suspicion and thus an attempt to discover the keys [9].
- Sheba Malarchelvi in 2021. The study propose key generation approach that integrate between two technque Elliptic Curve Diffie-Hellman (ECDH) protocol and Chinese Remainder Theorem (CRT). The Researchers aiming to minimize both communication overhead and computational complexity for secure data exchange [11].
- Gupta and N. V. S. Reddy (2022). The work suggests that the classical Diffie-Hellman algorithm can be combined with RSA algorithms for improved authentication and data security. The combined approach offers improved resilience against Man-in-the-Middle attacks. However, it introduces higher computational overhead and increased resource consumption, which may pose challenges for low-power devices. Moreover, the confidentiality level is directly tied to the RSA key length shorter keys significantly weaken the system's resistance to unauthorized access [10].
- Smith, M. Lee, and A. Kumar [2023], presented work on real-time key generation algorithms in 60 GHz mmWave systems, which utilized the physical layer parameters such as RSS and AoA. This method generates symmetric keys using a directed mmWave signal. While this type of signal is resistant to eavesdropping, it cannot generate exchange keys. The downsides of this method include challenges such as synchronization accuracy, vulnerability to environmental factors, and its ineffectiveness with common encryption systems, such as RSA, which affects efficiency and security [18].
- Ismail R et al. [2025]. The present authors propose an original method for creating asymmetric cryptographic keys, utilizing the random order of bits within pixels. Using varying pixels, objects in motion, and colors, their system produces high-entropy bit sequences, which are an improvement over the traditional pseudo-random number generators. Although the method improves the randomness of keys, it suffers from high computational complexity, insensitivity to video quality or scene changes, and extra calculations for asymmetric key systems like RSA and ECC [19].

The method of generating a key based on the audio proposed differs from previous works in:

- Dimensional engagement of randomness by structured diagonal extraction and XOR gate.
- Generating both public and private keys directly from ambient audio
- Enabling real-time implementation with minimal computational overhead
- Seamlessly integrating with existing DH protocols without requiring specialized hardware

3. Diffie-Hellman algorithm

Diffie-Hellman Algorithm (DH) was discovered by Whitfield Diffie and Martin Hellman and published in 1976, where its name (Diffie-Hellman) comes from the final names of its discoverers. It is a numerical algorithm used for confidential communications between two devices in different regions, even though they may have never met [9, 12].

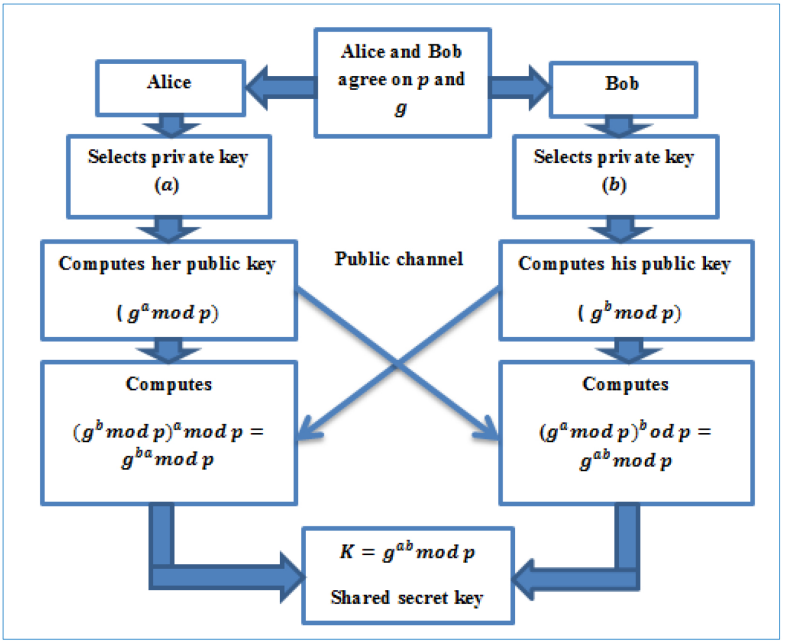

Fig. 1. Diffie-Hellman algorithm.

The Diffie-Hellman protocol is based on applying public-key encryption, which works in an unsecured medium (a public channel), utilizing two keys to cipher and decipher, known as the public and private keys [10]. The Diffie-Hellman protocol works as shown in the following steps [13]:-

1. Source (Alice) and destination (Bob) concur on a prime number (g, p) as it is an elementary root.
2. Source (Alice) and destination (Bob) have selected keys that are familiar to them, called 'a' and 'b', respectively, as their private keys.
3. The source's public key is generated by (A = g^a mod p).
4. Destination's public key is generated by (B g b mod p).
5. The source and destination swap their public keys. Now, the source has B and the destination has A.
6. The source computes B a mod p = gba mod p = K.
7. The destination computes A b mod p g ba mod p K.

Then, the source and destination get 'K' as their shared secret key, which is displayed in Fig. 1.

4. Security attacks on Diffie-Hellman protocol

In the past decade, the structure of cryptography has proven useful in resolving problems with its capabilities. However, it is typically prevented by attacks, including key exchanges and user communication. Swapping keys between two users who do not share a secret channel is difficult. Some of these attacks are [14]:

4.1. Man in the middle attack

In the type of security attack, an attacker inserts himself between two individuals who are involved in the key exchange and secure connection. The attacker places itself between the sender (Alice) and the receiver (Bob). Where the sender thinks he is exchanging information with the receiver, while the receiver thinks he is exchanging information with the sender. That allows the attacker to intercept any information passing through an erroneously protected channel, obtaining both public keys (ga and gb), and then pass a harmful third key (gc) to both [1, 14].

4.2. Discrete logarithm attack (DLA)

The Diffie-Hellman protocol is based on a finite cyclic group G, which involves computational difficulties known as discrete logarithms. The protocol's security decreases depending on the ease of discrete logarithm computation. The discrete logarithm (DL) is a mathematical problem that occurs in many settings of (x) when the base (g) is the smallest nonnegative integer, such as ($x = ga$), which is written ($\log_g x = a$), where (x) has been taken regularly at random from the group. The problem of discrete logarithm in a periodic group G is to find the discrete logarithm of x to the base g. The first step in the Diffie-Hellman protocol, sender (Alice) and receiver (Bob) concur on a large prime (p) and a nonzero integer (g) that (g modulo p). Alice and Bob make the values of (p) and (g) public information, so the attacker realizes them, and the sender and receiver have the option of a secret integer (a,b) that is not disclosed to anyone. They used their unknown integers to compute $A \equiv ga \pmod p$ and $B \equiv gb \pmod p$ and then exchanged them through an unsecured channel. The attacker can know the shared value determined by the sender(Alice) and receiver (Bob) if they calculate discrete logarithms; contrariwise, if an attacker can compute the shared value, he will be able to calculate the discrete logarithm, so the safety of keys shared depends on how difficult the difficulty [1, 15].

5. Waveform audio file

The WAV (Waveform Audio File Format) is a popular audio file format developed by IBM and Microsoft in 1991. It is widely used for storing high-quality, uncompressed audio data. Here are some key features of the WAV format [16]:

1. **Uncompressed Audio**: WAV files preserve audio data in its original form for high sound quality.
2. **Lossless Quality**: The data stored in a wav file is raw, uncompressed, providing complete, untampered data, the original quality is preserved.
3. **Large File Size**: Since the file is not compressed, the amount of data will be large, which will result in a large file size, so problems will arise in the transfer and storage processes.
4. **Metadata Integration**: WAV files may include variouse informations such as artist name, release date and trck details. These informaations added for better file organization.
5. **Multi-Channel Support**: The wave file supports multiple channels, which allows for the inclusion of some advanced features such as surround sound, tuning, and audio mixing.

6. **Platform Compatibility**: Although the WAV file is widely used across various operating systems and applications, there are some applications that impose limitations such as file size or format on playing this type.

6. The proposed technique

The robustness of the Diffie-Hellman key exchange protocol is fundamentally dependent on the generation of cryptographic keys that are both strong and unpredictable. In traditional approaches usually, use large prime numbers with complex mathematical operations to confirm security behind to increase the confidentiality. However, the proposed algorithm improve thses approches by utilize the unique properties of WAV audio files to generate keys and enhance the security of any algorithms that falls under the key exchange protocols and introducing a novel and effective solution to genrate both public and private keys through an audio file extracted from any multimedia program(viber, whats up and other) in real time, which improves the protocol security and avoids the security attacks issues. The approach mitigates common security vulnerabilities and enables dynamic key generation without relying solely on mathematical randomness. The audio file used for key extraction can be transmitted over any communication channel, whether the audio file can send through any channel public or secure in any application like the social media applications (Facebook, what's up, Viber, and others). The algorithm underlying the proposed technique is detailed in the following algorithm.

Algorithm 1: WAV-KeyGen for Diffie-Hellman.

Input: WAV file (audio waveform)
Output: Cryptographic key for Diffie-Hellman protocol
Begin
Step 1: Read the WAV File
- Load the WAV file and extract audio samples into a 1D array A[]
- Retrieve metadata: sample rate, number of channels

Step 2: Preprocessing
- Let L be the total number of audio samples in A[]
- Determine the largest integer N such that $N \times N \leq L$
- If $L > N \times N$: trim A[] to the first $N \times N$ samples
- If $L < N \times N$: pad A[] with zeros to reach $N \times N$ length
- Reshape A[] into a square matrix M[N][N]

Step 3: Diagonal Vector Extraction
- Extract main diagonal → V1[i] = M[i][i]
- Extract secondary diagonal → V2[i] = M[i][N - 1 - i]

Step 4: XOR Operation
- For each i in 0 to N - 1:
X[i] = V1[i] XOR V2[i]

Step 5: Prime Selection
- Search array X[] for the two largest prime numbers
- Assign them as P and Q

Step 6: Diffie-Hellman Integration
- Use P,Q as input parameters for key exchange protocol(like DH protocol)
- Execute DH protocol to shared secret key

End

Explain an Algorithm 1 how can converts an audio signal into a structured digital matrix, which base for generating keys, as outlined in the following steps.

1. Audio Acquisition and Preprocessing
   The algorithm begins by upload audio file to expract sample data and put in 1D array A[]. To prepare the samples for matrix operations, the array is reconstract into 2D array M[N][N], where N is the largest integer satisfying $N^2 \leq L$, and L is the total number of audio samples. Now, if the samples count override N^2, the array is reduced, if it falls short, zero-padding is applied to ensures consistent clarity array construction.
2. Diagonal Extraction and XOR Operation From the square matrix, derives two vectors: Vector V_1 is the primary diagonal and V_2 is the secondary diagonal, each that present some of audio-based sequences. A bitwise XOR operation is then applied between corresponding elements of V_1 and V_2, resulting in a new array X[] characterized by elevated entropy levels:
   $X[i] = V1[i] \oplus V2[i]$
3. Prime Validation Method: Important security step in in the Diffie-Hellman key generation process to ensure the cryptographic integrity of generated keys. Each number extracted from WAV file after applying XOR function is subjected to a primality test. Due to the possibility of large numbers appearing and also to improve accuracy of the results the Miller-Rabin probabilistic test is employed. The Miller-Rabin test is widely accepted in many cryptographic applications thrught the efficiency and reliability. The strength of Miller-Rabin test depends on the number of cycles used. While the multiple rounds are led to increase statistical confidence. The proposed algorithm tests the number through ten consecutive cycles to ensure the integrity of the chosen number.

A novel method is used to generate cryptographic keys from WAV audio files in the WRKBB dataset, which contains over 13,100 recordings of one speaker reading non-fiction book. The approach offers an effect pathway for protecting sensitive data to exchange over internet, while found some of the limitations found in traditional algorithms. Also it enhances digital communication security in traditional key excgange protocol to produce a new approach for key exchange operations based on confidentiality, high reliability and protection against attacks.

7. Results and discussion

7.1. Experimental results

The proposed system was evaluated by using database extracted from authentic voice recordings in WhatsApp to improve real-world communication scenarios and highlights its potential for secure key generation based on everyday speech inputs. The proposed system was implemented in a series of experiments to evaluate the effectiveness of the proposed algorithm. The outcomes show that the technique can produce cryptographic keys that are both secure and unexpected. The important metrics listed below were examined Table 1. Were the effectiveness of proposed system is contingent on high-quality audio recordings and proper handling of privacy concerns.

The Measure of the time required for key generation and how long it take time to generate these cryptographic keys from WAV files. The results present that the algorithm is suitable for real-time applications (like whatsoever and other reality program) as the algorithm can generate keys in a few amounts of time.

The Table 1 shows a set of tests like for a 9-second WAV file, the key creation procedure took about 0.073458 seconds on average.

Table 1. Experimental results.

Samples	Length (s)	No. of keys	Largest key 1	Largest key 2	Time to generate (s)
S1	8	92	101	97	0.05234
S2	5	101	107	103	0.054029
S3	9	125	127	*113*	*0.07343*
S4	1	61	127	109	0.029343

Table 2. Comparison results.

Samples	Sample Type	Size	Time to generate (s)	Entropy Source
Proposed system	Audio (WAV)	1 second	0.0293	Audio waveform (amplitude + frequency)
Mohsin R.M. et al. [9]	Image matrix	25×25	0.049	Pixel intensity
Murali P. and Palraj R [7]	Image matrix	25×25	0.0003	Matrix sampling
Ince et al. [20]	Video frame	1 frame (video)	0.0021	Chaotic TRNG (Lorenz, Chen-Lee)
Mohsin et al. [12]	Video stream	1 second (frame-based)	~0.031	Frame luminance + motion vectors

- Comparison with Advanced Methods:

The proposed approach was evaluated by comparing it with the work of other researchers to generate secret keys and the system showed. As illustrated in Table 2, the proposed system exhibits enhanced security by operating seamlessly in real-world environments without triggering alerts or suspicion from potential attackers. This capability minimizes the risk of data exchange over internet. The system design to reduce significantly the likelihood of any targeted cryptographic attacks. Additionally, WAV audio files with high entropy present introduces a substantial enhancement in randomness addition to improved security. Unlike other static algorithms, audio signals exhibit naturally fluctuating and unpredictable patterns, making it considerably more difficult for attackers to infer or replicate the generated keys. The variability in real audio contributes to the system's resilience and strengthens its cryptographic robustness. The Table 2 represents a comparison between five previous works on different key generation methods with highlighting on differences in sample type, size, time to generate and Entropy Source. The audio-based method stands out with a solid balance—it takes just 0.0293 seconds to generate a key from a 1-second audio clip. Its strength comes from the dynamic nature of audio file, which enables it to adapt to different environments and remain hidden when necessary.

Beginning with Murali & Palraj [7] and Mohsin et al. [9], rely on static image matrices to extreact keys, the experiments were faster in Murali's case (0.0003 s) but lack contextual randomness. These image based methods may raise suspicion due to their synthetic nature, especially in constrained or monitored environments

While Ince et al. [10], introduce algorithem based on chaotic TRNGs on video frames, achieving high speed (0.0021 s) but based on mathematical chaos rather than multimedia content, thus increased in complication of the processes. Jawed & Sajid [11] utilize numerical entropy enhanced by Whale Optimization, offering algorithmic efficiency (~0.005 s), but with limited real-world variability.

The proposed system by Mohsin et al. [12], video-based system extracts entropy from motion vectors and luminance, achieving a generation time of ~0.031 seconds. It offers a multimedia-driven approach that enhances randomness, but this method led to a complication of the processes. Overall, the proposed system ability to operate in

real-world environments without alerting attackers, leveraging natural entropy sources that are difficult to replicate or predict.

7.2. The approach discussion

The discussion worked on presents a extensive analysis of obtained results from many experments of the proposed system based on to real samples extracted from WhatsApp Voice messages. The proposed system aim to generate keys for key exchange protcol (like Diffie-Hellman protocol), by leveraging the inherent unpredictability of audio waveforms, the system produced keys with high entropy for generation process. The evaluation containt many aspect limitations,practical relevance, key findings, implications and the Prime Validation Method.

1. **Key Observations**
   - The algorithm produce secure and unpredictable keys extracted from WAV file features with remained efficiency when different lengths of audio samples.
   - Key generation exhibited minimal latency, with execution times ranging from 0.0293 to 0.0734 seconds, affirming its applicability in real-time environments.
   - Cryptographic integrity was validated using the Miller-Rabin primality test, with multiple iterations reinforcing statistical confidence in the generated keys.
2. **Limitations**
   - The effectiveness of proposed system is affected by the quality of the input audio,the noisy or of low resolution may reduce the available entropy, thereby compromising the Number and size of generated keys.
   - The approach presumes access to clean audio samples, which may not be feasible in all operational contexts.
   - Current implementation is confined to the Diffie-Hellman protocol; broader applicability requires validation across diverse cryptographic frameworks.
3. **Implications**
   - Experiments has proven that audio waveforms is effective source of entropy and securely generating keys, offering new perspectives on real or physical security (PHY security).
   - The stochastic nature of audio data enhances resistance to key prediction and duplication, strengthening defenses against both passive and active attacks.
   - Audio-based key generation, due to its covert characteristics, reduces the likelihood of detection during transmission—an advantage in adversarial scenarios.
4. **Practical Relevance**
   - The algorithm is lightweight and efficient for real-time applications such as IoT devices, secure communication, and voice authentication.
   - The ubiquity of audio content through social media platforms (e.g., WhatsApp, Viber) enables practical deployment without the need for specialized hardware.
   - The method offers a lightweight, scalable solution for secure key exchange, particularly suited to resource-constrained environments.

8. Conclusion

The paper shows a novel algorithm for cryptographic key generation, like the Diffie-Hellman key exchange protocol using real-sound audio like whats-up and other applications of social media. The proposed algorithm improved security behind to unpredictability key by novel algorithm for key generation by using a WAV audio file

and taking advantage of the special characteristics of wave forms. The experimental results present that the algorithm is suitable for real-time applications (like what's up and other reality program) as the algorithm can generate keys in a few amounts of time the effectiveness of the novel. The novel approach makes suitable solution for some of the limitations of traditional key exchange techniques to improve secure communication, in addition to data protection in various domains. Also, it can be used in conjunction with any social media application and further optimization. The algorithm to enhance its applicability and performance. However, the system has certain limitations. The system's performance is influenced by the quality and diversity of the input audio, low-entropy or repetitive signals may weaken the strength of the generated keys. Moreover, assessing entropy in real-time environments remains a significant challenge, particularly when audio sources are noisy or compressed. Future work will focus on optimizing entropy extraction and integrating adaptive filtering techniques to enhance robustness and applicability.

Acknowledgment

None.

Conflict of interest

The authors declare no conflict of interest.

Data availability

The dataset used in this study (LJ Speech dataset) is publicly available and can be accessed online.

References

[1.] C. Gupta and N. V. S. Reddy, "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography," *Journal of Physics: Conference Series*, vol. 2161, no. 1, pp. 012014, 2022.
[2.] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 1996.
[3.] I. S. Diffie, W., and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[4.] S. A. Khader and L. David, "Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol," *22nd International Conference on Telecommunications (ICT 2015)*, 2015, 978-1-4799-8078-9/15/$31.00 ©2015 IEEE.
[5.] I. Alouani, "Breaking (and fixing) channel-based cryptographic key generation: a machine learning approach," In *Proceedings of the 25th Euromicro Conference on Digital System Design*, 2022, pp. 383–390. IEEE.
[6.] R. Borrás, J. Macías-Guarasa, E. Martín, and A. Peinado, "On the Use of Audio Features for Cryptographic Key Generation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 814–825, 2014.
[7.] P. Murali and R. Palraj, "True random number generator method based on the image for key exchange algorithm," *International Symposium on Computing, Communication, and Control*, 2011.
[8.] P. Sharma, R. Naga, L. Dileep, S. C. Bhargavi, and S. Ranjan Pattanaik, "A New Technique of Generating Key for Diffie Hellman Algorithm," *International Journal of Mechanical Engineering and Technology*, vol. 9, no. 1, pp. 565–571, 2018.
[9.] R. M. Mohsin, R. I. Ahmed, R. Yaqub, and S. Ethar, "A new technique for Diffie-Hellman key exchange protocol security using random image generation," *Proceedings of the First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 262–267.
[10.] C. Gupta and N. V. S. Reddy, "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography," *J. Phys.: Conf. Ser.*, vol. 2161, no. 1, pp. 012014, 2022.

[11.] S. Malarchelvi, "Self-Similar Key Generation for Secure Communication in Multimedia Applications," *Journal of Multimedia Security*, vol. 5, no. 4, pp. 112–119, 2021
[12.] S. F. Fahmy "Secure voice cryptography based on Diffie-Hellman algorithm," *2nd International Scientific Conference of Engineering Sciences (ISCES 2020), IOP Conf. Series: Materials Science and Engineering*, vol. 1076, pp. 012057, 2021, doi:10.1088/1757-899X/1076/1/012057.
[13.] A. Kumar C. and P. M. Durai Raj Vincent, "Enhanced Diffie-Hellman algorithm for reliable key exchange," *14th ICSET-2017, IOP Conf. Series: Materials Science and Engineering*, vol. 263, pp. 042015, 2017, doi:10.1088/1757-899X/263/4/042015.
[14.] A. A. Jain, K. Nandakumar, and A. Ross, "Biometric Cryptosystems: A Review of Recent Advances and Future Directions," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 3, March 2024.
[15.] M. F. Bollauf, R. Parisella, and J. Siim, "Revisiting Discrete Logarithm Reductions," *IACR Cryptology ePrint Archive*, vol. 2025, no. 1079, pp. 1–20, 2025.
[16.] E. Chen, *Digital Audio Explained: Formats, Fidelity, and Future Trends*, AudioTech Press, 2024.
[17.] K. Ito and L. Johnson, "The LJ Speech Dataset," 2017, https://keithito.com/LJ-Speech-Dataset.
[18.] J. Smith, M. Lee, and A. Kumar, "Real-time Physical Layer Secure Key Generation in a mmWave Communication System," *Proc. IEEE Int. Conf. on Communications (ICC)*, Paris, France, pp. 1234–1239, June 2023.
[19.] R. I. Ahmed, R. Mohammed, and S. F. Hassan, "Random Keys Generating for Asymmetric Cryptography using Video Entropy," *Academic Science Journal*, vol. 3, no. 3, 2025.
[20.] M. Ince, M. A. Ozdemir, and M. Kaya, "A novel Cosine-Cosine chaotic map-based video encryption scheme," *Journal of Electrical and Applied Systems*, vol. 4, no. 1, pp. 1–20, 2024.