European IT Certification Curriculum
Self-Learning Preparatory Materials

EITC/IS/CCF

Classical Cryptography Fundamentals

This document constitutes European IT Certification curriculum self-learning preparatory material for the EITC/IS/CCF Classical Cryptography Fundamentals programme.

This self-learning preparatory material covers requirements of the corresponding EITC certification programme examination. It is intended to facilitate certification programme's participant learning and preparation towards the EITC/IS/CCF Classical Cryptography Fundamentals programme examination. The knowledge contained within the material is sufficient to pass the corresponding EITC certification examination in regard to relevant curriculum parts. The document specifies the knowledge and skills that participants of the EITC/IS/CCF Classical Cryptography Fundamentals certification programme should have in order to attain the corresponding EITC certificate.

Disclaimer

This document has been automatically generated and published based on the most recent updates of the EITC/IS/CCF Classical Cryptography Fundamentals certification programme curriculum as published on its relevant webpage, accessible at:

https://eitca.org/certification/eitc-is-ccf-classical-cryptography-fundamentals/

As such, despite every effort to make it complete and corresponding with the current EITC curriculum it may contain inaccuracies and incomplete sections, subject to ongoing updates and corrections directly on the EITC webpage. No warranty is given by EITCI as a publisher in regard to completeness of the information contained within the document and neither shall EITCI be responsible or liable for any errors, omissions, inaccuracies, losses or damages whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes in the document may be made by EITCI at its own discretion and at any time without notice, to maintain relevance of the self-learning material with the most current EITC curriculum. The self-learning preparatory material is provided by EITCI free of charge and does not constitute the paid certification service, the costs of which cover examination, certification and verification procedures, as well as related infrastructures.

© 2023 European IT Certification Institute, EITCI, Brussels, Belgium, EU
All rights reserved. The document or any part of it cannot be reproduced in any form except
as permitted by EITCI. Inquiries about permission to reproduce the document should be directed to EITCI.

TABLE OF CONTENTS

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: INTRODUCTION
TOPIC: INTRODUCTION TO CRYPTOGRAPHY

Cryptography is a fundamental aspect of cybersecurity that involves the use of mathematical algorithms to secure information. In this didactic material, we will explore the basics of classical cryptography, starting with an introduction to cryptography and its classification.

Cryptography can be classified into various categories based on its purpose and techniques. The classification helps us understand the different types of cryptographic systems and their applications. By studying these classifications, we can gain insights into how cryptography functions and how it can be used to protect sensitive information.

One of the primary classifications of cryptography is based on its purpose. This classification includes three main categories: confidentiality, integrity, and authentication. Confidentiality focuses on keeping information secure and hidden from unauthorized individuals. Integrity ensures that the information remains unaltered and intact during transmission. Authentication verifies the identity of the communicating parties, ensuring that they are who they claim to be.

Another classification of cryptography is based on the techniques used. This classification includes two main categories: symmetric cryptography and asymmetric cryptography. Symmetric cryptography, also known as secret-key cryptography, involves the use of a single key for both encryption and decryption. This key must be kept secret to maintain the confidentiality of the information. Asymmetric cryptography, on the other hand, uses a pair of keys: a public key for encryption and a private key for decryption. This technique allows for secure communication without the need for a shared secret key.

Understanding these classifications is crucial for comprehending the various cryptographic systems and their applications. By utilizing different techniques and purposes, cryptography plays a vital role in securing sensitive information in various domains, such as finance, healthcare, and communication.

Cryptography is a vital component of cybersecurity that ensures the confidentiality, integrity, and authentication of information. By classifying cryptography based on purpose and technique, we can better understand its applications and how it can be used to protect sensitive data.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: HISTORY OF CRYPTOGRAPHY
TOPIC: MODULAR ARITHMETIC AND HISTORICAL CIPHERS

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: STREAM CIPHERS
TOPIC: STREAM CIPHERS, RANDOM NUMBERS AND THE ONE-TIME PAD

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: STREAM CIPHERS
TOPIC: STREAM CIPHERS AND LINEAR FEEDBACK SHIFT REGISTERS

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: DES BLOCK CIPHER CRYPTOSYSTEM
TOPIC: DATA ENCRYPTION STANDARD (DES) - ENCRYPTION

In this lecture, we will be discussing block ciphers, specifically the Data Encryption Standard (DES). Block ciphers are cryptographic algorithms that operate on fixed-size blocks of data. Unlike stream ciphers, which encrypt data bit by bit, block ciphers encrypt data in fixed-size blocks.

Before we delve into DES, let's provide some context. Cryptography is a relatively young field, and it is important to understand its development in a broader context. DES was proposed in 1974 by IBM Research in Yorktown Heights, with input from the National Security Agency (NSA). At that time, cryptography was primarily used by intelligence services, and there were no widely adopted cryptographic standards in the public domain.

The significance of DES lies in the fact that it was the first encryption standard introduced by a major Western government, the United States. The U.S. government sought a secure cryptographic algorithm and IBM responded by developing DES. While the details of the algorithm were kept secret, the cipher itself was made public.

DES was designed to be a strong and secure encryption algorithm, and it became widely adopted in various applications. Its development marked a significant turning point in the history of cryptography, as it signaled a shift towards governments and organizations embracing encryption as a means to secure data.

Now, let's focus on the specifics of DES. It is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. DES operates on 64-bit blocks of data and uses a 56-bit key. The algorithm consists of several rounds of permutation, substitution, and transposition operations.

During encryption, the plaintext is divided into 64-bit blocks, and each block undergoes a series of transformations. These transformations involve substitution tables, known as S-boxes, which introduce non-linearity into the encryption process. The output of each round is fed into the next round, and after the final round, the ciphertext is obtained.

To decrypt the ciphertext, the process is reversed. The ciphertext is divided into 64-bit blocks, and each block undergoes the inverse transformations of the encryption process. After the final round, the original plaintext is recovered.

It is worth noting that DES has been widely used in practice, particularly in internet browsers and banking applications. However, due to advances in computing power, DES is no longer considered secure against modern attacks. As a result, it has been replaced by more robust encryption algorithms, such as the Advanced Encryption Standard (AES).

DES is a historic encryption algorithm that played a pivotal role in the development of cryptography. It was the first encryption standard introduced by a major Western government and paved the way for widespread adoption of encryption. While DES is no longer considered secure, its impact on the field of cryptography cannot be overstated.

The Data Encryption Standard (DES) is a block cipher cryptosystem that was widely used for more than 20 years, making it the best studied cipher in the world. While it was initially a standard for the US government, many commercial applications also adopted DES, making it the most popular cipher during that time. It is estimated that around 80 to 90 percent of real-world applications used DES.

DES was used in various applications, including passports and electronic identity cards. For example, the German passport and citizen card both utilized DES, specifically Triple DES, which is a more secure variant of DES. Triple DES involves encrypting the data three times in a row, providing a higher level of security.

Now, let's dive into how DES works. At a high level, DES is a simple encryption function. It takes in plaintext and a key, and produces ciphertext as output. DES operates on blocks of data, specifically 64 bits or 8 bytes at a time. This is different from stream ciphers, which encrypt individual bits. The length of the key used in DES is 56 bits.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

To build a block cipher like DES, we follow the principles defined by Claude Shannon, the inventor of information theory. Shannon identified two atomic operations that a good block cipher should perform. The first operation is called confusion, which obscures the relationship between plaintext and ciphertext. An example of confusion is a substitution table, where certain values are replaced with others.

The second operation is called diffusion, which ensures that changes in the plaintext result in multiple changes in the ciphertext. Diffusion spreads the influence of each bit throughout the ciphertext. This is achieved through operations like permutation and mixing of bits.

Building a block cipher involves combining these atomic operations in a way that provides both confusion and diffusion. The specific details of how to build a block cipher can be considered more of an art than a science. However, Shannon's principles serve as a guide for creating a secure and effective block cipher.

DES is a widely used block cipher cryptosystem that operates on 64-bit blocks of data. It was the most popular cipher for many years and found applications in various domains, including passports and identity cards. DES follows the principles of confusion and diffusion, as defined by Claude Shannon, to ensure the security of encrypted data.

A lookup table is a table with binary entries that is used in encryption. Each input selects a specific address in the table, and the corresponding output is obtained. This table is also known as a substitution table or a lookup table. Lookup tables are used in various encryption methods, such as the Caesar cipher and the substitution cipher.

However, lookup tables alone are not sufficient to create a strong cipher. Another important concept is diffusion, which involves spreading the influence of each plaintext bit over multiple ciphertext bits. One example of diffusion is permutation. By combining confusion (using lookup tables) and diffusion (such as permutation), a strong block cipher can be constructed.

To achieve this, the confusion and diffusion steps should be repeated multiple times. Starting with the plaintext, the confusion step (using a lookup table) is performed, followed by the diffusion step (such as permutation). This process is repeated multiple times until the final output, which is the deciphered text, is obtained. This construction principle is known as a product cipher.

The product cipher involves combining confusion and diffusion steps repeatedly to create a strong block cipher. It is important to note that this explanation is at a high-level and will be further elaborated in the upcoming sections.

Diffusion also occurs on the block cipher level. For example, if there is a single bit flip in the input, a good cipher will result in multiple bit flips in the output. This spreading effect is known as the avalanche effect or the diffusion property.

This was an introduction to the concept of diffusion and confusion in classical cryptography. The next chapter will delve into the details of the DES block cipher cryptosystem.

The DES block cipher cryptosystem, also known as Data Encryption Standard (DES), is a classical encryption algorithm that operates on a network of physical structures. While many modern ciphers are physical ciphers, not all ciphers fall into this category. The DES consists of 16 encryption rounds, each performing a specific encryption operation. This round-based cipher approach ensures that the encryption process incorporates both confusion and diffusion, as recommended by Claude Shannon.

In each encryption round, a specific operation is performed repeatedly. This can be visualized as a software flow diagram, where computations are performed, and the output is set back to the input. This process is repeated 16 times, ensuring a comprehensive encryption process.

To understand the inner workings of an encryption round, we need to examine its internal structure. By analyzing what happens inside one encryption round, we gain insight into how the entire cipher operates. One of the most exciting aspects of the DES is exploring the details of an encryption round.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

Within an encryption round, the data path is split into two parts: a 32-bit right part and a 32-bit left part. The right part is then passed through the crucial f function, which plays a significant role in the encryption process. This function, along with a subkey, forms the heart of the DES encryption. The output of the f function is combined with the left-hand side, and the two sides are then swapped, resulting in a new configuration: l1 r1.

Now, let's address an essential question regarding the encryption round: which half of the data is being encrypted? Some might assume that the right-hand side is being encrypted due to its involvement in the f function. However, this assumption is incorrect. In reality, the left-hand side is the part being encrypted in the round. While the right-hand side does pass through the f function, it remains unchanged and serves as a part of the diffusion process.

Understanding the encryption process in the DES block cipher cryptosystem is crucial for comprehending its overall functionality. By examining the inner workings of an encryption round, we gain valuable insights into the encryption process as a whole.

In classical cryptography, the Data Encryption Standard (DES) is a widely used block cipher cryptosystem. One of the fundamental operations in DES encryption is the XOR gate. XOR stands for exclusive OR, which is a logical operation that outputs true only when the number of true inputs is odd. In the context of DES, XOR is used to encrypt the input plaintext.

In the DES encryption process, the input plaintext is divided into 64-bit blocks. Each block goes through multiple rounds of encryption, where a subset of the bits in the block are XORed with a key. The result of this XOR operation is then passed through a function called the f function.

The f function takes a 32-bit input and a 48-bit key as its inputs. It performs various mathematical operations on these inputs, including permutations, substitutions, and XOR operations, to produce a 32-bit output. This output is then XORed with another subset of the bits in the block.

It is important to note that most of the lines in the DES encryption process are 32 bits long, except for one line called k1, which is 48 bits long. This discrepancy in bit length is addressed in the encryption process.

In the DES encryption process, only the left half of the block, denoted as l0, is encrypted using an XOR operation. The right half of the block, denoted as r0, remains unchanged. This means that the output of the encryption process, denoted as r1, is equal to r0.

The DES encryption process can be seen as similar to stream ciphers, where a pseudo-random key stream is XORed with the plaintext to produce the ciphertext. In each round of DES, the output of the f function can be viewed as a pseudo-random key stream, which is XORed with the plaintext.

To reverse the encryption process and decrypt the ciphertext, the same f function is used. The input to the f function remains the same, which is the key. However, an additional input, denoted as r0, is required. This input is obtained from the previous round of encryption, where r0 is equal to l1.

In order to decrypt the ciphertext and recover the original plaintext, the same f function is applied with the same key and the input r0. This allows us to reverse the XOR operation and obtain l0, which is the original plaintext.

The DES block cipher cryptosystem uses an XOR operation to encrypt the left half of the block, while the right half remains unchanged. The f function is used to generate a pseudo-random key stream, which is XORed with the plaintext. To decrypt the ciphertext, the same f function is applied with the same key and the input from the previous round of encryption.

The DES block cipher cryptosystem, which stands for Data Encryption Standard, is a fundamental encryption algorithm used in cybersecurity. In DES, encryption is achieved through a series of operations, including an initial permutation (IP), 16 rounds of encryption, and a final permutation (IP-1).

The initial permutation (IP) is the first step in the encryption process. It is a bit permutation that rearranges the input data, which is a 64-bit plaintext, into a different order. This permutation is also known as IP and is often abbreviated as such. The IP permutation is a simple bit permutation that involves copying specific bits from one

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

position to another. For example, bit 1 is copied to bit position 40, and bit 48 is copied to position 1. This process continues for all 64 bits, resulting in a rearranged input.

After the initial permutation, the encryption process proceeds through 16 rounds. Each round involves several operations, including a function called the f function. The f function generates a key stream, which is a crucial component of the encryption process. However, the details of the f function are not discussed in this lecture.

At the end of the 16 rounds, the final permutation (IP-1) is applied to the encrypted data. This permutation is the inverse of the initial permutation and rearranges the encrypted data back into its original order. The IP-1 permutation undoes the effects of the IP permutation, effectively decrypting the data.

It is important to note that the initial permutation and final permutation are necessary components of the DES encryption algorithm. The initial permutation rearranges the input data, while the final permutation restores the encrypted data back to its original order. These permutations play a crucial role in ensuring the security and effectiveness of the DES encryption process.

The DES block cipher cryptosystem uses an initial permutation, 16 rounds of encryption, and a final permutation to encrypt data. The initial permutation rearranges the input data, while the final permutation restores the encrypted data back to its original order. These permutations are essential for the proper functioning of the DES encryption algorithm.

The Data Encryption Standard (DES) is a block cipher cryptosystem that has been widely used in the field of classical cryptography since its development in 1974. One of the key components of DES is a permutation called the Initial Permutation (IP). The IP table, which consists of a simple permutation of bits, is publicly known and not kept secret.

Initially, it may seem counterintuitive to perform a permutation that is publicly known, as an attacker could easily reverse it if they have knowledge of the input and the permutation being applied. However, the reason for the inclusion of the IP permutation in DES becomes clear when considering the historical context.

During the early days of DES, Don Coppersmith, one of the original designers of the system, revealed that the inclusion of the IP permutation was primarily driven by practical electrical engineering reasons. At that time, there were challenges in efficiently transferring data to and from the chip used for DES. The built-in cross-wiring within the chip necessitated a certain permutation, which was incorporated into the specification of DES. It was never intended to enhance the security of the system.

It is worth noting that there are several anecdotes surrounding DES, one of which suggests that the National Security Agency (NSA) only allowed the use of DES in hardware, not software. This claim is unverified, but it is true that performing the IP permutation in hardware is much faster and simpler than in software. In hardware, the wiring required for the permutation can be implemented directly, without the need for complex computations. However, in software, the permutation has to be achieved through iterative operations, resulting in slower execution.

The assumption that the inclusion of the IP permutation in DES was a deliberate attempt by the NSA to slow down software implementations is not accurate. While it is true that the IP permutation adds a minor overhead to software execution, it does not significantly impact the overall speed of the algorithm. The DES algorithm consists of 32 permutations, including the IP permutation at the beginning and end, resulting in a total of 34 permutations. The difference between having 32 or 34 permutations is negligible in terms of performance.

The inclusion of the Initial Permutation (IP) in the DES block cipher cryptosystem was primarily driven by practical electrical engineering considerations rather than cryptographic security. The IP permutation, although publicly known, was necessary to address the specific challenges in data transfer within the chip used for DES. Its inclusion does not significantly impact the speed or security of the algorithm.

The Data Encryption Standard (DES) is a block cipher cryptosystem that is widely used in cybersecurity. In this didactic material, we will explore the fundamentals of DES encryption and focus on the details of the f function.

The f function is a crucial component of the DES encryption process. It takes as input the output of the previous round, which is denoted as ri-1, and expands it from 32 bits to 48 bits using the expansion box. The expansion

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

box adds confusion and diffusion to the encryption process. Confusion refers to making the relationship between the input and output bits complex, while diffusion ensures that a change in one input bit affects multiple output bits.

To understand the expansion box, we need to examine its inputs and outputs. The input to the expansion box is ri-1, a 32-bit value. The output is a 48-bit value. This expansion is achieved by applying a permutation to the input bits. The expansion box plays a critical role in increasing the complexity of the encryption process.

After the expansion box, the next step is to perform a key XOR operation. This involves XORing the expanded input with a subkey. The subkey is derived from the original encryption key and varies with each round of encryption. The key XOR operation adds another layer of complexity to the encryption process.

The most important part of the f function is the S-boxes. The S-boxes are substitution tables that replace groups of input bits with corresponding output bits. Each S-box takes in 6 bits and outputs 4 bits. There are a total of 8 S-boxes in the DES encryption process. The S-boxes introduce non-linearity to the encryption algorithm, making it more resistant to attacks.

Once the S-boxes have been applied, a bit permutation known as the permutation P is performed. The permutation P rearranges the bits to produce the final output of the f function, which is denoted as "out". The permutation P is a simple rearrangement of the bits and does not introduce any additional complexity to the encryption process.

The f function in the DES encryption process consists of several steps: expansion, key XOR, S-box substitution, and permutation. These steps are designed to add confusion and diffusion to the encryption process, making it more secure against attacks.

The DES block cipher cryptosystem, which stands for Data Encryption Standard, is a fundamental encryption algorithm used in cybersecurity. It is important to understand the key components of DES, including diffusion and confusion, to grasp its functionality.

Diffusion refers to the spreading of changes in the input across the entire output. In DES, a simple strategy is used to expand the input from 32 bits to 48 bits. This strategy involves connecting certain input bits to multiple output positions. For example, bit number one is connected to both bit number one and bit number 33. This expansion process ensures that the output contains 48 bits.

Confusion, on the other hand, involves the use of S-boxes (substitution boxes) in DES. S-boxes are lookup tables that take in six bits of input and produce four bits of output. The number of table locations required is determined by the number of input bits, which in this case is six. The S-boxes play a crucial role in providing confusion in DES.

To better understand the diffusion and confusion elements of DES, let's take a closer look at the expansion box and the S-boxes.

The expansion box takes in 32 bits of input and expands it to 48 bits. This expansion is achieved by connecting certain input bits to multiple output positions. Half of the input bits are connected once, while the other half are connected twice. This arrangement allows for the spreading of changes in the input across the output, facilitating diffusion.

The S-boxes, on the other hand, are lookup tables that perform substitution. They take in six bits of input and produce four bits of output. The number of S-boxes used in DES is eight, labeled as S1 to S8. Each S-box has a specific configuration, which determines the output bits based on the input bits. The S-boxes are the heart of DES, providing confusion by replacing input bits with output bits according to their configurations.

The DES block cipher cryptosystem employs both diffusion and confusion to ensure secure encryption. Diffusion is achieved through the expansion box, which spreads changes in the input across the output. Confusion is provided by the S-boxes, which perform substitution based on specific configurations.

The Data Encryption Standard (DES) is a widely used block cipher cryptosystem in classical cryptography. It is important for professionals in the field of cryptography to have a thorough understanding of DES and its

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

fundamental concepts.

One key aspect of DES is the use of a specific table, known as S-box, which plays a crucial role in the encryption process. The S-box can be viewed as a table with 64 entries, numbered from 1 to 64. Each entry corresponds to a specific output value based on a given input.

To illustrate this, let's consider a specific S-box, denoted as S1. If the input to S1 is all zeros, the output will be 1100, which is represented as the decimal number 12. Similarly, if the input is 63 (111111 in binary), the output will be 1101, which is the decimal number 13.

It is important to note that there is no specific rule governing the output values of the S-box. Each entry in the S-box is determined based on a predefined mapping, which is unique to each S-box. This mapping is what makes the S-box table a mystery and an essential part of DES.

The way the S-box table is presented may seem unusual at first. Instead of a simple list of 64 numbers, it is typically represented as a rectangle with 16 columns and 4 rows. Each entry in the table corresponds to a specific input configuration of 6 bits.

To determine the output value for a given input, we use a specific decoding method. The first 4 bits of the input select one of the 16 columns, while the last 2 bits select one of the 4 rows. This unconventional decoding method is different from what one might expect, where the first 4 bits select the column and the last 2 bits select the row.

For example, if we want to determine the S-box value for an input of 37, we first convert 37 to its binary representation: 100101. The middle 4 bits (0101) select the column, which corresponds to the binary number 2. The outer bits (10) select the row. Therefore, the S-box value for an input of 37 is the entry located at the intersection of column 2 and row 2.

Understanding the S-box and its decoding method is crucial for properly implementing DES and ensuring the security of encrypted data.

The Data Encryption Standard (DES) is a block cipher cryptosystem that was widely used for secure communication and data protection. It was proposed by IBM in the 1970s and became a standard in 1977. DES operates on 64-bit blocks of data and uses a 56-bit key for encryption.

One important component of DES is the Feistel network, which is a structure that allows for the encryption and decryption of data. The Feistel network consists of multiple rounds, each of which involves an initial permutation, an encryption function, and a final permutation. The encryption function, also known as the "F function," is applied to a subset of the data and the result is combined with the other subset using XOR operation.

During the development of DES, one of the main concerns was the selection of the S-boxes, which are lookup tables used in the encryption function. There are eight S-boxes in total, each with a different permutation of the input bits. The motivation behind the specific choice of these tables was not initially disclosed by IBM. This led to speculation and concerns about the security of DES, with some people suspecting the involvement of the NSA in the design process.

In the 1980s, as the field of cryptography gained popularity, researchers started attempting to break DES. It was widely believed that if someone could find a way to break DES, they would become famous and be rewarded. However, breaking DES proved to be a difficult task, and it wasn't until 1990 that two researchers, Adi Shamir and Eli Biham, discovered a technique called differential cryptanalysis that could be used to break DES.

Differential cryptanalysis exploits the structure of the S-boxes to analyze the differences in the output when small changes are made to the input. This attack heavily depends on the construction of the S-boxes and how they are filled. The discovery of this attack was a significant event in the field of symmetric cryptography and led to further research and improvements in encryption algorithms.

DES is a block cipher cryptosystem that uses a Feistel network structure and S-boxes for encryption. Its development and the selection of the S-boxes raised concerns about the security of the algorithm. Differential

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

cryptanalysis, discovered in 1990, provided a way to break DES by exploiting the structure of the S-boxes. This breakthrough had a significant impact on the field of symmetric cryptography and led to further advancements in encryption algorithms.

The Data Encryption Standard (DES) is a block cipher cryptosystem that was developed in the 1970s by IBM and the National Security Agency (NSA). It was widely used for many years and played a significant role in securing sensitive information.

However, it was later discovered that DES was vulnerable to a powerful attack known as differential cryptanalysis. This attack was actually known to the IBM team and the NSA about 18 years before it became public knowledge. The reason they did not disclose this attack to the public was because it was a highly effective tool for breaking Russian ciphers during the Cold War.

The attack exploited the structure of DES, particularly the S-boxes, which were designed to be resistant to differential cryptanalysis. These anti-differential cryptanalysis S-boxes ensured that the attack did not succeed against DES.

To understand the attack, let's take a closer look at the F function in DES. At the end of this function, there is a final permutation that is essentially a cross-wiring of the 32 input bits to the 32 output bits. This permutation ensures that any change in a single input bit results in a diffusion effect, where multiple output bits change.

To illustrate this diffusion effect, let's consider a scenario where all 32 input bits are initially set to zero. When these bits are passed through the F function, they produce a certain output. Now, if we flip one of the input bits, let's say the first bit, what happens at the output?

When a single input bit flips, there is a 50% chance that either one or two output bits will flip. This is due to the nature of the XOR gate, which flips its output bit whenever there is a change in its input bits, regardless of the value of the key bit. So, in this case, if the first bit flips from zero to one, the output of the XOR gate will definitely flip.

Next, the input is passed through the S-boxes. These S-boxes have the property that if one input bit flips, at least two output bits will flip. So, when the one bit flip reaches the S-boxes, it is guaranteed that at least two output bits will change.

At this point, the changes may seem localized, but the permutation box (P-box) ensures that these changes are spread out across the output. The P-box rearranges the bits in a way that ensures the changes are not concentrated in a specific region.

This diffusion effect, where a single bit flip results in multiple changes throughout the output, is a crucial aspect of DES's security. It ensures that even a small change in the input will lead to significant changes in the output, making it difficult for an attacker to deduce any meaningful information.

DES was a widely used block cipher cryptosystem that was secure against the powerful differential cryptanalysis attack. The structure of DES, including the S-boxes and the permutation box, ensured that any changes in the input resulted in significant changes in the output, making it difficult to break the encryption.

The Data Encryption Standard (DES) is a block cipher cryptosystem widely used for secure data encryption. In this system, the encryption process involves multiple rounds of operations, each consisting of several steps.

During each round, a key is applied to the input data, which is divided into blocks. One of the key steps in the encryption process is the E-box, where one bit changes can result in at least two bits changing in the subsequent round. This occurs when a bit in the E-box is connected to two output bits. Consequently, the likelihood of obtaining a bit connected to two output bits increases as the rounds progress.

Even if only two bits change in the E-box, the next round will involve two S-boxes. This means that at least four bits will be different in the subsequent round. The permutation step ensures that these four bits are spread across the data pairs. In the subsequent round, multiple S-boxes are activated, which further increases the number of active bits.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

This phenomenon is known as the avalanche effect, which is a metric used to measure the effectiveness of a block cipher. After approximately six to eight rounds, if a single bit is flipped in the input, the entire data path is affected. This demonstrates the strength of DES in quickly propagating changes throughout the encryption process.

The DES block cipher cryptosystem employs multiple rounds of operations to encrypt data. The E-box and S-boxes play crucial roles in introducing changes and spreading them across the data. The avalanche effect ensures that even a single bit flip can have a significant impact on the entire encryption process.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: DES BLOCK CIPHER CRYPTOSYSTEM
TOPIC: DATA ENCRYPTION STANDARD (DES) - KEY SCHEDULE AND DECRYPTION

The Data Encryption Standard (DES) is a block cipher cryptosystem that was widely used for secure communication in the past. In this didactic material, we will focus on the key schedule and decryption process of DES.

The key schedule in DES is responsible for generating the subkeys used in each round of encryption and decryption. It starts with a 64-bit key, but only 56 bits are used, with the remaining 8 bits being used for parity checks. The key is then subjected to a permutation and compression process to generate the 16 subkeys, each consisting of 48 bits.

During decryption, the subkeys are used in reverse order compared to encryption. This means that the last subkey used in encryption becomes the first subkey used in decryption, and so on. The decryption process itself is similar to encryption, with the main difference being the use of the subkeys in reverse order.

To decrypt a ciphertext, it is divided into 64-bit blocks. Each block undergoes an initial permutation, similar to encryption. Then, the 16 rounds of DES are applied, using the subkeys in reverse order. In each round, the block is subjected to a combination of permutation, substitution, and XOR operations. Finally, the block goes through a final permutation, which is the inverse of the initial permutation, resulting in the plaintext.

It is worth noting that DES has been replaced by more secure encryption algorithms due to advances in computing power and cryptanalysis. However, understanding the fundamentals of DES is still valuable for learning about classical cryptography and the historical development of encryption techniques.

The key schedule and decryption process are important components of the DES block cipher cryptosystem. The key schedule generates the subkeys used in each round, while decryption involves applying the rounds in reverse order using the subkeys. Although DES is no longer considered secure for modern applications, studying its fundamentals helps in understanding the evolution of encryption algorithms.

The Data Encryption Standard (DES) is a classical block cipher cryptosystem used for data encryption. In this didactic material, we will discuss the key schedule and decryption process of DES.

The key schedule is an important part of the DES algorithm. It takes the original encryption key and generates 16 different subkeys, each used in a specific round of encryption. The key schedule begins by permuting the original 64-bit key to generate a 56-bit key. This 56-bit key is then split into two 28-bit halves. In each round, these halves are shifted left by either one or two positions, depending on the round number. After the shifts, a permutation is applied to the 56-bit key to generate the subkey for that round.

During decryption, the subkeys are used in reverse order. The last subkey used in encryption becomes the first subkey used in decryption, and so on. The decryption process is similar to encryption, but the subkeys are applied in reverse order. Each round of decryption involves the use of a different subkey, derived from the key schedule.

To illustrate the key schedule and decryption process, let's consider an example. Suppose we have an original encryption key of 64 bits. The key schedule generates 16 subkeys, each of 48 bits, based on this original key. During decryption, these subkeys are used in reverse order to decrypt the ciphertext.

It is important to note that DES has been replaced by more secure encryption algorithms due to its vulnerability to brute force attacks. However, understanding the key schedule and decryption process of DES is still valuable for learning about classical cryptography and the evolution of encryption algorithms.

The key schedule and decryption process are crucial components of the DES block cipher cryptosystem. The key schedule generates subkeys that are used in each round of encryption, and during decryption, these subkeys are applied in reverse order. While DES is no longer considered secure, studying its fundamentals helps in understanding the evolution of encryption algorithms.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

The Data Encryption Standard (DES) is a classical block cipher cryptosystem that was widely used for secure communication in the past. In this didactic material, we will focus on the key schedule and decryption process of DES.

The key schedule in DES involves generating 16 subkeys from the original 64-bit encryption key. Each subkey is 48 bits long and is derived through a combination of permutation and rotation operations. These subkeys are used in the subsequent encryption and decryption rounds.

During the decryption process, the ciphertext is fed into the DES algorithm along with the 16 subkeys in reverse order. Each round of decryption is similar to the encryption process but with the subkeys used in reverse order. This ensures that the original plaintext is obtained from the ciphertext.

It is important to note that DES has a block size of 64 bits, meaning that it operates on blocks of 64 bits at a time. If the plaintext is not a multiple of 64 bits, padding is added to make it compatible with the block size.

DES has been widely studied and analyzed for its security. It is known that DES is vulnerable to brute-force attacks due to its relatively small key size of 56 bits. However, DES can still be used securely in certain contexts, such as when combined with other cryptographic techniques or when used for legacy systems.

In recent years, DES has been largely replaced by more secure and efficient encryption algorithms, such as the Advanced Encryption Standard (AES). AES provides a higher level of security and has become the de facto standard for secure communication.

The key schedule and decryption process are important components of the DES block cipher cryptosystem. Understanding these fundamental concepts is crucial for comprehending the inner workings of DES and its role in classical cryptography.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: AES BLOCK CIPHER CRYPTOSYSTEM
TOPIC: INTRODUCTION TO GALOIS FIELDS FOR THE AES

The topic of this didactic material is the introduction to Galois Fields for the AES block cipher cryptosystem. Galois Fields, also known as finite fields, play a crucial role in the implementation of the Advanced Encryption Standard (AES), which is one of the most widely used block ciphers in the world.

In order to understand Galois Fields, it is important to have a basic understanding of classical cryptography and the AES block cipher cryptosystem. Classical cryptography refers to the encryption methods used before the advent of modern computer-based encryption algorithms. The AES block cipher cryptosystem is a symmetric encryption algorithm that operates on fixed-size blocks of data. It uses a series of mathematical operations, including Galois Fields, to encrypt and decrypt data.

Galois Fields are mathematical structures that have properties similar to those of ordinary arithmetic, but with a finite number of elements. They are widely used in cryptography because they provide a way to perform arithmetic operations on binary data efficiently. In the context of the AES block cipher cryptosystem, Galois Fields are used to perform operations on the data blocks during the encryption and decryption processes.

One important concept in Galois Fields is the notion of a prime field. A prime field is a Galois Field that has a prime number of elements. In the case of the AES block cipher cryptosystem, the prime field used is GF(2^8), which has 256 elements. This means that each element in the field can be represented by an 8-bit binary number.

Another important concept in Galois Fields is the notion of field operations. Field operations, such as addition and multiplication, are defined in such a way that they satisfy certain properties, such as closure, associativity, commutativity, and distributivity. These properties ensure that the operations can be performed consistently and efficiently.

In the context of the AES block cipher cryptosystem, Galois Fields are used to perform operations on the data blocks during the encryption and decryption processes. For example, the AES algorithm uses a special kind of Galois Field multiplication, called the AES MixColumns operation, to mix the columns of the data blocks. This operation provides diffusion and confusion, which are important properties for achieving strong encryption.

Galois Fields are a fundamental concept in the implementation of the AES block cipher cryptosystem. They provide a way to perform arithmetic operations on binary data efficiently and are used to perform operations on the data blocks during the encryption and decryption processes. Understanding Galois Fields is essential for understanding the inner workings of the AES algorithm and for gaining a deeper understanding of modern cryptographic systems.

In the field of cybersecurity, classical cryptography plays a crucial role in ensuring the security and confidentiality of sensitive information. One of the fundamental concepts in classical cryptography is the AES block cipher cryptosystem. In order to understand the AES cryptosystem, it is important to have a basic knowledge of Galois Fields.

Galois Fields, also known as finite fields, are mathematical structures that play a significant role in modern cryptography. They provide a foundation for various cryptographic algorithms, including the AES cryptosystem. Galois Fields are finite sets of elements with defined addition and multiplication operations.

In the context of the AES cryptosystem, Galois Fields are used to perform mathematical operations on the plaintext and the encryption key. The AES algorithm operates on 128-bit blocks of data, which are represented as elements of a Galois Field with 2^8 elements. This means that each element in the Galois Field can be represented by an 8-bit binary number.

The addition operation in the Galois Field is performed using bitwise XOR, which is a binary operation that returns true if the bits being compared are different, and false if they are the same. The multiplication operation, on the other hand, is performed using a polynomial multiplication algorithm called the Galois Field multiplication.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

The Galois Field multiplication is based on the concept of irreducible polynomials, which are polynomials that cannot be factored into lower degree polynomials. In the AES cryptosystem, a specific irreducible polynomial is used to define the Galois Field multiplication. This irreducible polynomial is denoted as AES polynomial and has the form x^8 + x^4 + x^3 + x + 1.

By performing addition and multiplication operations in the Galois Field, the AES algorithm achieves confusion and diffusion, which are two essential properties of a secure encryption algorithm. Confusion ensures that the relationship between the plaintext and the ciphertext is complex and difficult to decipher. Diffusion ensures that a change in one bit of the plaintext affects multiple bits in the ciphertext.

Galois Fields are a fundamental concept in the AES block cipher cryptosystem. They provide a mathematical framework for performing operations on the plaintext and the encryption key. By utilizing the properties of Galois Fields, the AES algorithm achieves a high level of security and confidentiality in encrypting sensitive information.

Classical Cryptography Fundamentals - AES Block Cipher Cryptosystem - Introduction to Galois Fields for the AES

In the field of cybersecurity, classical cryptography plays a significant role in ensuring the confidentiality and integrity of sensitive information. One of the most widely used encryption algorithms is the Advanced Encryption Standard (AES) block cipher cryptosystem. To fully understand AES, it is essential to have a solid understanding of Galois Fields.

Galois Fields, also known as finite fields, are mathematical structures that form the foundation for AES. They are sets of elements with specific properties that allow for operations such as addition, subtraction, multiplication, and division. In the context of AES, the Galois Field used is GF(2^8), which consists of 256 elements.

AES operates on blocks of data, with each block containing 128 bits. These blocks are divided into four columns and four rows, forming a 4x4 matrix. The elements of this matrix are bytes, which can be represented as polynomials over GF(2^8).

In GF(2^8), addition and subtraction are performed using the bitwise XOR operation. Multiplication, on the other hand, is more complex. It involves multiplying two polynomials and reducing the result modulo an irreducible polynomial. The irreducible polynomial used in AES is x^8 + x^4 + x^3 + x + 1.

To better understand the operations in GF(2^8), let's consider an example. Suppose we have two bytes, A and B, represented as polynomials a(x) and b(x) respectively. The multiplication of A and B in GF(2^8) can be computed as follows:

1. Multiply a(x) and b(x) using standard polynomial multiplication.
2. Reduce the result modulo the irreducible polynomial x^8 + x^4 + x^3 + x + 1.

This process ensures that the result of the multiplication is within the field GF(2^8).

In addition to multiplication, AES also utilizes a substitution operation called the S-box. The S-box is a lookup table that replaces each byte in the 4x4 matrix with a corresponding byte from a predefined table. This substitution operation adds an extra layer of security to the AES algorithm.

Galois Fields are fundamental to the AES block cipher cryptosystem. They provide the mathematical framework for performing operations on the data blocks used in AES encryption. Understanding Galois Fields is crucial for comprehending the inner workings of AES and its role in ensuring secure communication and data protection.

In the field of cybersecurity, classical cryptography plays a crucial role in ensuring the security of data and communications. One important cryptographic algorithm is the Advanced Encryption Standard (AES) block cipher cryptosystem. In order to understand AES, it is necessary to have a basic understanding of Galois Fields.

Galois Fields, also known as finite fields, are mathematical structures that have properties similar to the real numbers but with a finite number of elements. They are used in AES to perform operations such as addition and

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

multiplication on the binary representation of data.

The AES block cipher operates on 128-bit blocks of data and uses a key of either 128, 192, or 256 bits. The algorithm consists of several rounds, each of which performs a series of operations on the data and the key. These operations include substitution, permutation, and linear transformations.

In AES, the substitution step is performed using a substitution box (S-box) that replaces each byte of the input with a corresponding byte from a predefined table. The S-box is constructed using a combination of mathematical operations, including the use of Galois Fields.

Galois Fields are particularly useful in AES because they allow for efficient and secure computation of the S-box. The S-box is designed to have certain cryptographic properties, such as non-linearity and resistance to differential and linear attacks. These properties are achieved through the use of Galois Fields and other mathematical techniques.

In addition to the S-box, Galois Fields are also used in other parts of the AES algorithm, such as the key expansion and the mix-columns step. The mix-columns step involves multiplying each column of the data matrix by a fixed matrix, which is constructed using elements from a Galois Field.

Galois Fields are a fundamental concept in the AES block cipher cryptosystem. They provide a mathematical framework for performing secure and efficient operations on data and keys. By understanding Galois Fields, one can gain a deeper insight into the inner workings of AES and the principles behind its cryptographic strength.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: AES BLOCK CIPHER CRYPTOSYSTEM
TOPIC: ADVANCED ENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES) is a block cipher cryptosystem widely used in cybersecurity. It was developed by the National Institute of Standards and Technology (NIST) in the early 2000s and has become the standard encryption algorithm for securing sensitive data.

AES operates on fixed-size blocks of data, typically 128 bits in length. It uses a symmetric key, meaning the same key is used for both encryption and decryption. The key length can be 128, 192, or 256 bits, depending on the desired level of security.

The AES algorithm consists of several rounds of substitution, permutation, and mixing operations. These operations are performed on the input data using a series of mathematical transformations. The result is a ciphertext that is difficult to decipher without knowledge of the key.

One of the key strengths of AES is its resistance to various types of attacks. It has been extensively analyzed by cryptographers and has withstood rigorous testing. AES has been proven to be secure against known cryptographic attacks, making it a reliable choice for protecting sensitive information.

AES has wide-ranging applications in areas such as secure communication, data storage, and financial transactions. It is used by governments, organizations, and individuals around the world to safeguard their data and ensure privacy.

The Advanced Encryption Standard (AES) is a robust and widely adopted block cipher cryptosystem used in cybersecurity. Its strength lies in its resistance to attacks and its versatility in securing various types of data. By implementing AES, organizations and individuals can protect their sensitive information and maintain confidentiality.

The Advanced Encryption Standard (AES) is a widely used block cipher cryptosystem in the field of cybersecurity. It is important to understand the fundamentals of classical cryptography and how AES works to ensure secure data transmission and storage.

AES operates on fixed-size blocks of data and uses a symmetric key algorithm, meaning the same key is used for both encryption and decryption. The key length can be 128, 192, or 256 bits, depending on the security requirements.

The AES algorithm consists of several rounds of transformations, including substitution, permutation, and mixing of data. These operations are designed to provide confusion and diffusion, making it difficult for an attacker to decipher the encrypted message without the correct key.

During the encryption process, the input data is divided into blocks and undergoes a series of transformations. The key expansion process generates a set of round keys based on the original encryption key. Each round of AES encryption involves substitution, permutation, and mixing operations, which are applied to the data using the corresponding round key.

The substitution step involves replacing each byte of data with a corresponding value from a substitution table. This table, known as the S-box, is constructed using a mathematical function that ensures each input byte is mapped to a unique output byte. This non-linear substitution provides confusion in the encryption process.

The permutation step, known as the shift rows operation, rearranges the bytes within each row of the data block. This diffusion ensures that changes in one byte affect multiple bytes in subsequent rounds, spreading the influence of each byte throughout the block.

The mixing step, known as the mix columns operation, applies a linear transformation to each column of the data block. This mixing operation further increases the diffusion and makes it difficult to extract information about the original data.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

After completing the specified number of rounds, the final encrypted data is obtained. To decrypt the data, the same AES algorithm is applied in reverse, using the round keys in the opposite order.

AES has become the standard encryption algorithm for a wide range of applications, including secure communication protocols, file encryption, and data storage. Its strength lies in its resistance to various cryptographic attacks, such as differential and linear cryptanalysis.

Understanding the fundamentals of classical cryptography and the workings of the AES block cipher cryptosystem is crucial for ensuring secure data transmission and storage. AES provides a robust and widely adopted encryption solution, offering confidentiality and integrity for sensitive information.

The Advanced Encryption Standard (AES) is a widely used block cipher cryptosystem in the field of cybersecurity. It is considered one of the most secure symmetric encryption algorithms available today.

AES operates on fixed-size blocks of data, with a block size of 128 bits. The input to the AES algorithm is divided into blocks, and each block undergoes a series of transformations. These transformations include substitution, permutation, and mixing of the data.

The AES algorithm consists of several rounds, with the number of rounds depending on the key size. For a 128-bit key, AES uses 10 rounds, for a 192-bit key, AES uses 12 rounds, and for a 256-bit key, AES uses 14 rounds.

During each round, the input block is subjected to four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The SubBytes operation substitutes each byte of the input block with a corresponding byte from a substitution box. The ShiftRows operation shifts the bytes in each row of the input block. The MixColumns operation mixes the columns of the input block. And the AddRoundKey operation XORs the input block with a round key derived from the original key.

The AES algorithm provides a high level of security due to its key size and the number of rounds. It is resistant to various cryptographic attacks, including brute-force attacks and differential attacks. Additionally, AES has been extensively analyzed and tested by the cryptographic community, further validating its security.

The Advanced Encryption Standard (AES) is a block cipher cryptosystem widely used in cybersecurity. It operates on fixed-size blocks of data and employs a series of transformations during each round. AES provides a high level of security and is resistant to various cryptographic attacks.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: APPLICATIONS OF BLOCK CIPHERS
TOPIC: MODES OF OPERATION FOR BLOCK CIPHERS

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: CONCLUSIONS FOR PRIVATE-KEY CRYPTOGRAPHY
TOPIC: MULTIPLE ENCRYPTION AND BRUTE-FORCE ATTACKS

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: INTRODUCTION TO PUBLIC-KEY CRYPTOGRAPHY
TOPIC: NUMBER THEORY FOR PKC - EUCLIDEAN ALGORITHM, EULER'S PHI FUNCTION AND EULER'S THEOREM

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union

EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS DIDACTIC MATERIALS
LESSON: INTRODUCTION TO PUBLIC-KEY CRYPTOGRAPHY
TOPIC: THE RSA CRYPTOSYSTEM AND EFFICIENT EXPONENTIATION

This part of the material is currently undergoing an update and will be republished shortly.

© 2023 European IT Certification Institute
EITCI, Brussels, Belgium, European Union