UNDERSTANDING ENCRYPTION: THE FOUNDATION OF DATA PROTECTION

Naga Vinod Duggirala[*1]

[*1]Andhra University, India.

DOI : https://www.doi.org/10.56726/IRJMETS56732

ABSTRACT

This paper tells you everything you need to know about encryption, which is one of the most important technologies for keeping private information safe in the digital world. It talks about the main ideas, methods, and uses of encryption, like symmetric encryption, asymmetric encryption, and hybrid encryption systems. The article talks about the uses of encryption in secure communication, data storage, and other areas and stresses how important it is to handle keys properly. Individuals and businesses can make smart choices about how to protect their data by knowing the basic ideas and best practices behind encryption.

Keywords: Encryption, Symmetric Encryption, Asymmetric Encryption, Hybrid Encryption, Key Management.

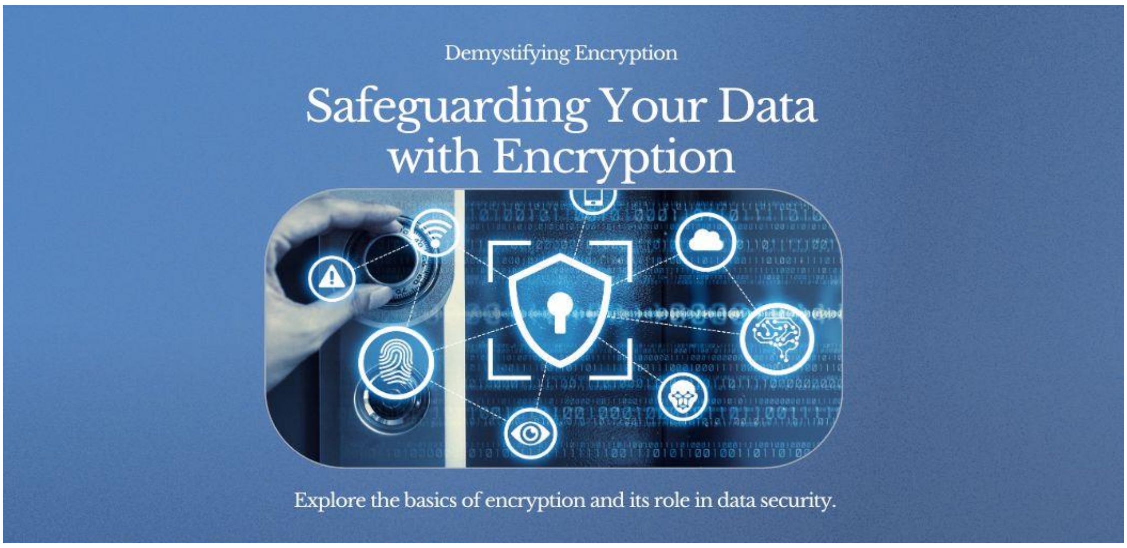
I. INTRODUCTION

Data protection has become very important for everyone in this digital age, including individuals, businesses, and governments. As the amount of digital data being created and kept grows at an exponential rate, strong security measures have never been more important. An International Data Corporation (IDC) study says that by 2025, the world's data will have grown to 175 zettabytes [1]. The main part of data security strategies is encryption, which changes plaintext into ciphertext. It makes sure that personal information stays safe and private, even if someone else gets a hold of it without permission [2].

Cyberattacks are becoming more common and more complex, which shows how important security is. The FBI's Internet Crime Complaint Center (IC3) got more than 791,790 reports of possible Internet crimes in 2020, with losses of more than $4.2 billion [3]. As a first line of defense against these kinds of threats, encryption is an important tool for keeping private data safe in many fields, such as government, healthcare, and finance [4].

It's possible to track the history of encryption all the way back to ancient times when Julius Caesar used the Caesar cipher to keep military communications safe [5]. However, the rise of modern computers has changed cryptography in a big way, leading to the creation of more advanced encryption methods and protocols. Encryption is now commonly used to protect data while it's being sent and while it's being stored, making sure that information is kept private, correct, and real [6].

The goal of this piece is to give a complete introduction to encryption by looking at its basic ideas, key techniques, and real-world uses. By knowing the basic ideas and best practices of encryption, people and businesses can make smart choices about how to protect their data in the digital world.


Demystifying Encryption
Safeguarding Your Data with Encryption
Explore the basics of encryption and its role in data security.

II. SYMMETRIC ENCRYPTION

One key is used to both secure and decrypt data with symmetric encryption, which is also called secret key encryption. Since both the sender and the receiver share the same key, it is very important to keep the key secret. Many people use symmetric encryption methods like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) because they work well and quickly [7]. AES is the most popular symmetric encryption method right now [8]. It was made a standard by the National Institute of Standards and Technology (NIST) in 2001. Keys can be 128, 192, or 256 bits long, and the amount of security changes depending on the key length [9].

One of the best things about symmetric encryption is how quickly it works. Symmetric encryption algorithms are much faster than asymmetric encryption algorithms, which means they can be used to encrypt big amounts of data [10]. One study by Schneier et al. found that AES is around 1,000 times faster than RSA, which is a well-known asymmetric encryption method [11]. This level of speed is very important in situations where data needs to be processed in real-time, like when streaming video or talking on the phone [12].

One problem is that the key exchange method can be hard to do, especially in big systems [13]. Since the same key is used for both encryption and decryption, the people who are talking to each other must share it safely. In situations where the people involved don't trust each other or when they're talking over unprotected lines [14], this can be a problem. Key exchange protocols, like Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH), are used to set up a shared secret key over a path that isn't safe [15].

One more problem with symmetric encryption is that it needs safe ways to keep track of keys. There are an increasing number of keys needed as the number of people talking grows. An example of this is a system with n parties that needs (n(n-1))/2 keys [16]. You may have to deal with more keys and possible security risks if they are not stored and handled properly [17]. Key rotation, safe key storage, and the use of hardware security modules (HSMs) are some of the best ways to reduce these risks [18].

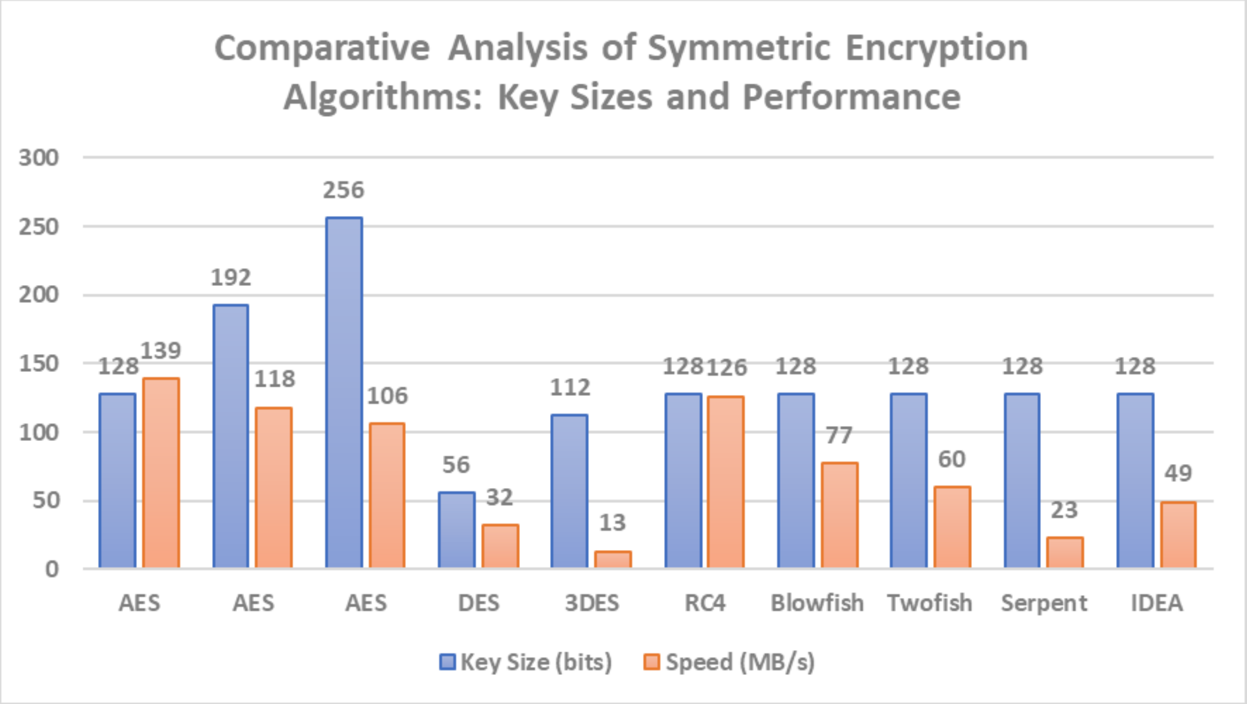


Fig. 1: Benchmarking Symmetric Encryption: A Comprehensive Overview of Algorithm Speeds and Key Lengths [7-18]

III. ASYMMETRIC ENCRYPTION

The key-sharing problem that comes with symmetric encryption is fixed by asymmetric encryption, also known as public key encryption. A set of keys is used: a public key to encrypt and a private key to decrypt it. The owner of the private key has to keep it secret, but anyone can use the public key [19]. With this method, there is no need for a safe channel for exchanging keys because the public key can be shared freely without putting the private key at risk [20].

RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are two examples of asymmetric encryption methods that offer better security but take longer to compute [21]. One of the most popular asymmetric encryption methods is RSA, which is named after the people who came up with it. It rests on the fact that large composite numbers are hard to factor, which means that attackers can't use computers to get the private key from the public key [22]. The amount of security in RSA depends on the size of the key; larger key sizes offer higher levels of protection. RSA key sizes usually fall between 1024 and 4096 bits, with 2048 bits being the bare minimum for safe contact [23].

ECC, on the other hand, is built on how elliptic curves over finite fields are structured algebraically. The amount of security is the same as RSA, but the key sizes are smaller, which makes it better in terms of bandwidth and computing power [24]. One example is that a 256-bit ECC key is just as safe as a 3072-bit RSA key [25]. Because of this, ECC works best on devices with limited resources, like smartphones and IoT (Internet of Things) devices [26].

Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, but they take longer to compute. Indeed, in asymmetric encryption, the steps for encrypting and decrypting can be up to 1,000 times longer than in symmetric encryption [27]. Because it takes longer to run, asymmetric encryption is not as good for encrypting big amounts of data. Most of the time, symmetric encryption is used to encrypt data [28], while asymmetric encryption is used to trade keys and create digital signatures [28].

The public key infrastructure (PKI) must be trustworthy for asymmetric cryptography to work. PKI is a system that makes communication safe by giving a reliable way to check that public keys are real [29]. Digital certificates are used. These are given out by trusted certificate authorities (CAs), and the owners of the public keys are linked to their names [30]. However, the PKI ecosystem has had problems, like bad handling of certificates and attacks on CAs. These problems have led to the creation of new trust models, like blockchain-based PKI [31].

Table 1: Comparison of Key Sizes, Security Levels, and Relative Speeds for RSA, ECC, and Symmetric Encryption Algorithms [19-31]

Encryption Algorithm	Key Size (bits)	Security Level (bits)	Relative Speed
RSA	1024	80	1
RSA	2048	112	0.25
RSA	3072	128	0.1
RSA	4096	140	0.05
ECC	160	80	10
ECC	224	112	8
ECC	256	128	6
ECC	384	192	4
Symmetric (e.g., AES)	128	128	1000

Symmetric (e.g., AES)	256	256	800

IV. HYBRID ENCRYPTION

Most of the time, hybrid encryption methods are used to get the best of both symmetric and asymmetric encryption. As part of a mixed system, asymmetric encryption is used to send a symmetric key safely. The symmetric key is then used to encrypt the data [32]. This method takes the best parts of both symmetric and asymmetric encryption and combines them into a single, well-balanced answer for safe data storage and communication [33].

A lot of different security systems, like Transport Layer Security (TLS) and Pretty Good Privacy (PGP), use hybrid encryption. Both the client and the server use asymmetric encryption to set up a shared secret key during the original handshake process in TLS, which is the basis of HTTPS. The data sent between the client and server is then encrypted in a way that is equal for both sides using this shared key [34]. Google did a study that showed that over 95% of web traffic on Google goods and services is encrypted using HTTPS. This shows how widely hybrid encryption is used to protect online communication [35].

PGP is a standard for encrypting email messages, and it also uses mixed encryption to keep them safe. First, the sender makes a random symmetric key, which is used to encrypt the message. Next, the sender uses the recipient's public key to encrypt the symmetric key. Then, the message and symmetric key are encrypted and sent to the recipient. The receiver uses their private key to decrypt the symmetric key and then the message [36]. Over 90% of targeted attacks use email as their main method, according to a study by Symantec [37]. This shows how important email encryption tools like PGP are for protecting against these kinds of risks.

Hybrid encryption is good for encrypting big amounts of data because it works well, like in cloud storage systems. In these systems, a symmetric key is used to encrypt the data, and the public key of the person who owns the data is used to encrypt the symmetric key itself. This makes it easy to encrypt and decrypt data and keep track of keys safely [38]. MarketsandMarkets says that the global cloud encryption market will grow from USD 1.7 billion in 2020 to USD 4.2 billion by 2025. This is because more people are using cloud services and more people want good data security solutions [39].

However, the safety of hybrid encryption depends on the safety of both the symmetric and asymmetric methods that are used. If one of the methods is broken, the system as a whole is at risk [40]. So, it's important to use encryption methods that have been around for a long time and have been tested a lot. For example, AES is a good choice for symmetric encryption, and RSA or ECC are good choices for asymmetric encryption. Hybrid encryption systems must also be managed properly, with safe key creation, storage, and rotation being some of the most important steps [41].

Table 2: Prevalence of Hybrid Encryption in Various Protocols and Services [32-41]

Protocol/Service	Encryption Scheme	Key Exchange Method	Data Encryption Method
HTTPS (TLS)	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)
PGP (Email)	Hybrid	Asymmetric (RSA)	Symmetric (AES)
Cloud Storage	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)
SSH	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)
VPN (IPsec)	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)
Signal (Messaging)	Hybrid (Double	Asymmetric (X3DH)	Symmetric (AES)

	Ratchet)		
WhatsApp (Messaging)	Hybrid (Double Ratchet)	Asymmetric (X3DH)	Symmetric (AES)
Secure File Transfer (SFTP)	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)
Full Disk Encryption (BitLocker)	Symmetric	N/A	Symmetric (AES)
End-to-End Encrypted Backup	Hybrid	Asymmetric (RSA/ECC)	Symmetric (AES)

V. KEY MANAGEMENT

Key management that works well is essential for keeping secure systems safe. It includes making encrypted keys, giving them out, storing them, and replacing them [42]. Proper key management makes sure that keys are produced safely using trustworthy random number generators, sent safely through encrypted channels, and kept safely [43]. The Ponemon Institute did a study and found that 63% of companies have had a data breach because of bad key management [44]. This shows how important it is to have strong key management practices.

It is called "key generation" to make the cryptographic keys that are used for encryption and decryption. Cryptographically secure random number generators (CSRNGs) must be used to make sure that the keys produced are unpredictable and unique [45]. Some common CSRNGs are the methods suggested by NIST SP 800-90A, like Hash_DRBG, HMAC_DRBG, and CTR_DRBG [46]. There have been a lot of tests and confirmations that these algorithms are safe, and they are used in many industry-standard security systems and programs [47].

Key distribution is the safe sending of keys from one person to another, making sure that the keys are not stolen or changed in transit. Several tools, like secure key sharing protocols (like Diffie-Hellman), public key infrastructure (PKI), and quantum key distribution (QKD) [48], can be used to do this. Quantum Key Distribution (QKD) is a new system that uses quantum mechanics to make key exchange safe over channels that can't be trusted. The European Telecommunications Standards Institute (ETSI) recently did a study that says the global QKD market will reach USD 2.8 billion by 2024 [49]. This is because people will want safe ways to communicate.

Another important part of key management is storing keys. To keep encryption keys safe from theft or illegal access, they need to be kept in places that can't be changed. Hardware security modules, or HSMs, are specialized hardware pieces that are made to store and handle keys safely [50]. When it comes to physical and mental security, HSMs are very good. They keep keys safe even if the system is broken into. A MarketsandMarkets study says that the global HSM market will grow from USD 1.1 billion in 2020 to USD 1.7 billion by 2025 [51]. This is because more people want secure key management solutions and more people are using the cloud.

To keep the security of encrypted data, you must regularly rotate keys and make secure backups of keys. Key rotation means changing encryption keys on a regular basis to lessen the damage that could be done if a key is stolen [52]. By changing keys on a regular basis, businesses can make it less likely that someone will get into protected data without permission, even if a key is stolen. Secure key backup, on the other hand, keeps encryption keys safe and makes sure they can be recovered if something goes wrong or the system crashes [53]. This is usually done with safe backup methods like encrypted files and storage that is not on-site.

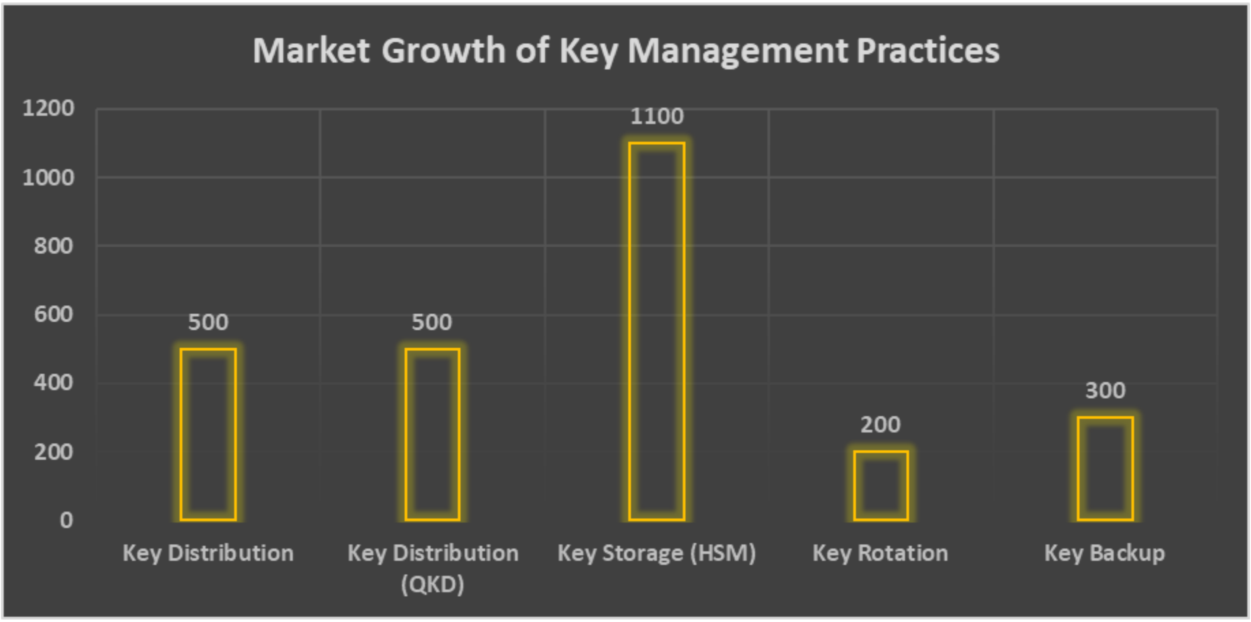


Fig. 2: Comparative Analysis of Key Management Practice Market Sizes and Growth Rates [42-53]

VI. APPLICATIONS OF ENCRYPTION

Encryption has many uses, such as keeping data safe and ensuring secure contact. When you use private communication, encryption keeps the privacy and integrity of data sent over networks like the Internet safe [54]. Statista says that there will be 5.3 billion internet users around the world by 2023. This shows how important it is to have safe ways to communicate [55]. End-to-end encryption is what keeps users' information safe on secure messaging apps like WhatsApp and Signal [56]. Encryption methods like the Signal Protocol protect these platforms from different types of attacks and provide forward secrecy [57]. The Signal Protocol uses the Double Ratchet algorithm, prekeys, and the Diffie-Hellman key exchange.

Another way that encryption is used to keep information safe is in virtual private networks (VPNs). VPNs protect users' internet data from being spied on or changed by creating a secure tunnel between their device and a remote network using encryption [58]. A study by Global Market Insights says that the global VPN market will grow to more than USD 54 billion by 2024 [59]. This is because more people want safe remote access and more people are using cloud-based services.

When you store data, encryption makes sure that private data stays safe even if the storage devices are lost or stolen [60]. This is especially important when it comes to cloud storage, where data is kept on computers in the cloud that are managed by outside companies. The Ponemon Institute did a study and found that 48% of businesses have had a data breach in the cloud [61]. This shows how important encryption is for keeping data safe. To help businesses keep their data safe, cloud storage companies like Amazon Web Services (AWS) and Google Cloud Platform (GCP) offer different types of encryption, such as server-side encryption and client-side encryption [62].

It is also very important to encrypt sensitive data that is kept locally on devices like laptops and smartphones. When you use full disk encryption (FDE), all of the data on a storage device is encrypted. This keeps your data safe even if you lose or steal the device [63]. Transparency Market Research says that the global FDE market will reach USD 1.2 billion by 2027 [64]. This is because more people want to protect their data and more people are using mobile devices.

Encryption is used for more than just safe contact and data storage. It is used in secure payment systems, digital rights management (DRM), and blockchain technology, among other things. Private money details like credit card names and bank account numbers are kept safe in secure payment systems by encrypting them [65]. Encryption is used by DRM systems to stop people from accessing and sharing digital material like movies, music, and software without permission [66]. Cryptocurrencies like Bitcoin and Ethereum are based on blockchain technology, which uses encryption to keep transactions safe and unchangeable [67].

VII. DATA IN MEMORY ENCRYPTION USING CONFIDENTIAL COMPUTE

In any, less trusted or untrusted environments, sensitive data in memory handling in plain text will have the information disclosure risk during the cross-process accesses or the core dump of the applications. Any sensitive data that includes passwords, cryptographic keys, and personal information must be cryptographically protected in memory using Secure Confidential Computing environments such as Intel SGX, and AMD SEV, and when it is operated within the cloud respective confidential computing such as AWS Nitro and Confidential Containers.

VIII. HOMOMORPHIC ENCRYPTION OR SEARCHABLE ENCRYPTION

Data Analytics and data models will demand the data need to be available in plain text for performing the data modeling in which case the data will be at risk of exposure and applications need to leverage the homomorphic encryption techniques to ensure the data gets processed on the encrypted data.

Similarly, the data should be able to be searched without disclosing the sensitive data using various industry-available searchable encryption methods.

IX. CONCLUSION

In the digital world, encryption is a key tool for keeping data safe. Organizations can successfully protect sensitive data by comprehending the basic ideas behind symmetric, asymmetric, and hybrid encryption schemes. To keep encrypted systems safe, the article stresses the value of good key management practices like making, sharing, storing, and rotating keys in a secure way. As the amount of digital data increases and online threats change, encryption is still an important way to protect private data in many areas, such as secure communication, data storage, secure payment systems, digital rights management, and blockchain technology. By following best practices for encryption and keeping up to date on the latest developments in the field, people and businesses can improve the security of their data and lower the risks of data breaches and unauthorized access.

X. REFERENCES

[1] D. Reinsel, J. Gantz, and J. Rydning, "The Digitization of the World: From Edge to Core," IDC White Paper, Nov. 2018, doi: 10.1007/978-3-030-02683-7_1.

[2] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1996.

[3] Federal Bureau of Investigation, "Internet Crime Report 2020," Internet Crime Complaint Center (IC3), 2021, [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[4] R. Chandramouli, S. Chokhani, and M. Baum, "Cryptographic Key Management Issues & Challenges in Cloud Services," NIST Interagency/Internal Report 7956, Sep. 2013, doi: 10.6028/NIST.IR.7956.

[5] D. Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet," Scribner, 1996.

[6] W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson Education, 2017.

[7] W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson Education, 2017.

[8] National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, Nov. 2001.

[9] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Springer, 2002, doi: 10.1007/978-3-662-04722-4.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[11] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions," Proceedings of the 2nd AES Candidate Conference, pp. 15-34, Mar. 1999.

[12] S. Srivastava and S. Yadav, "Analysis and Comparison of Symmetric Key Cryptographic Algorithms," International Journal of Computer Science and Network Security (IJCSNS), vol. 18, no. 1, pp. 43-49, Jan. 2018.

[13] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[14] R. Oppliger, "SSL and TLS: Theory and Practice," Artech House, 2016.

[15] E. Rescorla, "Diffie-Hellman Key Agreement Method," RFC 2631, Jun. 1999, doi: 10.17487/RFC2631.

[16] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications," Springer, 2015, doi: 10.1007/978-3-662-47974-2.

[17] R. Chandramouli, S. Chokhani, and M. Baum, "Cryptographic Key Management Issues & Challenges in Cloud Services," NIST Interagency/Internal Report 7956, Sep. 2013, doi: 10.6028/NIST.IR.7956.

[18] E. Barker, "Recommendation for Key Management: Part 1 - General," NIST Special Publication 800-57 Part 1 Revision 5, May 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[19] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978, doi: 10.1145/359340.359342.

[21] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203-209, Jan. 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[22] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1996.

[23] E. Barker and Q. Dang, "Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance," NIST Special Publication 800-57 Part 3 Revision 1, Jan. 2015, doi: 10.6028/NIST.SP.800-57pt3r1.

[24] V. S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85 Proceedings, Lecture Notes in Computer Science, vol. 218, pp. 417-426, 1986, doi: 10.1007/3-540-39799-X_31.

[25] National Institute of Standards and Technology (NIST), "Recommendation for Key Management: Part 1 - General," NIST Special Publication 800-57 Part 1 Revision 5, May 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[26] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51-58, Sep. 2011, doi: 10.1109/MC.2011.291.

[27] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[28] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications," Springer, 2015, doi: 10.1007/978-3-662-47974-2.

[29] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 2459, Jan. 1999, doi: 10.17487/RFC2459.

[30] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 3647, Nov. 2003, doi: 10.17487/RFC3647.

[31] A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda, and R. State, "A blockchain-based PKI management framework," Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS), pp. 1-6, Apr. 2018, doi: 10.1109/NOMS.2018.8406325.

[32] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications," Springer, 2015, doi: 10.1007/978-3-662-47974-2.

[33] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1996.

[34] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018, doi: 10.17487/RFC8446.

[35] Google, "HTTPS encryption on the web," Google Transparency Report, [Online]. Available: https://transparencyreport.google.com/https/overview.

[36] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," RFC 4880, Nov. 2007, doi: 10.17487/RFC4880.

[37] Symantec, "Internet Security Threat Report, Volume 24," Feb. 2019, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[38] R. Chandramouli, S. Chokhani, and M. Baum, "Cryptographic Key Management Issues & Challenges in Cloud Services," NIST Interagency/Internal Report 7956, Sep. 2013, doi: 10.6028/NIST.IR.7956.

[39] MarketsandMarkets, "Cloud Encryption Market by Component (Solution and Services), Service Model (Infrastructure-as-a-Service, Software-as-a-Service, and Platform-as-a-Service), Organization Size, Vertical, and Region - Global Forecast to 2025," Jul. 2020, [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-encryption-market-227254588.html.

[40] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[41] E. Barker, "Recommendation for Key Management: Part 1 - General," NIST Special Publication 800-57 Part 1 Revision 5, May 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[42] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols," IEEE Transactions on Software Engineering, vol. 22, no. 1, pp. 6-15, Jan. 1996, doi: 10.1109/32.481513.

[43] E. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation," NIST Special Publication 800-133, Dec. 2019, doi: 10.6028/NIST.SP.800-133r2.

[44] Ponemon Institute, "2019 Global Encryption Trends Study," Apr. 2019, [Online]. Available: https://www.ncipher.com/resources/2019-global-encryption-trends-study.

[45] E. Barker and J. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators," NIST Special Publication 800-90A Revision 1, Jun. 2015, doi: 10.6028/NIST.SP.800-90Ar1.

[46] National Institute of Standards and Technology (NIST), "Recommendation for Random Number Generation Using Deterministic Random Bit Generators," NIST Special Publication 800-90A Revision 1, Jun. 2015, doi: 10.6028/NIST.SP.800-90Ar1.

[47] S. Bajaj and R. Sion, "TrustedDB: A Trusted Hardware-Based Database with Privacy and Data Confidentiality," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 3, pp. 752-765, Mar. 2014, doi: 10.1109/TKDE.2013.38.

[48] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications," Springer, 2015, doi: 10.1007/978-3-662-47974-2.

[49] European Telecommunications Standards Institute (ETSI), "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI White Paper No. 8, Jun. 2015, [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[50] R. Chandramouli, S. Chokhani, and M. Baum, "Cryptographic Key Management Issues & Challenges in Cloud Services," NIST Interagency/Internal Report 7956, Sep. 2013, doi: 10.6028/NIST.IR.7956.

[51] MarketsandMarkets, "Hardware Security Modules Market by Deployment Type (On-premises and Cloud-based), Type (LAN Based/Network Attached and PCI Based/USB Based), Applications (Authentication, Database Encryption, Document Signing, and Secure Sockets Layer), Vertical, and Region - Global Forecast to 2025," Aug. 2020, [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/hardware-security-modules-market-175567556.html.

[52] E. Barker, "Recommendation for Key Management: Part 1 - General," NIST Special Publication 800-57 Part 1 Revision 5, May 2020, doi: 10.6028/NIST.SP.800-57pt1r5.

[53] E. Barker, "Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations," NIST Special Publication 800-57 Part 2, Jan. 2019, doi: 10.6028/NIST.SP.800-57pt2r1.

[54] R. Oppliger, "SSL and TLS: Theory and Practice," Artech House, 2016.

[55] Statista, "Global digital population as of January 2021," Jan. 2021, [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[56] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," RFC 4880, Nov. 2007, doi: 10.17487/RFC4880.

[57] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A Formal Security Analysis of the Signal Messaging Protocol," Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 451-466, Apr. 2017, doi: 10.1109/EuroSP.2017.27.

[58] S. Frankel and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, Feb. 2011, doi: 10.17487/RFC6071.

[59] Global Market Insights, "VPN Market Size By Component, By Type, By Deployment Model, By Application, By End-Use, Industry Analysis Report, Regional Outlook, Growth Potential, Competitive Market Share & Forecast, 2018 - 2024," Feb. 2019, [Online]. Available: https://www.gminsights.com/industry-analysis/virtual-private-network-VPN-market.

[60] M. Blaze, "A cryptographic file system for UNIX," Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS '93), pp. 9-16, Nov. 1993, doi: 10.1145/168588.168590.

[61] Ponemon Institute, "2020 Cost of a Data Breach Report," Jul. 2020, [Online]. Available: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[62] Amazon Web Services (AWS), "AWS Key Management Service (KMS)," [Online]. Available: https://aws.amazon.com/kms/.

[63] E. Barker, "Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations," NIST Special Publication 800-57 Part 2, Jan. 2019, doi: 10.6028/NIST.SP.800-57pt2r1.

[64] Transparency Market Research, "Full Disk Encryption Market - Global Industry Analysis, Size, Share, Growth, Trends, and Forecast, 2019-2027," Mar. 2020, [Online]. Available: https://www.transparencymarketresearch.com/full-disk-encryption-market.html.

[65] Payment Card Industry (PCI) Security Standards Council, "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1," May 2018, [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

[66] A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," Signal Processing: Image Communication, vol. 16, no. 7, pp. 681-699, Apr. 2001, doi: 10.1016/S0923-5965(01)00004-1.

[67] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Oct. 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf.