Learning Guide Unit 4

Site:	University of the People	Printed by:	Mejbaul Mubin
Course:	CS 3340-01 Systems and Application Security - AY2025-T1	Date:	Thursday, 5 September 2024, 2:36 PM
Book:	Learning Guide Unit 4		

Description

Learning Guide Unit 4

Table of contents

Overview

UNIT 4: Encryption and Authentication

Topics

- Introduction to Encryption and Authentication
- Fundamentals of encryption
- Symmetric vs. asymmetric encryptions
- RSA and PKI
- Brute Force attack

Learning Objectives

By the end of this Unit, you will be able to:

1. Discuss the advantages and disadvantages of using email encryption and digital signatures.
2. Recall and share your personal experience(s) related to encryption and/or the use of digital certificates for a personal signature.
3. Identify trends for the future in the application of cryptology.
4. Explore Encryption and Authentication.

Tasks

- Peer assess Unit 3 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz

Introduction to Encryption and Authentication

Authentication is a way to determine if someone or something is the same who or what it says it is. Encryption plays a great role in the authentication process.

Encryption has been known and used by people for centuries. The first historically documented encryption goes back to 600BC when the ancient Spartans "used a device called a scytale to send secret messages during battle" (A brief history of encryption, 2021). The history of modern cryptography begins in the early 1970s. IBM developed a block cipher that was adopted in 1973 as Data Encryption Standard (DES). DES is a Symmetric encryption algorithm. It means the same encryption key is used to both encrypt and decrypt the data. The cipher served its purpose until 1997 when American cryptographers Whitfield Diffie and Martin Hellman proved that DES can be broken by Brute Force. Moreover, Diffie & Hellman introduce a new approach in encryption using two encryption keys (one public and one private) to exchange protected messages over the computer networks. This methodology is still in use, though encryption algorithms have seen changes over time. Asymmetric encryption algorithms came to replace symmetric ones. To learn more about the history of Cryptography, visit the resources listed under the References.

Resources

A brief history of encryption. (2021, March 21). Thalesgroup. Retrieved June 6, 2021 from https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

*How to become a cryptographer. (*2021, December 8). Cyberdegrees. https://www.cyberdegrees.org/jobs/cryptographer/

Istoria, A. (2020, June 18). *How did ancient Greeks send secret messages?* [Video]. YouTube. https://www.youtube.com/watch?v=ac3l8J_rYNg

What is DES? Understanding DES algorithm and operation. (2021, May 10). Simplilearn. https://www.simplilearn.com/what-is-des-article#:~:text=The%20DES%20(Data%20Encryption%20Standard,ciphertext%20using%2048%2Dbit%20keys.

Fundamentals of Encryption

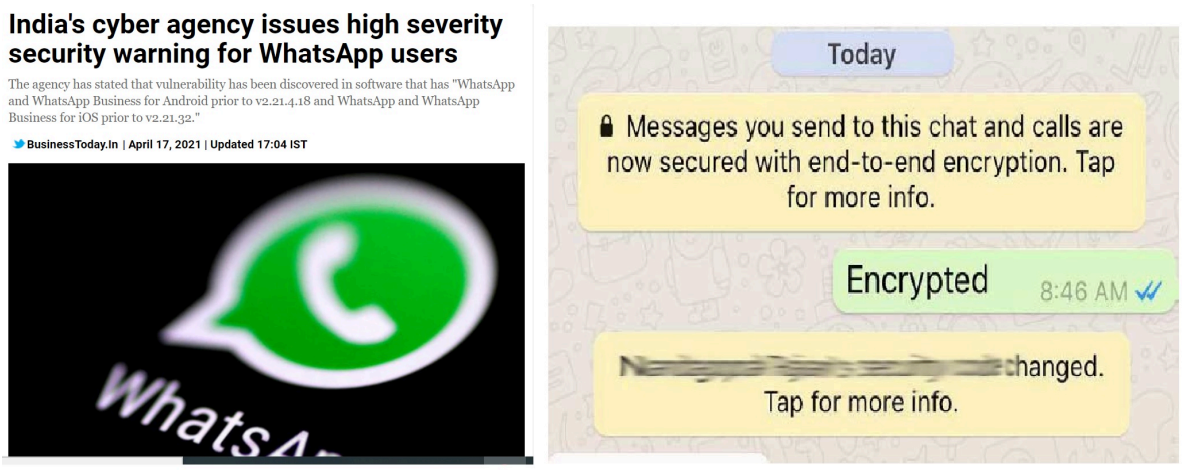

Figure 1

India's cybersecurity agency has warned WhatsApp users in the country about certain vulnerabilities detected in the messaging app. These vulnerabilities could lead to a breach of sensitive information of WhatsApp users.

Read the news headlines shown on the left-hand side of Fig.1 or read the full news article provided under the resources.

From the news article, you can infer that personal data is not fully protected. The personal data is not private completely and can be used by any third party for their benefit. To avoid such situations, Cryptographers put control on the data.

Encryption is a security control, used primarily to provide confidentiality protection for data. It is a mathematical transformation to scramble data requiring protection (plaintext) into a form not easily understood by unauthorized people or machines (ciphertext) (Stine & Dang, 2011).

Reading Assignments:

Read What Is Data Encryption? Definition, Best Practices & More

Watch Encryption Basics | Cryptography

Resources

India's cyber agency issues high severity security warning for WhatsApp users. (2021, April 17). *BusinessToday*. https://www.businesstoday.in/technology/news/indias-cyber-agency-issues-high-severity-security-warning-for-whatsapp-users/story/436889.html

Lord, N., (2020, December 1). *What is data encryption? Definition, best practices & more.* Digital Gardian. https://digitalguardian.com/blog/what-data-encryption

Network Direction. (2019, October 30). *Encryption basics | cryptography* [Video]. YouTube. https://www.youtube.com/watch?v=V67drkkk2aA

Stine, K. & Dang, Q. (2011, May). *Encryption basics.* AHIMA. https://library.ahima.org/doc?oid=104090#.Ydlbpf5Bw2w

Untitled illustration of WhatsApp Encryption. (2016). [Online image]. Indianexpress. https://images.indianexpress.com/2016/04/whatsapp_encryption_1_new.jpg

Symmetric vs. Asymmetric Encryption

With symmetrical encryption, the same key is used to encrypt and decrypt messages because the whole thing depends on keeping the key secret. This means that it must be shared with the receiver securely so that only he can use it to decrypt the message.

Asymmetric Encryption involves the use of two connected mathematical keys. Both the public key (which everyone knows) and the private key (which only you know) are needed to encrypt and decrypt the message. The private key is not allowed to come from the public key.

Reading Assignments:

Read: Symmetric vs. asymmetric encryption

Watch: Symmetrical vs asymmetrical Encryption Pros and Cons by Example

Resources

Nasser, H. (2019, June 8). *Symmetrical vs asymmetrical encryption pros and cons by example* [Video]. YouTube. https://www.youtube.com/watch?v=Z3FwixsBE94

Professor Messer. (2014, September 21*). Symmetric vs. asymmetric encryption - compTIA security+ SY0-401: 6.1* [Video]. YouTube. https://www.youtube.com/watch?v=z2aueocJE8Q

Edpresso Team. (n.d.). *Symmetric vs. asymmetric encryption*. educative. https://www.educative.io/edpresso/symmetric-vs-asymmetric-encryption?aid=5082902844932096&utm_source=google&utm_medium=cpc&utm_campaign=edpresso-dynamic&gclid=Cj0KCQjwktKFBhCkARIsAJeDT0gFV4c5VUuxZKZSTlysDKO-Hc3j-WBnV0fRKNx4RGP9yXr8rZilk1QaArnPEALw_wcB

RSA and PKI

The first asymmetric encryption RSA was developed by three MIT scientists Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman, and was named after them using 1st letters of each last name. RSA is widely used and known as a core of Public Key Infrastructure PKI.

To know more about Public Key Infrastructure (PKI) watch the following video.

Reading Assignments:

Read Public Key Cryptography

Watch How RSA Encryption Works

Resources:

Cryptography – public key encryption. (2015). *Cryptography for beginners*, 49-56. https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

Mental Outlaw. (2021, February 10). *How RSA encryption works* [video]. YouTube. https://www.youtube.com/watch?v=ZPXVSJnDA_A

Turner, P. (2017, January 30). *PKI bootcamp - what is a PKI?* [Video]. YouTube. https://www.youtube.com/watch?v=5OqgYSXWYQM

Brute Force Attack

Brute Force attacks are used to gain access to user accounts by trying every possible way to crack passwords, encryption keys, and login credentials. Thus, the longer the encryption key, the more possible combination of its symbols will be. The most common use of the Brute Force attack is breaking passwords used for user authentication. Once the password is revealed, the attacker can access the computer system and private data in the system.

Reading Assignments:

Read Brute Force Attack: Definition and Examples

Watch What is Brute Force Attack? | Password Cracking Using Brute Force Attacks | Edureka

Resources:

Brute force attack: Definition and examples. (n.d.). Kaspersky. https://www.kaspersky.com/resource-center/definitions/brute-force-attack

edureka!. (2019, November 1). *What is brute force attack? | password cracking using brute force attacks/ edureka* [Video]. YouTube. https://www.youtube.com/watch?v=fHsJAei2ocM&t=3s

Professor Messer. (2019, June 9). *brute force attacks - compTIA A+ 220-1002 - 2.5* [Video]. YouTube. https://www.youtube.com/watch?v=W_NaKJrTmRk

Reading Assignment

1. *A brief history of encryption*. (2021, March 21). Thalesgroup. Retrieved June 6, 2021 from **https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption**
2. *Brute force attack: Definition and examples*. (n.d.). Kaspersky. **https://www.kaspersky.com/resource-center/definitions/brute-force-attack**
3. Cryptography – public key encryption. (2015). *Cryptography for beginners*, 49-56. **https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf**
4. Edpresso Team. (n.d.). *Symmetric vs. asymmetric encryption*. educative. **https://www.educative.io/edpresso/symmetric-vs-asymmetric-encryption?aid=5082902844932096&utm_source=google&utm_medium=cpc&utm_campaign=edpresso-dynamic&gclid=Cj0KCQjwktKFBhCkARIsAJeDT0gFV4c5VUuxZKZSTlysDKO-Hc3j-WBnV0fRKNx4RGP9yXr8rZilk1QaArnPEALw_wcB** licensed under CC-BY-SA 4.0.
5. *How to become a cryptographer. (*2021, December 8). Cyberdegrees. **https://www.cyberdegrees.org/jobs/cryptographer/**
6. India's cyber agency issues high severity security warning for WhatsApp users. (2021, April 17). *BusinessToday*. **https://www.businesstoday.in/technology/news/indias-cyber-agency-issues-high-severity-security-warning-for-whatsapp-users/story/436889.html**
7. Lord, N., (2020, December 1). *What is data encryption? Definition, best practices & more.* Digital Gardian. **https://digitalguardian.com/blog/what-data-encryption**
8. Stine, K. & Dang, Q. (2011, May). *Encryption basics.* AHIMA. **https://library.ahima.org/doc?oid=104090#.Ydlbpf5Bw2w**
9. *What is DES? Understanding DES algorithm and operation.* (2021, May 10). Simplilearn. **https://www.simplilearn.com/what-is-des-article#:~:text=The%20DES%20(Data%20Encryption%20Standard,ciphertext%20using%2048%2Dbit%20keys**

Video/Image Resources

1. edureka!. (2019, November 1). *What is brute force attack? | password cracking using brute force attacks/ edureka* [Video]. YouTube. **https://www.youtube.com/watch?v=fHsJAei2ocM&t=3s**
2. Istoria, A. (2020, June 18). *How did ancient Greeks send secret messages?* [Video]. YouTube. **https://www.youtube.com/watch?v=ac3l8J_rYNg**
3. Mental Outlaw. (2021, February 10). *How RSA encryption works* [video]. YouTube. **https://www.youtube.com/watch?v=ZPXVSJnDA_A**
4. Nasser, H. (2019, June 8). *Symmetrical vs asymmetrical encryption pros and cons by example* [Video]. YouTube. **https://www.youtube.com/watch?v=Z3FwixsBE94**
5. Network Direction. (2019, October 30). *Encryption basics | cryptography* [Video]. YouTube. **https://www.youtube.com/watch?v=V67drkkk2aA**
6. Professor Messer. (2014, September 21*). Symmetric vs. asymmetric encryption - compTIA security+ SY0-401: 6.1* [Video]. YouTube. **https://www.youtube.com/watch?v=z2aueocJE8Q**
7. Professor Messer. (2019, June 9). *brute force attacks - compTIA A+ 220-1002 - 2.5* [Video]. YouTube. **https://www.youtube.com/watch?v=W_NaKJrTmRk**
8. Turner, P. (2017, January 30). *PKI bootcamp - what is a PKI?* [Video]. YouTube. **https://www.youtube.com/watch?v=5OqgYSXWYQM**
9. Untitled illustration of WhatsApp Encryption. (2016). [Online image]. Indianexpress. **https://images.indianexpress.com/2016/04/whatsapp_encryption_1_new.jpg**

Discussion Assignment

It is commonly accepted that businesses use strong encryption for messaging and data protection. Is the same true for individuals?

- Discuss the advantages and disadvantages of using email encryption and digital signatures by individuals. What is your opinion about encryption dominating all aspects of communication in the future?
- Share your personal experience(s) related to encryption and/or use of digital certificates for personal signature (i.e. something like: https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512).
- Support your arguments with external research references.

Your Discussion should be a minimum of 200 words in length and not more than 500 words. Please include a word count. Following the APA standard, use references and in-text citations for the textbook and any other sources.

Resource:

Obtain a digital certificate and create a digital signature. (n.d.). In *support*. Microsoft. https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512

Written Assignment

Submit a paper that is 2-3 pages in length exclusive of the reference page, double-spaced using 12-point Times New Roman font. The paper must cite at least two (2) outside sources in APA format and be well-written. Check all content for grammar, spelling and be sure that you have correctly cited all resources (in APA format) used. Refer to the UoPeople APA Tutorials in the LRC for help with APA citations.

Cryptology has become an integral part of business operations around the world. Conduct online research to identify a minimum of 2 trends for the future application of cryptology.

- Choose what you think works best in your research.
- Provide a brief explanation of the mechanics of each selected cryptographic trend.
- Explain in your own words why you think they work best.
- Reinforce your arguments with appropriate quotes in the text and research references.

Written Assignment Peer Assessment

In the unit following the submission of your written assignment, you will peer assess three (3) of your classmates' assignments according to the instructions found in the Assessment Form. During this peer assessment period, you are expected to provide details in the feedback section of the Assessment Form, indicating why you awarded the grade that you did to your peer. The written assignment grade is comprised of a combination of your submission (90%) and your peer assessments (10%).

Written Assignment Peer Assessment Rubric

Learning Journal

The Learning Journal is a tool for self-reflection on the learning process. In addition to completing directed tasks, you should use the Learning Journal to document your activities, record problems you may have encountered, and draft answers for Discussion Forums and Assignments. The Learning Journal should be updated regularly (weekly), as your instructor will assess the learning journals as part of your Final Grade.

In this unit, we learned about various topics related to Encryption and Authentication. To reflect on what you have learned, answer each of the following questions:

- Describe what was the most interesting facts you learned about Encryption and Authentication. Give rationale to support your selection of the facts.
- List your plans for further exploration of Encryption and Authentication.

The Learning Journal entry should be a minimum of 500 words and not more than 750 words. Use APA citations and references if you use ideas from the readings or other sources. Refer to the UoPeople APA Tutorials in the LRC for help with APA citations.

Refer Learning Journal Rubrics

Self-Quiz

The Self-Quiz gives you an opportunity to self-assess your knowledge of what you have learned so far.

The results of the Self-Quiz do not count towards your final grade. However,the quiz is an important part of the University's learning process and it is expected that you will take it to ensure understanding of the materials presented. Reviewing and analyzing your results will help you perform better on future Graded Quizzes and the Final Exam.

Please access the Self-Quiz on the main course homepage; it is listed inside the Unit.

Checklist

- Peer assess Unit 3 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz