International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 07 | July - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Secure Data Transmission Using Different Cryptography Algorithms

Ms. Harpreet Kaur[1], Ms. Mandeep Kaur[2], Ms. Sukhwinder Kaur [3] Ms. Pooja [4]

[1]Ms.Harpreet Kaur UCCA & Guru Kashi University
[2]Ms.Mandeep Kaur UCCA & Guru Kashi University
[3]Ms.Sukhwinder Kaur UCCA & Guru Kashi University
[4]Ms.Pooja UCCA & Guru Kashi University

Abstract - Data security has emerged as a major worry for everyone using the internet as it has merged with our lives and grown explosively over the past few decades. Data security ensures that only the intended recipient has access to our data and prohibits any modification or change of the data. Many techniques and procedures have been developed in order to reach this level of security. The term "cryptography" refers to procedures that cipher data using particular algorithms, rendering it unintelligible to the human eye until it is decoded using algorithms that have been set by the sender.

***Key Words*:** Cryptography, Security, Algorithm, Cipher, Decryption, Data Security.

1. INTRODUCTION

A method to ensure message confidentiality is cryptography. Greek speakers understand the phrase to imply "secret writing" specifically. However, today's high-level encryption ensures that information delivered is safe in a way that only the authorised recipient can access this information [1], protecting the privacy of people and organisations. Cryptography can be viewed as an ancient method that is continually being improved upon because of its historical roots. Examples date as far back as 2000 B.C., when the ancient Egyptians employed "secret" hieroglyphics. Other examples include obscure texts from ancient Greece or the renowned Caesar cypher from ancient Rome [2].

Every day, millions of people use cryptography to protect their data and information around the world.

2. LITERATURE REVIEW

According to Susan et al. [4], network and computer security is a young and developing discipline of computer science, and teaching computer security is like shooting at a moving target. The primary emphasis of security courses is on algorithmic and mathematical concepts, such as hashing methods and encryption. New courses are developed that address the most recent types of assaults as crackers discover new ways to compromise network systems, however each of these attacks becomes old daily owing to the reactions from new security software. As security language continues to mature, security practises and abilities are developing in the fields of business, network optimisation, security architecture, and legal basis.

The fundamental principles, traits, and objectives of cryptography were illustrated by Othman O. Khalifa et al. [5].

They talked about how communication plays a significant part in our time—the age of information—in the development of technology and how sending data through the medium of communication necessitates privacy protection and assurance.

Data security is given top attention when utilising encryption techniques to ensure that data reaches the intended users safely and without being compromised, according to Nitin Jirwan et al. [6]. Data communication is described as relying mostly on digital data transfer. They also illustrated the various symmetric and asymmetric cryptography algorithms that are employed in the transmission of data.

Sandeep Tayal et al. [7] noted in a review on network security and cryptography that organisations all over the world produce enormous amounts of data every day as a result of the rise of social networks and commerce apps. Due to this, information security becomes a major concern in terms of protecting the security of data transit through the internet. This problem highlights the need for cryptographic methods even more as more people connect to the internet. An overview of the many security-enhancing methods employed by networks, including cryptography, is given in this study.

Anjula Gupta et al.'s [8] presentation of the history and significance of cryptography as well as how information security has developed into a difficult problem in the computer and communications areas [8] were both highlights. This paper provides various asymmetric algorithms that have enabled us to protect and secure data, in addition to showing how cryptography can be used to ensure identification, availability, integrity, authentication, and confidentiality of users and their data.

Cryptography, privacy-enhancing technology, legislative developments affecting cryptography, dependability, and privacy-enhancing technologies were all mentioned in a research by Callas, J. [9]. He pointed out that the future of cryptography will depend on how society employs it, which depends on rules, existing laws, and practices, as well as what society wants it to do. He

stated that there are numerous gaps in the realm of cryptography that need to be filled by upcoming researchers. Additionally, a management system that generates strong keys is essential to the future of cryptography in order to guarantee that only authorised users with authorised keys can access data and that unauthorised users cannot. Last but not least, Callas stated that individuals' perceptions and ideas regarding security and communication privacy.
Cryptography will so continue to be important for the protection of data and information both today and in the future.

Moving on to the objectives of cryptography, James L. Massey [10] noted that there are now two objectives that cryptography seeks to fulfil: authenticity and/or secrecy. He explored both Shannon's theory of theoretical secrecy and Simmon's notion of theoretical authenticity in terms of the security it provides (which can be either practical or theoretical).

Finally, Schneier [11] came to the conclusion that security secrecy is not a good thing and that it is bad for security to be hidden because security that only depends on secrecy can be weak. It would be impossible to regain that secret if it was lost. Schneier went on to say that in order to provide effective security, cryptography based on brief secret keys that are simple to transfer and alter must adhere to a fundamental concept, according to which the cryptographic algorithms must be both powerful and well known. Accepting public scrutiny is the only surefire method to continue to improve security.

N. Varol et al.'s research on symmetric encryption, which is used to encrypt specific texts and spoken language, was published in Varol et al. In this work, the content that has to be encrypted is first transformed into an encapsulation chipher that a cypher algorithm cannot decipher.
In their study of secure sharing using cryptography in cloud computing, Chachapara, K. et al. [13] showed a framework that uses cryptography algorithms like RSA and AES, with AES being the most secure algorithm in the field. Users of the cloud can create keys for various users with various access rights to their content.

As the author stated, hash functions play a crucial role in cryptography by providing nearly any piece of data with a number. As a result, Orman, H. [14] mentioned that many discussions and developments are generated about hash functions. When MD5's flaws were discovered, this created uncertainty about how to design hash functions.

In his discussion of randomness in cryptography, Gennaro, R. [15] defined a random process as one with unpredictable results and noted that this is why randomness is important in cryptography since it offers a mechanism to generate information that an adversary cannot discover or predict.

In the post-Snowden era, Preneel, B. [16] presented cryptography and information security. He covered mass surveillance techniques, the security of ICT systems, and well-known ways that skilled attackers can get around or destroy cryptography.

As well as pointing out the current status of the Arabic industrial and academic efforts in this field in the past that are related to the existing cryptographic and search for new evaluation methods for the security of information, Sadkhan, S. B. [17] highlighted the main processes and trends of the fields in cryptography from the time of Julius Cesar to the modern era.

3. CRYPTOGRAPHY CONCEPT

A cryptographic system's fundamental idea is to cipher data or information in order to achieve secrecy of the information in a way that prevents an unauthorized person from deducing its meaning. The two most frequent uses of cryptography are to transfer data over an insecure network, like the internet, or to prevent unauthorised users from understanding what they are looking at after they have gained access to the material.
The masked data is typically referred to as "plaintext" in cryptography, and the method of hiding it is called "encryption"; the plaintext that has been encrypted is called "cypher text." A set of guidelines referred to as "encryption algorithms" enable this operation. Standard encryption

Fig. 1. Cryptography concept

4. HISTORICAL ALGORITHMS

A few historical algorithms will be explained in this section, along with examples for a non-mathematical reader using pencil and paper. Long before the idea of using public key cryptography, these techniques were developed and put to use.

A. Caesar Cipher

The Roman ruler Julius Caesar developed this as one of the earliest and most historic uses of encryption during the Gallic Wars. The letters that appear three positions before each letter in the alphabet are used to represent the letters A through We in this sort of algorithm, while

the remaining letters A, B, and C are represented by X, Y, and Z. This indicates that a "shift" of 3 is used, while we could also get a similar result on the encrypted text by using any value between 1 and 25. As a result, a shift is now frequently thought of as a Caesar Cypher [18].

As the Caesar cipher is one of the simplest examples of cryptography, it is simple to break. In order for the cipher text to be decrypted, the letters that were shifted get shifted three letters back to their previous positions. Despite this weakness, it might been strong enough in historical times when Julius Caesar used it during his wars. Although, as the shifted letter in the Caesar Cipher is always three, anyone trying to decrypt the cipher text has only to shift the letters to decrypt it [19].

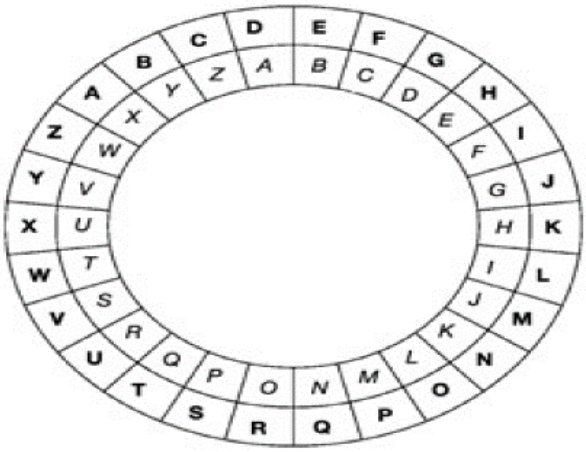

Fig. 2. Caesar Cipher encryption wheel

B. Simple Substitution Ciphers

Consider the Monoalphabetic Cypher, often known as the Simple Substitutions Cypher. In a simple substitution cypher, the letters of the alphabet are placed beneath the correctly spelled alphabet in random sequence, as shown here:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

The same key is utilised during both encryption and decryption. "Each letter gets replaced by the letter beneath it" is the rule of encryption in this case, while the rule of decryption would be the inverse. For example, QDN [18] is the appropriate cypher text for the plaintext CAN.

C. Transposition Ciphers

Other cypher families function by employing a key and a specific rule to arrange the letters of the plaintext to convert it to cypher text. Transposition is the process of changing the plaintext letters using rules and a unique key. One of the simplest types of transposition cyphers is the "complete columnar transposition" cypher, which has two variations: "incomplete columnar" and "complete columnar transposition." Whichever form is chosen, the written plaintext is represented horizontally by a rectangle whose width should match the length of the key being used. As many rows as are required to write the message may exist. Full columnar transposition is employed, and the plaintext

s e c o n d
d i v i s o
n a d v a n
c i n g t o
n i g h t x

Then, based on the key, the cipher text is produced from the columns. If the key in this example was "321654", the cipher text would be as follows:

cvdng eiaii sdncn donox nsatt oivgh

However, since the columns for an incomplete columnar transposition cypher do not need to be fully filled out, the null letters are omitted. The ciphertext may be more challenging to read without the key as a result of the length variations created by this [20].

IV. MODERN ALGORITHMS

A. Stream cipher

The plaintext is encrypted by XORing the plaintext and the pseudorandom bits, which are used by stream cyphers to generate pseudorandom bits from the key. In the past, stream cyphers were occasionally avoided because they were more likely than block cyphers to be cracked. However, the stream cypher is now more secure and can be depended upon to be used in connections, Bluetooth, communications, mobile 4G, TLS connections, and other applications after years of refining designs.

Each bit is separately encrypted in a stream cypher. There are two different kinds of stream cyphers: the synchronous stream cypher and the asynchronous stream cypher. In the former, the key stream depends on the key, whereas in the latter, the cypher text depends on the key stream.

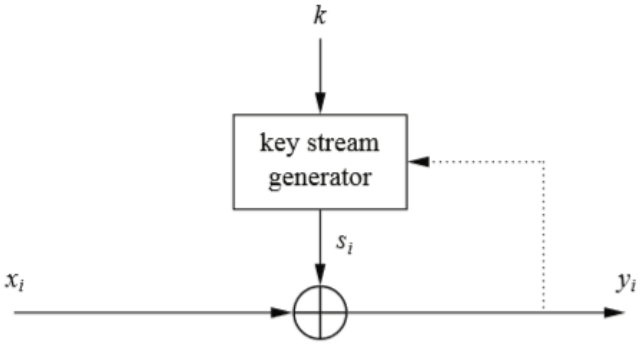

Fig. 3. Asynchronous and synchronous types of stream ciphers

B. Block cipher:

This kind of cipher includes both an encryption algorithm and a decryption algorithm:

• A block of plaintext (P) and an encryption method (E) are each given a key (K), and the resultant, C, is made up of a block of ciphertext. The encryption process is denoted by the equation C = E (K, P).

• The decryption algorithm (D) reverses the preceding procedure, which involved decrypting the cipher text for the plaintext, P. The formula is: P = D (K, C).

The block cipher is strengthened by using a pseudorandom permutation (PRP). In other words, if the key is maintained a secret, a hacker won't be able to decrypt the block cipher and compute the output from any input. This is provided that K's secrecy and randomness are guaranteed from the attacker's point of view. This basically means that an attacker would be unable to discern any patterns in the values entered into or output from the block cipher.

Two values are often mentioned in a block cipher: the block size and the key size. The value of both is crucial to the security. A 64-bit block or a 128-bit block are commonly used in block ciphers. The blocks must not be too big, so the memory footprint and cipher text length are both minimal. Block ciphers process blocks rather than bits when it comes to cipher text length. In other words, in order to encrypt a 16-bit message and 128-bit blocks, the message must first be translated to 128-bit blocks. Only then can the block cipher begin processing and produce a 128-bit cipher text.

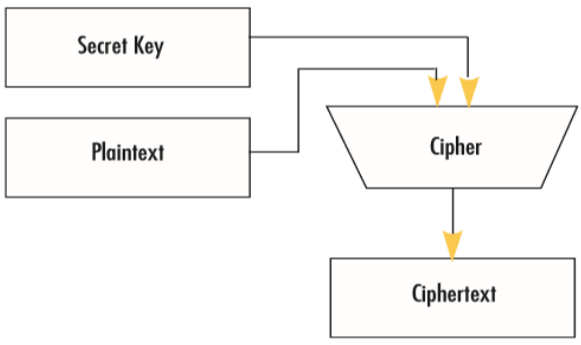

Fig. 4. Block cipher diagram

C. Hash functions:

Previously known as pseudo random functions (PRF), they operate through a technique called compression that maps an input of any size to an output of a specific size. However, this is not the same compression seen in.zip or.rar files. Instead, it is a non-invertible mapping.

• The first property of a hash function is that it must be one-way

• The second property is that it must be collision-resistant in order to be effective.

A key feature of a hash function is that it implies a one-way output and is collision resistant, meaning it would be difficult to find another input that would produce the same output (a collision). There are two types of collision resistance that can be used:

1. Preimage collision resistance: This type of hash function works with an output Y that is obtained by locating another input M in a way that ensures M's hash is, nontrivially, identical to Y's.

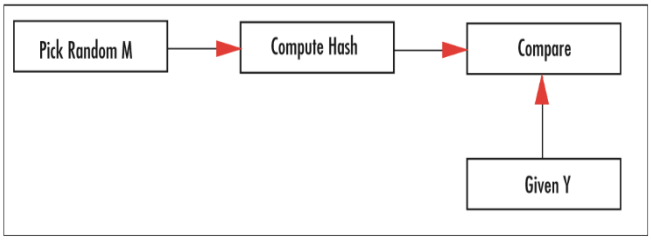

Fig. 5. Preimage collision resistance

2. 2. Second preimage collision resistance: This is the second type of hash function in which two messages (M1 and another, M2 that is selected at random) are provided and the match is nontrivial [21].

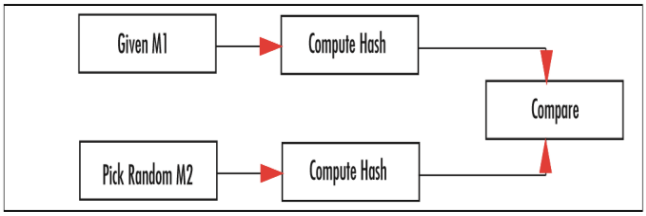

Fig. 6. Second preimage collision resistance

D. Public key systems:

A revolution in cryptography was brought about by the development of public key encryption. It is clear that generic cryptography and encryption were only used in the military and intelligence sectors even during the 1970s and 1980s. Cryptography only became widespread in other fields thanks to public key infrastructure and methodologies.
Since the public key can be made public without any concern, public key encryption enables communication without the need for private channels. Here is a list of the public key's attributes:

1) Key distribution is permitted over public channels with the use of public key encryption, potentially simplifying the initial deployment of the system and making it easier to maintain the system when parties join or leave.

2) The requirement for storing numerous secret keys is reduced by public key encryption. Each participant can utilise a safe method to store their own private key, even in a scenario where all parties desire the capacity to initiate secure communication. The public keys of third parties may be obtained when necessary or kept in an unsecured manner.
3) Public key cryptography is more appropriate in open contexts, particularly when parties that have never interacted before want to communicate and engage safely. For instance, a retailer might be able to publish their public key online, and anyone looking to make a purchase could use that public key to encrypt their credit card information as needed [3].

V. DIGITAL SIGNATURES

Digital signatures, in contrast to cryptography, did not exist before the development of computers. With the advent of computer communications, the necessity for digital signatures to be discussed arose, particularly in business settings where numerous parties are involved and each must agree to uphold their declarations and/or proposals. Although those were handwritten signatures, the subject of unforgeable signatures was first considered millennia ago. Digital signatures were initially discussed in a work titled "New Directions in Cryptography" by Diffie and Hellman [22].
Therefore, authentication by itself cannot bridge the confidence gap between a sender and a receiver in a given context. In a manner analogous to the handwritten signature, something additional—the digital signature—is necessary [23].

A. Digital Signature Requirements:

The "digitalization" period that we are presently experiencing and living in gave rise to the interaction that established the connection between signature and encryption. An unforgeable signature schema would need to meet the following criteria:

• Every user should be able to create their own signature on any document of their choosing.
• Every user should be able to quickly determine whether a given string is the signature of a specific user.
• No one should be able to produce signatures on paperwork that the original owner did not sign [24].

B. Digital Signature Principles:

Both inside and beyond the digital domain, it is crucial to be able to demonstrate who created a communication. This is accomplished in the modern world by using handwritten signatures. Public-key cryptography is used to create digital signatures, and its fundamental tenet is that although the person signing a message or document uses a private key (referred to as a private-key), the person receiving the message or document must use the corresponding public-key. Figure 7 illustrates the digital signature scheme's fundamental workings.

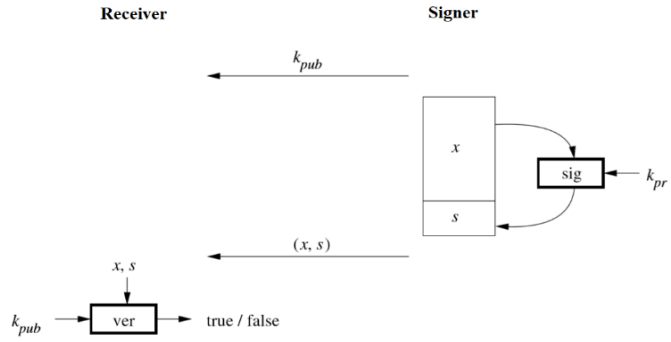

Fig. 7. Digital signature principle (signing and verifying)

The signer of the message x initiates this process by signing it. With the understanding that the signer will keep the private key a secret, the algorithm employed in the signing process is a function that is part of the signer's private key (kpr). As a result, since the message x is also sent to the signature algorithm as input, a relationship between the message x and the signature method can be established. The message is signed, the signature is added, and the message and signature are sent as a pair, (x, s), to the recipient. A digital signature must be attached to a specific message in order to be used, just like a handwritten signature must be placed on a cheque or other legal document.

The digital signature itself has a significant integer value, such as a 2048-bit string. A verification function that accepts both the message x and the signature s as inputs is required in order to verify the signature. The verification function will return "true" or "false" depending on whether it was able to connect the signature to the sender who signed it using a public key. If the message x was signed using the private key that is linked to the other key, i.e. the public verification key, the output would be true. If not, the verification function's output would be false [2].

C. Difference between Digital Signature and Message Authentication:

It may be desirable for parties interacting over an insecure channel to include authentication in the messages they transmit to the recipient so that the recipient can determine if the message is valid or has been altered. When a message is transmitted, an authentication tag is generated; the recipients must check it after receiving the message to make sure that no external attacker is able to create authentication tags that are not being utilized by the communicating parties.
Although there are some similarities between message authentication and digital signature, message authentication differs from digital signature in that only the second party is necessary to verify the message.

There is no way for a third party to confirm the message's authenticity or whether the real sender was behind its creation or not. However, using a digital signature, a third party can verify the signature's legitimacy. As a result, message authentication has a solution thanks to digital signatures [24].

VI. CONCLUSION

The basic objectives of security goals, such as authentication, integrity, confidentiality, and no-repudiation, are achieved in large part thanks to cryptography. These objectives are pursued through the development of cryptographic algorithms. The crucial function of cryptography is to offer trustworthy, solid, and dependable network and data security. We reviewed some of the research in the field of cryptography in this paper, as well as the operation of the many cryptographic algorithms used for diverse security objectives. In order to preserve and provide a decent level of privacy for personal, financial, medical, and e-commerce data, cryptography will continue to be integrated into business and IT strategies.

REFERENCES

[1] N. Sharma , Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.
[2] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[3] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC , 2008.
[4] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.
[5] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.
[6] N. Jirwan, A. Singh and S. Vijay , "Review and Analysis of Cryptography Techniques," International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013 .
[7] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763-770, 2017.
[8] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.
[9] J. Callas, "The Future of Cryptography," Information Systems Security, vol. 16, no. 1, pp. 15-22, 2007.
[10] J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986.
[11] B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10, pp. 120-120, 2004.
[12] N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targetting Android Cellphones," in The 5th International Symposium on Digital Forensics and Security (ISDFS 2017), Tirgu Mures, 2017.
[13] K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud," in 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2013.
[14] H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing, vol. 18, no. 1, pp. 82-86, 2014.
[15] R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006.
[16] B. Preneel, "Cryptography and Information Security in the Post-Snowden Era," in IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, Florence, 2015.
[17] S. B. Sadkhan, "Cryptography : current status and future trends," in International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, 2004.
[18] F. Piper and S. Murphy, Cryptography: A Very Short Introduction, London: Oxford University Press, 2002.
[19] J. P. Aumasson, SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption, San Francisco: No Starch Press, Inc, 2018 .
[20] J. F. Dooley, A Brief History of Cryptology and Cryptographic Algorithms, New York: Springer, 2013.
[21] T. S. Denis and S. Johnson, Cryptography for Developers, Boston: Syngress Publishing Inc, 2007 .
[22] W. D. A. M. E. HELLMAN, "New directions in cryptography," IEEE Transactions on Information Theory, Vols. IT-22, no. 6, pp. 644-654, 1976.
[23] W. Stallings, Cryptography and Network Security Principles and Practices, New York: Prentice Hall, 2005.
[24] O. Goldreich, Foundations of Cryptography Basic Tools, Cambridge: Cambridge University Press, 2004.
View publication