Cryptography and Security Fundamentals

(Protecting Data in the Digital Age)

FEBIA THOMAS

This Page Intentionally Left Blank

Cryptography and Security Fundamentals

FEBIA THOMAS

www.jpc.in.net

Cryptography and Security Fundamentals

Author:
Febia Thomas

First Published: January 2024

ISBN: 978-93-91303-99-0

DOI: https://doi.org/10.47715/JPC.B.978-93-91303-99-0

Pages: 160 (Front pages 14 & Inner pages 146)

Price: 350/-

Publisher
Jupiter Publications Consortium
Chennai, Tamil Nadu
www.jpc.in.net

Imprint:
Magestic Technology Solutions (P) Ltd
Chennai. Tamil Nadu, India.
www.magesticts.com

TITLE VERSO

Title of the Book:
Cryptography and Security Fundamentals

Author's Name:
Febia Thomas

Published By:
Jupiter Publications Consortium
Publisher's Address:
22/102, Second Street, Venkatesa Nagar
Virugambakkam, Chennai 600 092.
Tamil Nadu

Printer's Details:
Magestic Technology Solutions (P) Ltd.

Edition Details: First Edition

ISBN: 978-93-91303-99-0

COPYRIGHT

Jupiter Publications Consortium
22/102, Second Street, Virugambakkam
Chennai 600 092. Tamil Nadu. India

Imprint Magestic Technology Solutions (P) Ltd

Printed on acid-free paper
International Standard Book Number (ISBN): 978-93-91303-99-0Paperback)
Digital Object Identifier (DOI): 10.47715/JPC.B.978-93-91303-99-0

Visit the Jupiter Publications Consortium Web site at
http://www.jpc.in.net

DEDICATION

This book is dedicated to my grandparents, who have always been my source of inspiration and support. Their unwavering love and encouragement have helped me pursue my passion for technology and knowledge.

I would also like to thank my father, who instilled in me a love for learning and a strong work ethic. He taught me the value of perseverance and determination, which have been instrumental in shaping my career.

To my mother, who has been my rock and my biggest cheerleader, thank you for always believing in me and for being my constant source of strength. Your unwavering support and encouragement have helped me overcome countless obstacles and challenges.

Last but not least, I would like to thank my sister, who has always been my best friend and confidant. Your support and encouragement throughout the writing process have been invaluable, and I could not have done this without you.

Thank you all for your love, support, and guidance. This book is a testament to your unwavering belief in me, and I hope to continue making you proud.

With all my love and gratitude,

Febia Thomas
Author

This Page Intentionally Left Blank

FOREWORD

In today's digital age, the importance of cryptography and security cannot be overstated. With the rise of cybercrime and the increasing vulnerability of digital systems, it has become more important than ever to protect our sensitive data and information. This book, Cryptography and Security Fundamentals, is a comprehensive guide to understanding the principles and techniques of cryptography and security. It is written by an expert in the field who has dedicated years to researching and developing cutting-edge solutions for securing digital information.

The author's expertise and passion for the subject matter are evident throughout the book, making it an invaluable resource for anyone seeking to understand the intricacies of cryptography and security. The book covers a wide range of topics, from the basics of cryptography to advanced techniques such as public key cryptography and digital signatures. What sets this book apart is its accessibility. The author has a talent for explaining complex concepts in a clear and concise manner, making it easy for readers of all levels to understand. The book is also filled with real-world examples and case studies, which bring the concepts to life and show their practical applications.

Whether you are a student of computer science, a cybersecurity professional, or simply someone interested in the field, Cryptography and Security Fundamentals is a must-read. It is a testament to the author's dedication to the field and his commitment to making the world a safer place. I highly recommend this book to anyone seeking to deepen their understanding of cryptography and security. It is an inspiring and invaluable resource that will undoubtedly have a profound impact on the field for years to come.

Mr. Shibu Thomas
Senior General Manager
ITC Infotech, Chennai

This Page Intentionally Left Blank

PREFACE

The world today is driven by data and the transfer of information. In this era, the safety of our data has become a paramount concern. The exponential growth of the internet has brought about the increased possibility of cyber-attacks, leading to data breaches, loss of confidential information, and compromised systems. Therefore, it is essential to have a comprehensive understanding of Cryptography and Security Fundamentals to secure our data and protect it from unauthorized access.

This book aims to provide the reader with an in-depth understanding of information and network security, security attacks, and the importance of security. It explores various security services, components, and policies that safeguard our data, and delves into modern cryptographic techniques and their applications in real life.

The book starts by outlining the challenges of security and the various security attacks that can occur, both passive and active. It highlights the need for security measures, and the consequences of not implementing them. The second section covers various security policies, including virus and spyware protection, firewall policy, and access control mechanisms.

The third section focuses on Cryptography, exploring classical and modern cryptographic techniques, including symmetric-key cryptography, stream ciphers, and Feistel-Block Ciphers. It also looks at the application of cryptography in real-life scenarios such as authentication, digital signatures, electronic money, and encryption in emails, WhatsApp, and Instagram.

The book is designed to provide readers with a strong foundation in Cryptography and Security Fundamentals. The examples and programs in the book are written in Python, making it easy for readers to understand and implement. The book is ideal for students, researchers, and professionals in the field of Computer Science and Information Technology, as well as anyone interested in understanding how cryptography and security fundamentals work.

I hope this book will be an essential guide in understanding Cryptography and Security Fundamentals and provide valuable insight into how to protect our data in today's digital world.

Author:

Febia Thomas

ABSTRACT

The field of cryptography and security has become increasingly important in our modern digital age. This book provides an introduction to information and network security, addressing the challenges and risks associated with security attacks. The various types of security attacks are discussed, including passive attacks, active attacks, and malware, along with their potential consequences. The importance of security is emphasized, as is the need for security measures in a variety of settings. The book also explores the components and policies necessary for effective security, including confidentiality, integrity, and access control. Finally, the book covers the basics of cryptography, including classical and modern techniques, symmetric-key cryptography, and public-key cryptography. Real-world applications of cryptography, including authentication, digital signatures, and encryption, are also discussed. This book serves as a valuable resource for anyone interested in the fundamentals of cryptography and security.

Keywords: Cryptography, Security fundamentals, Confidentiality services, Integrity services, Email security, Access control mechanism, Modern cryptographic techniques, Symmetric-key cryptography, Feistel block ciphers, Authentication, Digital signatures

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

1

INTRODUCTION TO INFORMATION AND NETWORK SECURITY

This Page Intentionally Left Blank

Chapter-1

1.0 Introduction to Information and Network Security

Computer data frequently leaves the security of its physical surroundings and moves from one computer to another. It is possible for anyone with malicious intent to alter or fabricate your data once it is out of your control. Thanks to cryptography, it is possible to reformat and alter our data, making it more secure as it moves between computers. Technology is built on the fundamentals of secret codes and advanced mathematics to safeguard our data effectively.

In computer security, the term refers to tools meant to safeguard data and frustrate hackers. Security methods that secure data as it transmits through a network are called network security. Data protection during transmission through interconnected networks is known as internet security. The manager in charge of security requires a systematic manner to define security requirements and characterise approaches to meet those criteria to analyse a business's security demands properly. One method is to consider the three aspects of information security [1].

A security attack is any activity that risks the confidentiality or integrity of the information that belongs to a company. A security

mechanism is a tool for detecting, preventing or recovering from an attack on one's system's security [2].

Information security services a service that strengthens the protection of an organization's computer systems and data flows. In order to deliver the service, the services use one or more security procedures to counter security attacks [1].

Network and Internet security entail procedures to dissuade, prevent, detect, and repair transmission-based security infractions.

The NIST Computer Security Handbook [NIST95] defines computer security as follows: "Computer Security: The protection afforded to an automated information system in order to preserve the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) [3]."

This definition outlines the fundamental goals at the core of computer security:

The confidentiality of information: This word encompasses two related ideas:

Data confidentiality: Ensures that private or personal information is not shared or made accessible to unauthorised parties.

Privacy: This assures that people control or influence what information about them can be gathered, held, and revealed, and by whom and to whom.

Integrity: This word encompasses two related concepts:

Data integrity: Ensures that information is stored or transmitted packets and programs are modified only according to a predetermined and approved method.

System integrity: Ensures that a system executes its intended purpose in an unimpaired way, unaffected by intentional or accidental unauthorised tampering.

Availability: Ensures that systems function efficiently and that authorised users are not denied service.

Authenticity: The quality of being authentic and verifiable; faith in the legitimacy of a transmission, message, or message source. This

involves confirming that users are whom they claim to be and that each input to the system originated from a reliable source.

Accountability: The security objective necessitates that an entity's acts be uniquely traceable to that entity. This facilitates nonrepudiation, deterrent, fault isolation, intrusion detection and prevention, post-action recovery and legal action. Because secure systems are not yet attainable, we must be able to identify the entity responsible for a security violation. Systems must maintain their activity logs so that forensic analysis may be used to trace security breaches and help in transaction disputes.

1.1 The Challenges of Security

The security of the computer and network is both intriguing and intricate.

The challenges are:

Security is not as straightforward as it may initially look to a newbie. Most of the essential aspects of security services can be summed up in a single word: confidentiality, authentication, non-repudiation, and integrity. However, the techniques to achieve these needs can be complicated, and comprehending them may necessitate quite nuanced thought [4].

When designing a specific security system or algorithm, one must constantly consider the possibility of an attack on such security characteristics. Effective attacks are often conceived by examining the problem from an entirely different perspective, exploiting an unanticipated system flaw.

Due to point 2, the processes utilized to supply certain services are frequently paradoxical. Usually, a security mechanism is intricate, and it is not evident from a requirement stating that such comprehensive safeguards are required. When all the dangerous components are considered, expensive security procedures make sense [5].

After designing many security procedures, it is crucial to determine where to implement them. This is valid regarding physical placement (e.g., at what points in the network particular security

measures are required) and logical placement (e.g., at what layer or levels of architecture such as TCP/IP should mechanisms be put) [1].

Typically, security techniques require more than a single algorithm or protocol. They also need that participants hold secret information (such as an encryption key), which creates problems around the development, distribution, and protection of this secret information. There may also be a dependency on communications protocols, the behaviour of which might complicate the process of building the security mechanism. If, for instance, the correct operation of the security mechanism entails setting time restrictions on the transit time of a message from sender to recipient, then any protocol or network that includes variable, unexpected delays may render such time limits ineffective [6].

The effectiveness of a security mechanism that relies on time restrictions for message transit can be severely compromised by network and protocol issues that cause delays or disruptions. Such issues may lead to messages not being delivered within the specified time frames, making the security mechanism ineffective in preventing unauthorized access or data breaches. Ensuring that the network and protocols used are designed to minimize delays and disruptions is essential to mitigate this risk. This can be achieved through the use of reliable, high-performance network infrastructure and standardized protocols that are optimized for secure communication. Additionally, monitoring tools can detect any delays or disruptions that may be impacting message transit times, allowing for prompt resolution of any issues that may arise. By taking these steps, organizations can help ensure that their security mechanisms function as intended and that their sensitive data is well-protected.

[1].

Computer and network security is a war of wits between a perpetrator attempting to uncover vulnerabilities and a designer or administrator attempting to plug them. The attacker has a significant advantage in that he or she only must identify a single vulnerability.

However, the designer must identify and eradicate all vulnerabilities to achieve complete security [7].

Users and system administrators are naturally inclined to perceive little gain from security investments until a security failure happens [8].

Security demands continuous, if not continual, monitoring, which is problematic in today's world of short-term overload.

Security is frequently an afterthought added to a system after its design rather than an intrinsic part of the design process.

Numerous consumers and even security administrators perceive robust security as a hindrance to an information system's practical and user-friendly functioning or the use of information.

1.2 Security Attacks

Passive and active attacks are used to classify security threats. A passive attack seeks to get or utilize information from the system without impacting system resources. Active attacks modify system resources or interfere with operations [9].

1.2.1 Passive attacks

Aim to gather or use information from a system without affecting its resources. Passive Attacks consist of eavesdropping and transmission monitoring. The objective of the opponent is to get conveyed information. Passive attacks are incredibly challenging to detect since they do not require data modification. Typically, message traffic is transmitted and received in a manner that appears normal. Neither the sender nor the recipient is conscious that a service provider has read the messages or monitored the traffic pattern. However, it is possible to prevent these attacks from succeeding, often using encryption. In dealing with passive attacks, then, prevention takes precedence over detection.

Types of passive attacks include the following:

1.2.2 Releasing message content

Transmission of message content that may be a discussion over the phone, an email message, or a file transfer may comprise sensitive or

secret information. We seek to prevent an adversary from gaining access to the information in these messages.

1.2.3 Traffic analysis

Supposing we had a method of masking (encrypting) information, an attacker could not extract information from a communication even if it was collected.

The adversary might discover the address and identity of the transmitting host, as well as the message exchange rate and duration. This information may well be utilised to infer the nature of the conversation.

The most effective safeguard from traffic analysis is SIP traffic encryption. To accomplish this, an attacker must access the SIP proxies (or their call log) to know who initiated the call.

1.2.4 Active attacks

These attacks aim to modify system resources or interfere with their functioning. Active attacks entail data stream manipulation or the fabrication of false claims. Active attacks have qualities opposite to those of passive attacks. Passive attacks are hard to detect. However, countermeasures seek to prevent their success. Due to the vast number of possible physical, software, and network vulnerabilities, it is relatively difficult to avoid active attacks altogether. Instead, the objective is to identify active attacks and recover from disruptions or delays. Detection that has a deterrent impact may also help in prevention.

Active attack types include the following:

1.2.5 Masquerade

A masquerade attack occurs when one entity impersonates another. A Masquerade attack is comprised of one of the other active attack types. If an authorisation mechanism is not safeguarded, it might become highly susceptible to masquerade attacks. Masquerade attacks can be carried out using stolen passwords and login details, software vulnerabilities, or a way around the authentication procedure.

certificate with a digital signature. A CA, also known as a Certifying Authority, is responsible for the following core responsibilities:
Generates the key pairs - The key pair that the CA creates may be generated independently or in partnership with the customer, depending on the situation.

5.13.1 Issuing of the digital certificates

The Certification Authority (CA) will issue a certificate to the customer when the client has successfully provided all the correct information about his identification. After then, CA will perform an additional digital signature on this certificate to ensure the information cannot be altered.
The certification authority (CA) publishes the certificates so users can locate them when needed. They can accomplish this goal by including them in an online telephone directory or handing out hard copies to various individuals.

5.13.2 Verification of the certificate

The CA will provide a public key to the user, which will assist in determining whether the attempted access is permitted.
Revocation: The CA retains the authority to revoke a digital certificate if the client engages in a questionable activity or the CA no longer trusts the client.

5.13.3 The Different Types of Digital Certificates

Four primary classifications may be applied to a digital certificate. These include:
Class 1: To receive one, all required is an email address.
Class 2: requires a more significant amount of personally identifying information.
Class 3: This method begins by validating the identification of the individual putting in a request.
Class 4: These items are used by governments and organisations.
The steps involved in creating a certificate are as follows:
The following steps constitute the process of creating a certificate:

- It is necessary to generate both public and private keys.
- CA requires identifying information to be provided about the private key's owner.

- A CSR, also known as a Certificate Signing Request, is where a public key and its associated properties are encoded.
- The signature of the key owner on that CSR is evidence that they have a private key.
- After validation, the certificate is then signed by the CA.
- The establishment of Trust tiers inside CA Hierarchies:
- Every CA has its certificate to prove its legitimacy. As a result, trust is established hierarchically via the process of one CA issuing certificates to other CAs. In addition, a root certificate has been signed by itself. Regarding a root certification authority (CA), the issuer and the subject are considered the same entity.

In the previous section, we saw that the root CA is the ultimate authority. This section will focus on the security of the root CA. As a result, the safety of the root CA is of the utmost significance. A disaster may ensue if the root CA's private key is not protected correctly. This is since anyone who poses as the root certification authority may issue certificates. A root CA should be offline 99.9 percent of the time to conform to the established security criteria. Nevertheless, it must connect to the internet to generate public and private keys and issue new certificates. These pursuits must be carried out between two and four times every calendar year, at the very least.

5.14 PKI's Function in Today's Digital World

In today's digital world, many applications call for authentication. Certifications are essential for working in millions of different settings. Without a Public Key Infrastructure, this task is impossible to complete. The relevance of public key infrastructure (PKI), which varies based on the use case and the requirements, has grown over time. This is a snippet from the song's track.

From 1995 to 2002, public key infrastructure (PKI) was restricted to the certificates deemed the most significant and valuable for the first time. This includes the certifications that eCommerce websites need in order to be allowed to show the lock symbol in the search box. The

customers' confidence in the safety and veracity of numerous websites was intended to be increased due to this project.

2003 to 2010 saw the beginning of the second chapter of PKI, which saw the introduction of businesses into the mix. Workers started receiving computers during this time, and the number of people using mobile phones increased. Therefore, workers needed access to the organization's resources even when not working. At that point, using a PKI seemed the most compelling authentication method.

2011 marked the beginning of the third phase, which is still ongoing to the present day. The usage of public key infrastructure (PKI) has become much more complicated in recent years due to the proliferation of cutting-edge technologies such as the Internet of Things (IoT) and the need to expand PKI. Today, the authentication of mobile workforces requires the issuance of millions of certificates. Nevertheless, keeping track of such a massive number of certifications is difficult.

PKI is also used for S/MIME documents, code, and app signing.

5.14.1 Challenges Overcome with a PKI:

PKI is so widely used because it offers solutions to various issues. The following are examples of uses for PKI:

- SSL/TLS certificates provide security for web browsers and networks used for communication.
- Managing Access Rights Across Intranets and Virtual Private Networks
- The Encryption of Data
- Software that has been digitally signed
- Access to Wi-Fi Without the Need for a Password

In addition, one of the most important use cases for PKI is focused on the Internet of Things (Internet of Things). The following is a list of two industries that make use of PKI for Internet of Things devices:

5.14.2 Automakers

Today's vehicles are equipped with various technologies, including a global positioning system (GPS), a phone system, assistants, etc. These need communication channels via which a significant amount of data is sent. Ensuring these connections' safety is crucial to

prevent criminals from breaking into the vehicles. PKI is where we find ourselves now.

Manufacturers of medical devices, please note that high levels of security are required for devices such as surgical robots. Additionally, the FDA requires that all medical devices of the next generation be capable of receiving software updates, which allows for correcting defects and resolving any security concerns. The Public Key Infrastructure (PKI) issues certificates to such devices.

Disadvantages of PKI:

Speed

Because PKI uses intricate algorithms to produce a reliable key pair, it gradually causes the procedure and data transmission to become slower.

Private Key Compromise:

Even though PKI cannot be hacked very quickly, a private key can be hacked by a professional hacker. Since PKI uses Public and Private keys to encrypt and decrypt data, the information can be decrypted easily with the user's private and public keys, which are readily available.

5.15 Key Management

In cryptography, distributing public and private keys between a sender and receiver is highly laborious and time-consuming. If the key is known by the third party (the person forging the documents or listening in on the conversation), then the whole security system is rendered useless. Therefore, the need arises to safeguard the trading of keys [112].

There are two different facets to what is known as Key Management:

- Distribution of public keys.
- Use of public-key encryption to distribute secrets.

5.16 Pubic Key Distribution

- Public announcement
- Public-key authority
- Public-key certificates.

- Publicly available directory

These are described in further detail as follows:

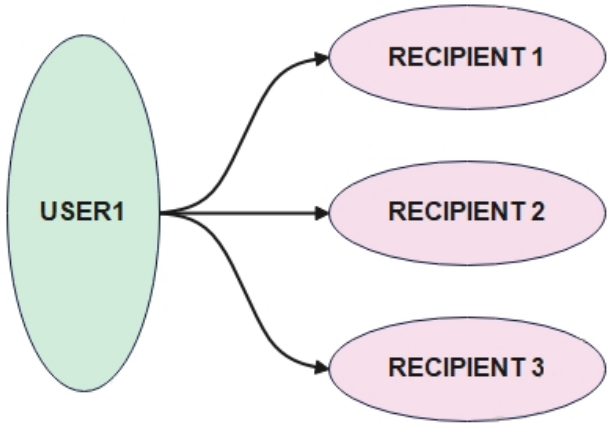

Fig.26 Public Key Announcement [112]

5.16.1. The Public Announcement

This is where the audience key is announced to the general public. The use of a forgery is this method's most significant flaw. Anyone can generate and broadcast a key while pretending to be someone else. The imposter may pose as the stated user if the counterfeit is not found.

5.16.2. Public Key directory

The public key for this type is kept in a directory accessible to the public. The directories that include qualities such as Participant Registration, access, and the ability to edit data at any time are trusted here. These directories also contain items such as "name, public key." Though directories may be viewed electronically, they are still susceptible to being forged or altered somehow.

5.16.3. Public Key Authority

There is a Public Key Authority for:

It is pretty much like the directory, but it enhances safety by providing a more stringent level of control over the dissemination of keys from the directory. Users need to possess the directory's public key to access it. Whenever the keys are required, the user performs real-time access to the directory to acquire any necessary public key securely.

5.16.4 Public Certification

This time authority delivers a certificate (which attaches an identity to the public key) to enable key exchange without requiring each time that the user has real-time access to the public authority. The certificate is accompanied by additional information, such as the time it is valid for usage, the associated rights, etc. The certificate authority's private key signs all this material, which can be confirmed by anybody owning the authority's public key [112].

After both the sender and the receiver have submitted a request to the CA for a certificate that includes a public key and other information, the two parties can exchange certificates and begin communicating.

5.17 Key Sharing in Cryptography

As was said before, the primary goal of cryptography is to prevent unwanted parties from gaining access to the information being stored. On the other hand, there are several classifications of cryptographic algorithms. Asymmetric and symmetric cryptography is the most often used [113].

The cryptographic keys provide the primary point of differentiation between symmetric and asymmetric forms of cryptography. Asymmetric cryptography makes use of two keys, known as the public key and the private key. Data may be encrypted with one key, and then decrypted using a different key.

In contrast, symmetric cryptography employs a single key for data encryption and decryption. The entities that encrypt and decrypt data need access to the same key in order to interact with one another in this manner.

The following diagram illustrates the steps required to encrypt and decode data using symmetric and asymmetric cryptography:

The techniques used in asymmetric cryptography are very flexible, and it is simple to distribute keys. In turn, symmetric algorithms are often more straightforward and efficient (regarding execution time) than their asymmetric counterparts. However, one of the most significant difficulties associated with symmetric algorithms is the

safe distribution of cryptographic keys to authorised parties. In the next part of this article, we will discuss several ways to distribute symmetric keys [113].

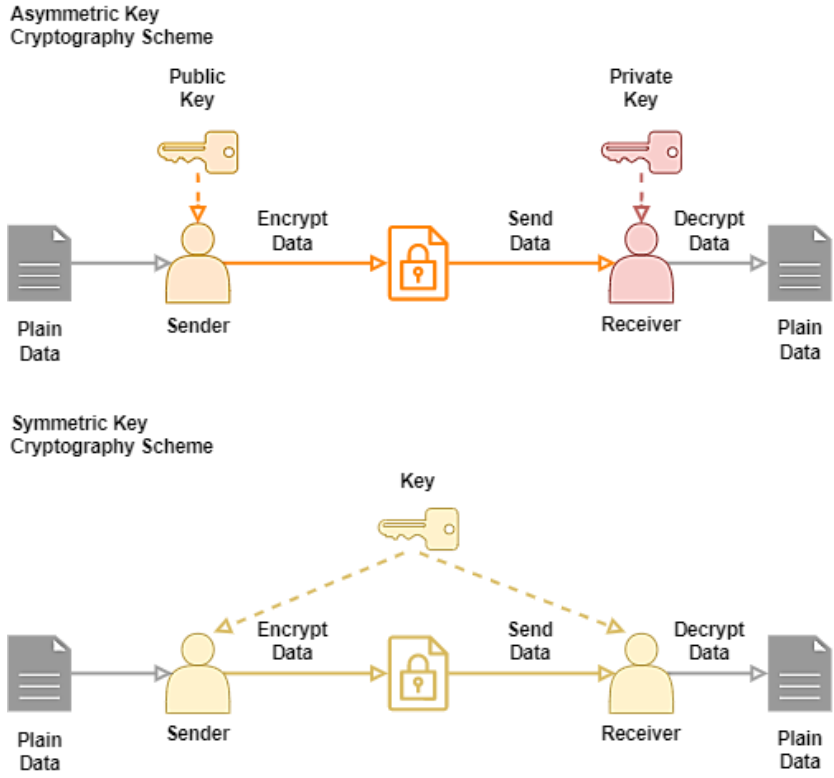

Fig.27 Asymmetric and Symmetric Key Sharing [113]

5.17.1 Key Encapsulation Mechanism

Sending a letter to the authorised entity is the first thing that comes to mind when thinking about key encapsulation. The envelope used to mail the letter needs to be safe and verifiable.

Consequently, the unique envelope is produced by a key encapsulation technique using both public and private asymmetric cryptography keys.

One of the parties participating in the communication process generates the symmetric key and encrypts it using another party's public key. After that, the first entity will transmit the encoded

symmetric key to the second entity, which will then receive it, then decode it using the appropriate private key.
In addition to merely encoding the symmetric key with a public key, the first entity may sign it with a private key to verify its authenticity. Therefore, the first entity also gives the second entity a public key. This allows the second entity to verify the validity of the symmetric key it has been given.
An example of one method for the encapsulation of keys may be shown in the following picture:

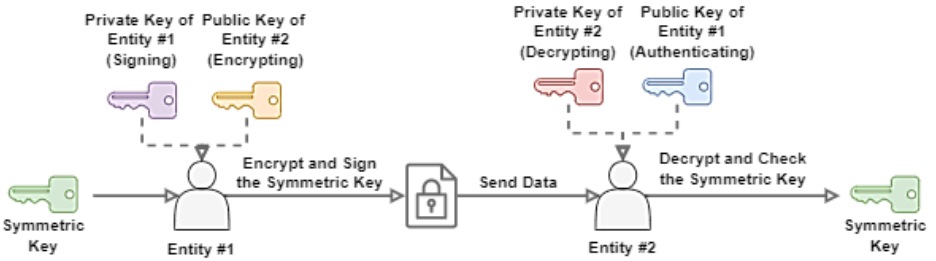

Fig.28 Possible process for key encapsulation [113]

Next, we may question why we do not just interact directly with public and private keys rather than utilising them to trade symmetric key pairs. Symmetric cryptography is generally more efficient when encoding and decoding lengthy communications than asymmetric encryption. This is the solution to our question.
In this sense, adopting less resource-intensive cryptography techniques, such as the symmetric ones, is desirable while conducting communications that include an extensive data exchange.

5.17.2 Out-of-Band Procedures

Out-of-band methods include using other communication means from the one typically used to exchange data to facilitate the distribution of symmetric cryptographic keys.
Therefore, in place of the customary practice of transmitting cryptographic keys over the Internet, the parties involved in the process can choose to exchange them by means such as making a phone call, sending a letter through the conventional postal service, or even physically meeting one another in the real world [113].

It is essential to highlight that the level of security associated with out-of-band operations might be challenging to assess. In a scenario like this one, the level of security depends on many factors of the communication channel and the dependability of the individuals participating in the transmission of the cryptographic key.

In any case, we assume that the likelihood of a malicious entity hunting for cryptographic keys outside the scope of networked connections is significantly lower than the possibility of such an entity. Therefore, it is possible that it would be desirable to adopt non-standard processes whenever it would be possible to do so.

5.17.3 Key Distribution Centre [114]

A Key Distribution Center, also known as a KDC, is a centralised authority that manages the keys for individual computers, also known as nodes, in a computer network. It is comparable to how Kerberos handles the Authentication Server (AS) and the Ticket Granting Server (TGS) concepts [114].

The fundamental premise is that each network node exchanges its unique secret key with the KDC. The following are the steps that must be taken if user A wishes to speak privately with user B:

The situation has been set up such that A has divulged the secret key KA to KDC. Likewise, it is presumed that B and the KDC both have access to the secret key KB.

A will make a request to KDC that has been encrypted using KA. This request will comprise

(a) The similarities between A and B

(b) A random number, denoted by the letter "nonce."

In response, KDC sends a message that is encrypted using KA and contains

(a) Key symmetric to the one-time only

(b) The first request for verification was submitted by A.

(c) KS has been encrypted using KB, and the ID of A has been encrypted using KB.

A and B can now communicate thanks to A's use of KS as an encryption method [114].

The following figure illustrates this point:

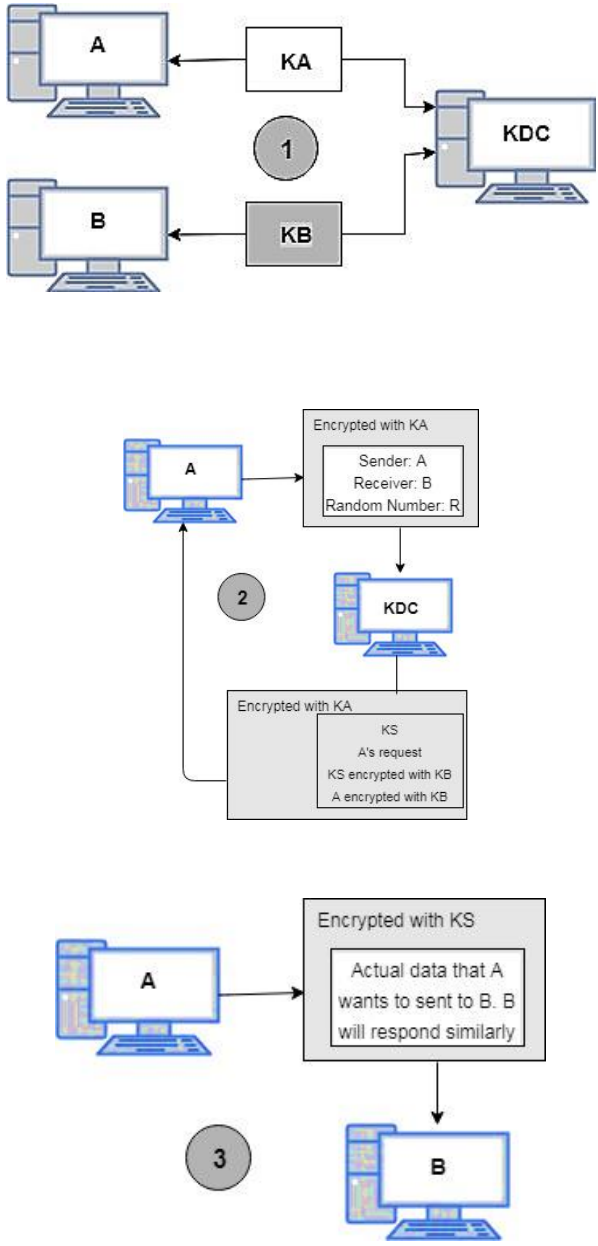

Fig: 28. Key Distribution Centre (KDC)

<<<O>>>

This Page Intentionally Left Blank

References, Bibliography and Webliography

1. Stallings, W., 2006. *Cryptography and network security, 4/E*. Pearson Education India.
2. Abou el Kalam, A., 2021. Securing SCADA and critical industrial systems: From needs to security mechanisms. *International Journal of Critical Infrastructure Protection*, *32*, p.100394.
3. Guttman, B. and Roback, E.A., 1995. *An introduction to computer security: the NIST handbook*. Diane Publishing.
4. Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 2018. *Handbook of applied cryptography*. CRC press.
5. Amoroso, E., 2012. *Cyber-attacks: protecting national infrastructure*. Elsevier.
6. Carman, D.W., Kruus, P.S. and Matt, B.J., 2000. Constraints and approaches for distributed sensor network security (final). *DARPA Project report, (Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, *1*(1), pp.1-39.
7. Whitman, M.E. and Mattord, H.J., 2021. *Principles of information security*. Cengage learning.
8. Cranor, L.F. and Garfinkel, S., 2005. *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.".
9. Nawir, M., Amir, A., Yaakob, N. and Lynn, O.B., 2016, August. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd international conference on electronic design (ICED)* (pp. 321-326). IEEE.
10. Abraham, S. and Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), pp.183-196.
11. Paxson, V., 1999. Bro: a system for detecting network intruders in real time. *Computer networks*, *31*(23-24), pp.2435-2463.
12. Chakkaravarthy, S.S., Sangeetha, D. and Vaidehi, V., 2019. A survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, pp.1-23.
13. Branscomb, A.W., 1990. Rogue computer programs and computer rogues: Tailoring the punishment to fit the crime. *Rutgers Computer & Tech. LJ*, *16*, p.1.
14. Singer, P.W. and Friedman, A., 2014. *Cybersecurity: What everyone needs to know*. oup usa.
15. Johnson, V.R., 2005. Cybersecurity, Identity Theft, and the Limits of Tort Liability. *ScL REv.*, *57*, p.255.

16. Chen, T.M. and Robert, J.M., 2004. The evolution of viruses and worms. In *Statistical methods in computer security* (pp. 289-310). CRC press.
17. Messe, N., Belloir, N., Chiprianov, V., El-Hachem, J., Fleurquin, R. and Sadou, S., 2020, December. An asset-based assistance for secure by design. In *2020 27th Asia-Pacific Software Engineering Conference (APSEC)* (pp. 178-187). IEEE.
18. Rogers, J., 2020. *The Gendering of Virtue: Cultural Influence on the Semantic Development of Aretē and Virtus* (Doctoral dissertation, University of Kansas).
19. Kruse II, W.G. and Heiser, J.G., 2001. *Computer forensics: incident response essentials*. Pearson Education.
20. Tekiner, E., Acar, A., Uluagac, A.S., Kirda, E. and Selcuk, A.A., 2021, September. SoK: cryptojacking malware. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 120-139). IEEE.
21. Ngo, F.T., Agarwal, A., Govindu, R. and MacDonald, C., 2020. Malicious software threats. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 793-813). Palgrave Macmillan, Cham.
22. Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data Security. In *Data Ethics and Challenges* (pp. 41-59). Springer, Singapore.
23. Sarkar, K.R., 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), pp.112-133.
24. Narwal, B., Mohapatra, A.K. and Usmani, K.A., 2019. Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems*, *22*(2), pp.301-325.
25. Shin, B. and Lowry, P.B., 2020. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*, p.101761.
26. Attaran, M., 2017. The internet of things: Limitless opportunities for business and society. *Journal of Strategic Innovation and Sustainability Vol*, *12*(1), p.11.
27. Minnaar, A. and Herbig, F.J., 2021. Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), pp.155-185.

28. Adebayo, O.S. and Dauda, U.S., 2020. CST 805: Computer and Network Security.
29. Biswas, K. and Ali, M., 2007. Security threats in mobile ad hoc network.
30. Molva, R., Tsudik, G., Herreweghen, E.V. and Zatti, S., 1992, November. KryptoKnight authentication and key distribution system. In *European Symposium on Research in Computer Security* (pp. 155-174). Springer, Berlin, Heidelberg.
31. Shetty, S., Red, V., Kamhoua, C., Kwiat, K. and Njilla, L., 2017, May. Data provenance assurance in the cloud using blockchain. In *Disruptive Technologies in Sensors and Sensor Systems* (Vol. 10206, pp. 125-135). SPIE.
32. Barsoum, A. and Hasan, A., 2012. Enabling dynamic data and indirect mutual trust for cloud computing storage systems. *IEEE transactions on parallel and distributed systems*, *24*(12), pp.2375-2385.
33. Khedr, W.I., Khater, H.M. and Mohamed, E.R., 2019. Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage. *IEEE Access*, *7*, pp.65635-65651.
34. Joshi, S., Stalin, S., Shukla, P.K., Shukla, P.K., Bhatt, R., Bhadoria, R.S. and Tiwari, B., 2021. Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain. *Wireless Communications and Mobile Computing*, *2021*.
35. Goyal, P., Parmar, V. and Rishi, R., 2011. Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management*, *11*(2011), pp.32-37.
36. Goyal, V. and Arora, G., 2017. Review paper on security issues in mobile ad-hoc networks. *International Research Journal of Advanced Engineering and Science*, *2*(1), pp.203-207.
37. Miller, W.R., Forcehimes, A.A. and Zweben, A., 2019. *Treating addiction: A guide for professionals*. Guilford Publications.
38. Kumar, S.N., 2015. Review on network security and cryptography. *International Transaction of Electrical and Computer Engineers System*, *3*(1), pp.1-11.
39. Peng, J., 2020. *Secure covert communications over streaming media using dynamic steganography* (Doctoral dissertation, University of West London).
40. "What is Email Security?" Proofpoint. Last modified September 6, 2022. https://www.proofpoint.com/us/threat-reference/email-security.

41. Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
42. Blakley, B., McDermott, E. and Geer, D., 2001, September. Information security is information risk management in *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104).
43. Caswell, B. and Beale, J., 2004. *Snort 2.1 intrusion detection*. Elsevier.
44. Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences* 80, no. 5 (2014): 973-993.
45. Taylor, Craig. "Access Control Mechanism." CyberHoot. Last modified January 10, 2022. https://cyberhoot.com/cybrary/access-control-mechanism/.
46. Sohraby, K., Minoli, D. and Znati, T., 2007. *Wireless sensor networks: technology, protocols, and applications*. John Wiley & sons.
47. Myers, J., Frieden, T.R., Bherwani, K.M. and Henning, K.J., 2008. Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. *American Journal of public health*, *98*(5), pp.793-801.
48. Alharbi, F., Alrawais, A., Rabiah, A.B., Richelson, S. and Abu-Ghazaleh, N., 2021. {CSProp}: Ciphertext and Signature Propagation {Low-Overhead}{Public-Key} Cryptosystem for {IoT} Environments. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 609-626).
49. Ryan, P., Schneider, S.A., Goldsmith, M. and Lowe, G., 2001. *The modelling and analysis of security protocols: the CSP approach*. Addison-Wesley Professional.
50. Asif, Ali Mir Arif Mir and Shaikh Abdul Hannan. "A Review on Classical and Modern Encryption Techniques." international journal of engineering trends and technology 12 (2014): 199-203.
51. Biswas, M.H., Ali, M.A., Rahman, M. and Sohel, M.M.K., 2019. A systematic study on classical cryptographic cypher in order to design a smallest cipher. *Int. J. Sci. Res. Publ*, *9*(12), pp.507-11.
52. Soofi, A.A., Riaz, I. and Rasheed, U., 2016. An enhanced vigenere cipher for data security. *Int. J. Sci. Technol. Res*, *5*(3), pp.141-145.
53. Apelbaum, Y., 2007. *User Authentication principles, theory and practice*. Fuji Technology Press.
54. Stamp, M., 2011. *Information security: principles and practice*. John Wiley & Sons.

55. Sharma, I.R. and Gupta, V., 2013. Comparative Analysis of DES and S-DES Encryption Algorithm Using Verilog Coding. In *India*.
56. Chowdhury, D., Dey, A., Anand, H., Sengupta, S. and Chakraborty, S., 2021. An Approach to Avoid Meet in the Middle Attack in 2 DES. In *Interdisciplinary Research in Technology and Management* (pp. 602-608). CRC Press.
57. "Avalanche Effect in Cryptography." GeeksforGeeks. Last modified March 14, 2022. https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/.
58. Lee, H.K., Malkin, T. and Nahum, E., 2007, October. Cryptographic strength of SSL/TLS servers: Current and recent practices. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (pp. 83-92).
59. "Data Encryption Standard (DES) | Set 1." GeeksforGeeks. Last modified May 15, 2022. https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/.
60. "Data Encryption Standard (DES) | Set 1." GeeksforGeeks. Last modified May 15, 2022. https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/.
61. Mardon, A., Barara, G., Chana, I., Di Martino, A., Falade, I., Harun, R., Hauser, A., Johnson, J., Li, A., Pham, J. and Varghese, N., 2021. Cryptography.
62. "Digital Signature Cryptography." EDUCBA. Last modified June 6, 2022. https://www.educba.com/digital-signature-cryptography/.
63. Burr, W.E., Dodson, D.F. and Polk, W.T., 2006. *Electronic authentication guideline* (pp. 800-63). US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
64. Denning, D.E. and Sacco, G.M., 1981. Timestamps in key distribution protocols. *Communications of the ACM*, *24*(8), pp.533-536.
65. Chaum, D., Grothoff, C. and Moser, T., 2021. How to issue a central bank digital currency. *arXiv preprint arXiv:2103.00254*.
66. Conti, M., Kumar, E.S., Lal, C. and Ruj, S., 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), pp.3416-3452.
67. "What is Encryption? - Definition, Types & More | Proofpoint US." Proofpoint. Last modified August 10, 2022. https://www.proofpoint.com/us/threat-reference/encryption.
68. "Public and Private Encryption Keys." PreVeil. Last modified March 22, 2021. https://www.preveil.com/blog/public-and-private-key/.

69. Callas, J., Donnerhacke, L., Finney, H., Shaw, D. and Thayer, R., 2007. *OpenPGP message format* (No. rfc4880).
70. Endeley, R.E., 2018. End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security*, *9*(01), p.95.
71. Wu, H., Wu, Q., Cheng, G. and Guo, S., 2020, July. Instagram user behavior identification based on multidimensional features. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1111-1116). IEEE.
72. Anwar, N., Riadi, I. and Luthfi, A., 2016. Forensic SIM card cloning using authentication algorithm. *International Journal of Electronics and Information Engineering*, *4*(2), pp.71-81.
73. Delfs, H. and Knebl, H., 2015. Symmetric-key cryptography. In *Introduction to Cryptography* (pp. 11-48). Springer, Berlin, Heidelberg.
74. Manifavas, C., Hatzivasilis, G., Fysarakis, K. and Papaefstathiou, Y., 2016. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks*, *9*(10), pp.1226-1246.
75. Alkhzaimi, H.A. and Knudsen, L.R., 2016. Cryptanalysis of selected block ciphers. *Kgs. Lyngby: Technical University of Denmark (DTU).(DTU Compute PHD*, (360).
76. "Feistel Block Cipher." Binary Terms. Last modified January 18, 2021. https://binaryterms.com/feistel-block-cipher.html.
77. IDEA Algorithm." EDUCBA. Last modified July 6, 2022. https://www.educba.com/idea-algorithm/
78. Rivest, R.L., 1994, December. The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86-96). Springer, Berlin, Heidelberg.
79. Rivest, R.L., 1994, December. The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86-96). Springer, Berlin, Heidelberg.
80. Zhang, Z. and Shi, Y., 2009. Communication complexities of symmetric XOR functions. *Quantum Information & Computation*, *9*(3), pp.255-263.
81. Knudsen, L. and Wagner, D., 2002, February. Integral cryptanalysis. In *International Workshop on Fast Software Encryption* (pp. 112-127). Springer, Berlin, Heidelberg.
82. Bellare, M. and Namprempre, C., 2000, December. Authenticated encryption: Relations among notions and analysis of the generic

composition paradigm. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 531-545). Springer, Berlin, Heidelberg.

83. Shan, W., Wang, L., Li, Q., Guo, L., Liu, S. and Zhang, Z., 2014, November. A chosen-plaintext method of CPA on SM4 block cipher. In *2014 Tenth International Conference on Computational Intelligence and Security* (pp. 363-366). IEEE.
84. Chang, X., Yan, A. and Zhang, H., 2020. Ciphertext-only attack on optical scanning cryptography. *Optics and Lasers in Engineering*, *126*, p.105901.
85. Arora, A. and Sharma, R.K., 2021. Known-plaintext attack (KPA) on an image encryption scheme using enhanced skew tent map (ESTM) and its improvement. *Optik*, *244*, p.167526.
86. Bhushan, B., Sahoo, G. and Rai, A.K., 2017, September. Man-in-the-middle attack in wireless and computer networking—A review. In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)* (pp. 1-6). IEEE.
87. Biswas, M.H., Ali, M.A., Rahman, M. and Sohel, M.M.K., 2019. A systematic study on classical cryptographic cypher in order to design a smallest cipher. *Int. J. Sci. Res. Publ*, *9*(12), pp.507-11.
88. Canale, F., Güneysu, T., Leander, G., Thoma, J., Todo, Y. and Ueno, R., 2022. SCARF: A Low-Latency Block Cipher for Secure Cache-Randomization. *Cryptology ePrint Archive*.
89. Abd, A.J. and Al-Janabi, S., 2019. Classification and identification of classical cipher type using artificial neural networks. *Journal of Engineering and Applied Sciences*, *14*(11), pp.3549-3556.
90. Giddy, J.P. and Safavi-Naini, R., 1994. Automated cryptanalysis of transposition ciphers. *The Computer Journal*, *37*(5), pp.429-436.
91. Naudts, B. and Kallel, L., 2000. A comparison of predictive measures of problem difficulty in evolutionary algorithms. *IEEE Transactions on Evolutionary Computation*, *4*(1), pp.1-15.
92. Boneh, D., DeMillo, R.A. and Lipton, R.J., 1997, May. On the importance of checking cryptographic protocols for faults. In *International conference on the theory and applications of cryptographic techniques* (pp. 37-51). Springer, Berlin, Heidelberg.
93. Sengupta, N. and Holmes, J., 2013, November. Designing of cryptography-based security system for cloud computing. In *2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies* (pp. 52-57). IEEE.

94. Balogun, A.O., Sadiku, P.O., Mojeed, H.A. and Rafiu, H.A., 2017. Multiple Caesar cypher encryption algorithm. *ABACUS (Mathematical Science Series)*, *44*(2), pp.250-258.
95. Merkle, R.C., 2019. Protocols for public key cryptosystems. In *Secure communications and asymmetric cryptosystems* (pp. 73-104). Routledge.
96. Pakshwar, R., Trivedi, V.K. and Richhariya, V., 2013. A survey on different image encryption and decryption techniques. *International journal of computer science and information technologies*, *4*(1), pp.113-116.
97. Nguyen, P.Q., 2009. Public-key cryptanalysis. *Recent Trends in Cryptography, Contemp. Math*, *477*, pp.67-119.
98. Milanov, E., 2009. The RSA algorithm. *RSA laboratories*, pp.1-11.
99. Gennaro, R., Krawczyk, H. and Rabin, T., 1997, August. RSA-based undeniable signatures. In *Annual International Cryptology Conference* (pp. 132-149). Springer, Berlin, Heidelberg.
100. Tsiounis, Y. and Yung, M., 1998, February. On the security of ElGamal based encryption. In *International Workshop on Public Key Cryptography* (pp. 117-134). Springer, Berlin, Heidelberg.
101. Toughi, S., Fathi, M.H. and Sekhavat, Y.A., 2017. An image encryption scheme based on elliptic curve pseudo-random and advanced encryption system. *Signal processing*, *141*, pp.217-227.
102. Nia, M.A., Sajedi, A. and Jamshidpey, A., 2014. An introduction to digital signature schemes. *arXiv preprint arXiv:1404.2820*.
103. "Cryptography Digital Signatures." Online Tutorials Library. Accessed September 27, 2022. https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.
104. Rivest, R.L., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), pp.120-126.
105. Li, J., Li, J., Chen, X., Jia, C. and Lou, W., 2013. Identity-based encryption with outsourced revocation in cloud computing. *Ieee Transactions on computers*, *64*(2), pp.425-437.
106. Schwenk, J., Brinkmann, M., Poddebniak, D., Müller, J., Somorovsky, J. and Schinzel, S., 2020, October. Mitigation of attacks on email end-to-end encryption. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1647-1664).
107. "Cryptography Digital Signatures." Online Tutorials Library. Accessed September 27, 2022.

https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.
108. Feige, U., Fiat, A. and Shamir, A., 1988. Zero-knowledge proofs of identity. *Journal of cryptology*, *1*(2), pp.77-94.
109. Brown, E.T., Ottley, A., Zhao, H., Lin, Q., Souvenir, R., Endert, A. and Chang, R., 2014. Finding waldo: Learning about users from their interactions. *IEEE Transactions on visualization and computer graphics*, *20*(12), pp.1663-1672.
110. "Digital Signature Standard (DSS)." GeeksforGeeks. Last modified May 28, 2020. https://www.geeksforgeeks.org/digital-signature-standard-dss/.
111. "Public Key Infrastructure." GeeksforGeeks. Last modified June 9, 2022. https://www.geeksforgeeks.org/public-key-infrastructure/?ref=gcse.
112. "Key Management in Cryptography." GeeksforGeeks. Last modified January 13, 2022. https://www.geeksforgeeks.org/easy-key-management-in-cryptography/?ref=gcse.
113. Symmetric Cryptography. Accessed September 27, 2022. https://www.baeldung.com/cs/symmetric-cryptography.
114. "Key Distribution Center (KDC)." Ques10 - Study Engineering Subjects Online. Accessed September 27, 2022. https://www.ques10.com/p/33951/key-distribution-center-kdc-1/.

<<< O >>>

This Page Intentionally Left Blank