IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Review Paper on Competent Cryptography Schemes for Network Security

Kartika Yadav
School Of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Chanchal Agrawal
School Of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Anchal Gupta
School Of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh

Abstract **- Network Security and Cryptography are the concepts to protect network and data transmission over wireless networks. Network Security involves the authorization of access to data, controlled by the network administrator. Network Security covers a variety of computer networks, both public and private, that are used in communications among business, conducting transactions and, in government agencies and individuals. Networks can be private, such as within a company, and other which might be open to public access. Network Security is involved in organizations, enterprises, and institutions.**

Cryptography is the science of information security. The word is derived from the Greek word "kryptos", meaning concealed. Cryptography includes techniques like merging words with images, microdots and other ways to hide or transit. Some applications of cryptography are ATM cards, computer passwords, etc. Cryptology in modern times is the same with Encryption. Encryption is the translation of understandable information to plain nonsense.

In this paper we studied cryptography along with its principles and encryption in the field of Network Security. Also, the cryptographic systems with cipher are described. Cryptographic models and algorithms are outlined.

I. INTRODUCTION

Network security is a critical aspect of modern digital systems and communication networks. The primary aim of network security is to safeguard the confidentiality, integrity, and availability of data transmitted over networks, while also protecting against unauthorized access, data breaches, and malicious activities.

Cryptography plays a crucial role in achieving the goals of network security. It provides a set of techniques and algorithms that enable secure communication and data protection. Cryptography involves the use of mathematical algorithms to transform plaintext data into cipher text, making it unreadable to unauthorized entities.

The importance of cryptography schemes in network security can be summarized as follows:

1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation
5. Key Management

A. Objective:

1. To provide a comprehensive analysis of competent cryptography schemes commonly used in network security.

2. To evaluate the security features, performance, scalability, and suitability of these cryptographic schemes.
3. To identify the strengths and weaknesses of different cryptography schemes for network security.
4. To highlight emerging trends and challenges in network security and their impact on cryptography schemes.

B. Scope:

1. The review paper will cover a broad range of cryptographic techniques used in network security, including symmetric encryption algorithms, asymmetric encryption algorithms, digital signatures, key exchange protocols, and secure hashing functions.
2. The focus will be on evaluating the competence and effectiveness of these cryptographic schemes in providing confidentiality, integrity, authentication, and other security properties.
3. The evaluation will consider factors such as security features, key lengths, computational complexity, performance, and resistance to known attacks.
4. The review will explore the suitability of cryptographic schemes for different network security scenarios, such as data transmission over public networks, secure communication between entities, and protection against various threats.
5. The paper will also address emerging trends in network security, such as quantum computing, post-quantum cryptography, and side-channel attacks, and discuss their implications for cryptographic schemes.
6. Potential future directions for cryptographic schemes in response to emerging trends and challenges will be suggested, including areas for further research and development.

II. Symmetric Encryption Algorithms

Symmetric encryption is a cryptographic technique that involves the use of a shared secret key for both the encryption and decryption processes. It is also known as secret key encryption or conventional encryption. In symmetric encryption, the same key is used by the sender to encrypt the plaintext and by the recipient to decrypt the cipher text, hence the term "symmetric."

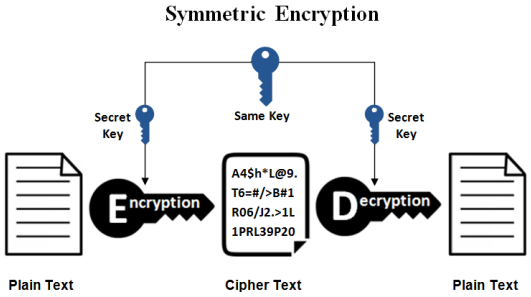

Fig 1. Symmetric Encryption

The role of symmetric encryption in network security is crucial and multifaceted. Here are the key aspects of its role:

1. Confidentiality: The primary role of symmetric encryption in network security is to provide confidentiality. By using a shared secret key, symmetric encryption ensures that only authorized parties can access and understand the information being transmitted. It prevents unauthorized interception and eavesdropping by encrypting the plaintext into cipher text, which can only be decrypted using the same secret key.
2. Data Integrity: Symmetric encryption also plays a role in ensuring data integrity within network communications. By encrypting the data, any modification or tampering with the encrypted message during transmission can be detected. If the cipher text is altered, the decryption process will result in incorrect plaintext, indicating that the data integrity has been compromised.
3. Performance: Symmetric encryption algorithms are typically faster and more computationally efficient than their asymmetric counterparts. This makes them suitable for securing large volumes of data and high-speed network communications. The efficiency of symmetric encryption enables real-time encryption and decryption of data without significant latency, ensuring smooth and secure network operations.
4. Key Management: Symmetric encryption requires the secure exchange and management of the shared secret key. Key management is an essential aspect of network security, and symmetric encryption schemes simplify the key management process. As there is only one key involved, distributing, and updating the shared secret key among authorized parties is relatively straightforward compared to asymmetric encryption, where key distribution is more complex.
5. Hybrid Encryption: Symmetric encryption is often used in conjunction with asymmetric encryption in a hybrid encryption scheme. In this approach, asymmetric encryption is used

to securely exchange the symmetric encryption key. Once the symmetric key is securely exchanged, the actual data transmission occurs using the more efficient symmetric encryption. This combination harnesses the advantages of both encryption types, achieving the security of asymmetric encryption and the efficiency of symmetric encryption.

- REVIEW OF COMPETENT SYMMETRIC ENCRYPTION ALGORITHMS, SUCH AS AES, TWOFISH, AND SERPENT:

There are several symmetric encryption algorithms available that are widely used for network security. Here, we review three of the most competent symmetric encryption algorithms, including AES, Twofish, and Serpent.

1. Advanced Encryption Standard (AES): AES is a widely used symmetric encryption algorithm and is considered one of the most secure. It was developed to replace the older Data Encryption Standard (DES) algorithm. AES uses a block cipher with variable key lengths of 128, 192, or 256 bits. It employs substitution-permutation network (SPN) with multiple rounds of encryption to ensure secure data transmission. AES is widely used in various network security applications, including VPNs, SSL and TLS protocols, and secure file transfers.
2. Twofish: Twofish is a symmetric encryption algorithm that uses a block cipher with key lengths of 128, 192, or 256 bits. It employs a Feistel network with 16 rounds of encryption. Twofish has excellent resistance to known cryptographic attacks and is considered one of the most secure symmetric encryption algorithms. Twofish is widely used in secure file transfers and disk encryption.
3. Serpent: Serpent is a symmetric encryption algorithm that uses a block cipher with key lengths of 128, 192, or 256 bits. It employs a substitution-permutation network (SPN) with 32 rounds of encryption. Serpent is considered one of the most secure symmetric encryption algorithms due to its high resistance to known cryptographic attacks. Serpent is commonly used in secure file transfers and disk encryption.

- EVALUATION OF SYMMETRIC ENCRYPTION ALGORITHMS:

A. Advanced Encryption Standard (AES):

- Security Features: AES is widely regarded as a highly secure encryption algorithm. It provides strong security features, including confidentiality, integrity, and authenticity of data. AES has undergone extensive analysis by the cryptographic community and is resistant to known attacks.
- Key Lengths: AES supports three key lengths: 128, 192, and 256 bits. The longer the key length, the stronger the encryption and resistance to brute-force attacks. AES with a 256-bit key length offers the highest level of security.
- Performance: AES is known for its excellent performance characteristics. It has been optimized and implemented efficiently in both software and hardware, making it suitable for high-speed network communication. AES encryption and decryption operations are computationally efficient, providing real-time processing capabilities.

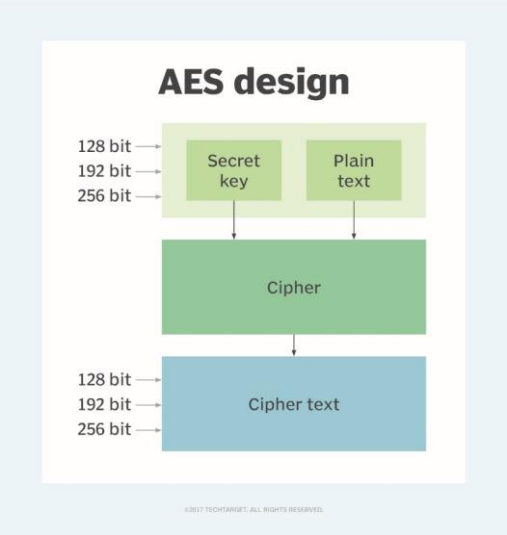

Fig 2. Advanced Encryption Standard

B. Twofish:

- Security Features: Twofish is a robust symmetric encryption algorithm with strong security features. It has undergone thorough analysis and is designed to resist known cryptographic attacks. Twofish ensures confidentiality and integrity of data and provides a high level of security.
- Key Lengths: Twofish supports key lengths of 128, 192, and 256 bits, offering flexibility in selecting the desired level of security. Longer key lengths enhance resistance to brute-force attacks and provide stronger encryption.
- Performance: Twofish exhibits good performance in software implementations, making it suitable for various network security applications. It can efficiently encrypt and decrypt data, allowing for real-time processing.

C. Serpent:

- Security Features: Serpent is a highly secure symmetric encryption algorithm known for its strong security features. It has been thoroughly analyzed and is designed to resist known attacks. Serpent ensures

confidentiality, integrity, and authenticity of data.

- Key Lengths: Serpent supports key lengths of 128, 192, and 256 bits, providing flexibility to choose the desired level of security. Longer key lengths enhance resistance against brute-force attacks and offer stronger encryption.
- Performance: Serpent has a more conservative design, which can result in slower encryption and decryption compared to some other algorithms. However, with hardware optimizations, its performance has been improved, making it suitable for various network security applications.

III. Asymmetric Encryption Algorithms

Asymmetric encryption, also known as public-key encryption, is a cryptographic technique that uses a pair of keys: a public key and a private key. Unlike symmetric encryption, where the same key is used for both encryption and decryption, asymmetric encryption employs different keys for these operations.

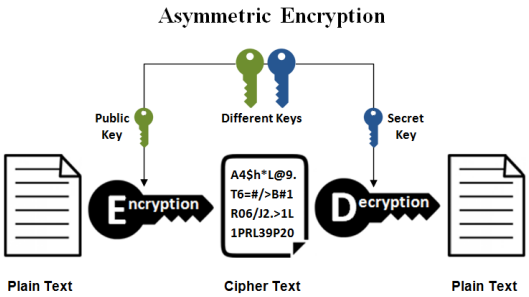

Fig 3. Asymmetric Encryption

In asymmetric encryption, the public key is widely distributed and used for encryption, while the private key is kept secret and used for decryption. The public key can be freely shared with anyone, allowing them to encrypt data intended for the owner of the corresponding private key. Only the private key holder can decrypt the ciphertext using their private key.
Here are some key aspects and applications of asymmetric encryption in network security:

1. Confidentiality: By encrypting data using the recipient's public key, only the intended recipient, who possesses the corresponding private key, can decrypt and access plaintext. This ensures that sensitive information remains confidential during transmission over the network.
2. Authentication: Digital signatures are created using the sender's private key and can be verified using their corresponding public key. By verifying the digital signature, the recipient can authenticate the sender's identity and ensure the integrity of the received data.
3. Key Exchange: The Diffie-Hellman key exchange protocol allows two parties to establish a shared secret key over an insecure network without directly transmitting the key itself.
4. Secure Protocols: There are so many secure protocols, such as SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security). These protocols use public-key encryption to establish secure connections between clients and servers, ensuring confidentiality, integrity, and authentication of data transmitted over the network.
6. Secure File Transfer: SFTP (SSH File Transfer Protocol), is a protocol to ensure the confidentiality and integrity of transferred files. The sender can encrypt the file using the recipient's public key, and only the recipient possessing the corresponding private key can decrypt and access the file.

- REVIEW OF COMPETENT ASYMMETRIC ENCRYPTION ALGORITHMS:

1. RSA (Rivest-Shamir-Adleman): RSA is one of the most widely used and trusted asymmetric encryption algorithms. It is based on the mathematical difficulty of factoring large composite numbers. Key features of RSA include:
   - Security Features: RSA provides strong security features, including encryption, decryption, and digital signatures. It ensures confidentiality, integrity, and authenticity of data.
   - Key Lengths: RSA supports various key lengths, typically ranging from 1024 to 4096 bits. Longer key lengths provide higher security but may require more computational resources.
   - Performance: RSA encryption and decryption operations are slow compared to symmetric encryption algorithms. However, with optimized implementations and hardware acceleration, RSA performance can be improved.
2. Elliptic Curve Cryptography (ECC): ECC is a modern asymmetric encryption algorithm that uses the mathematics of elliptic curves over finite fields.

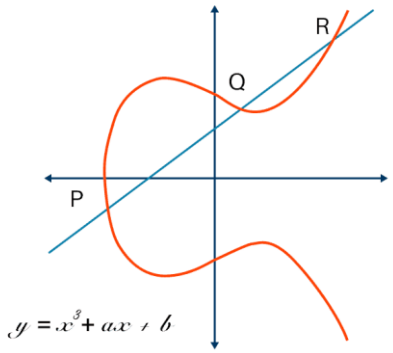

Fig 4. Elliptic Curve Cryptography

It offers comparable security to RSA with smaller key sizes, making it more efficient in terms of computation and memory usage. Key features of ECC include:

- Security Features: ECC provides strong security features, including encryption, decryption, and digital signatures. It ensures confidentiality, integrity, and authenticity of data.
- Key Lengths: ECC uses much smaller key sizes compared to RSA, while providing equivalent security. For example, a 256-bit ECC key is considered to provide the same level of security as a 3072-bit RSA key.
- Performance: ECC offers excellent performance characteristics due to its shorter key lengths. It requires fewer computational resources and is suitable for resource-constrained devices and networks.

3. ElGamal: ElGamal is an asymmetric encryption algorithm based on the Diffie-Hellman key exchange protocol. It provides encryption and digital signatures, making it suitable for secure communication and key exchange. Key features of ElGamal include:
   - Security Features: ElGamal provides encryption and digital signatures, ensuring confidentiality and authenticity of data. It can be used for secure communication and key exchange.
   - Key Lengths: ElGamal typically uses longer key lengths compared to RSA and ECC for equivalent security. Commonly used key lengths range from 2048 to 4096 bits.
   - Performance: ElGamal encryption and decryption operations are slower compared to RSA and ECC. It requires more computational resources, especially for longer key lengths.

IV. Digital Signatures

Digital signatures play a significant role in network security by providing authentication, integrity, and non-repudiation of electronic documents, messages, or transactions. A digital signature is a cryptographic mechanism that ensures the authenticity and integrity of data exchanged over a network.

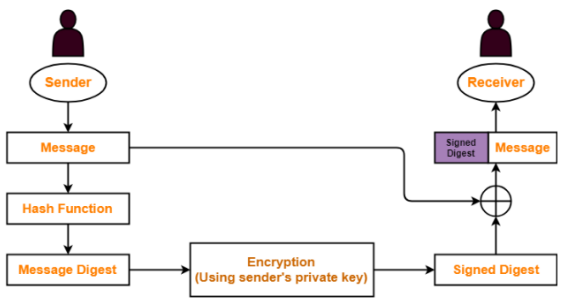

Fig 5. Block Diagram of Digital Signature

Here's an explanation of digital signatures and their significance in network security:

1. Authentication: The digital signature is created using the private key of the sender, which can only be decrypted using the corresponding public key. By verifying the digital signature with the sender's public key, the recipient can be confident that the message or document indeed came from the claimed sender.
2. Integrity: Digital signatures ensure the integrity of data. Any alteration or modification of the signed document or message, even a minor change, will invalidate the digital signature.
3. Non-Repudiation: Digital signatures provide non-repudiation, meaning the signer cannot deny their involvement in creating and sending the signed message or document.
4. Trust and Confidence: Digital signatures establish trust and confidence in electronic transactions and communications. By using digital signatures, parties can securely exchange sensitive information, conduct secure online transactions, and ensure the authenticity and integrity of the exchanged data.
5. Legal Compliance: In many jurisdictions, digital signatures hold legal significance and are recognized as legally binding. Digital signatures can be used as evidence in legal disputes, providing assurance of the authenticity and integrity of electronic records or transactions.
6. Secure Communication Protocols: Protocols, such as SSL/TLS and S/MIME and PGP are those protocols that use digital signatures to authenticate the identity of servers, ensure the integrity of transmitted data, and provide a secure communication channel.

V. Emerging Trends and Challenges

Network security is a rapidly evolving field, and emerging trends have a significant impact on the design and implementation of cryptography schemes. Here are some emerging trends in network security and their influence on cryptography schemes:

1. Quantum Computing: The development of quantum computing poses a potential threat to traditional cryptographic schemes particularly those based on factorization and discrete logarithm problems, which are the foundation of many asymmetric encryption algorithms. Quantum computers have the potential to break these algorithms and render them ineffective. As a result, there is a growing interest in post-quantum cryptography, which involves developing new algorithms that are resistant to quantum

attacks. This trend emphasizes the need to transition to quantum-resistant cryptographic schemes to ensure the long-term security of network communications.

2. Internet of Things (IoT) Security: The proliferation of IoT devices introduces new security challenges due to the large-scale deployment and heterogeneity of devices. IoT devices often have limited resources, making traditional cryptographic schemes less suitable. New lightweight cryptographic algorithms and protocols are being developed to address the resource constraints of IoT devices while maintaining strong security. These schemes focus on achieving efficient encryption, authentication, and secure key management for IoT networks.
3. Homomorphic Encryption: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, providing privacy and security for sensitive information. This emerging trend has the potential to revolutionize secure data processing in scenarios where sensitive data needs to be outsourced to third-party providers or processed in the cloud. Advancements in homomorphic encryption schemes, such as fully homomorphic encryption (FHE) and partially homomorphic encryption (PHE), are opening up new possibilities for secure computation and data privacy.
4. Post-Quantum Cryptography: With the increasing threat of quantum computing, post-quantum cryptography (PQC) is gaining attention as a critical area of research. PQC involves developing cryptographic algorithms that can withstand attacks from both classical and quantum computers. Many new PQC algorithms are being proposed, including lattice-based, code-based, and multivariate polynomial-based schemes. These algorithms aim to provide long-term security even in the presence of powerful quantum computers.
5. Blockchain and Distributed Ledger Technology (DLT): Blockchain and DLT technologies are transforming various industries, including finance, supply chain, and healthcare. Cryptography plays a central role in securing the integrity, confidentiality, and consensus mechanisms of blockchain networks. The design and selection of cryptographic schemes for blockchain applications need to address the specific security requirements of decentralized systems, including robust key management, digital signatures, and secure consensus protocols.
6. Machine Learning and Artificial Intelligence (AI): Machine learning and AI techniques are being leveraged to enhance network security, including threat detection, anomaly detection, and behavior analysis. Cryptography schemes can benefit from integrating AI techniques to improve key management, encryption algorithms, and intrusion detection systems. AI can assist in identifying patterns, predicting attacks, and improving the overall efficiency and effectiveness of cryptographic mechanisms.

VI. Conclusion

This review paper provides a comprehensive analysis of competent cryptography schemes for network security. It serves as a valuable resource for researchers, practitioners, and decision-makers involved in designing, implementing, and managing secure network systems. By evaluating the security features, computational efficiency, scalability, and suitability of various cryptography schemes, this review facilitates informed decision-making in selecting and deploying robust cryptographic techniques to fortify network security in diverse contexts. In summary, the suitability of each cryptography scheme depends on the specific network security scenario and requirements. Understanding their strengths and weaknesses allows for informed decisions in selecting the appropriate scheme to achieve the desired security objectives.

VII. References

[1]. https://nap.nationalacademies.org/read/5131/chapter/6
[2]. https://www.hindawi.com/journals/scn/2017/9036382/
[3]. https://www.informit.com/articles/article.aspx?p=3100069&seqNum=8
[4]. https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.4351
[5]. https://www.researchgate.net/publication/343171240_Secured_cloud_data_migration_technique_by_competent_probabilistic_public_key_encryption
[6]. https://www.mdpi.com/2410-387X/5/4/34
[7]. https://link.springer.com/chapter/10.1007/978-3-642-10433-6_3
[8]. https://www.iso.org/obp/ui/#iso:std:iso-iec:19896:-3:ed-1:v1:en
[9]. https://ieeexplore.ieee.org/document/8229881
[10]. https://www.researchgate.net/publication/347369689_Analysis_of_Cryptography_Encryption_for_Network_Security
[11]. https://www.sciencedirect.com/science/article/abs/pii/S1383762118304077
[12]. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6720296/
[13]. https://www.computer.org/csdl/proceedings-article/icsmdi/2023/648700a110/1NsKjY5c3bq
[14]. https://joint-research-centre.ec.europa.eu/cybersecurity-competence-survey_en