



Romel Cabiling ▾



Home

Home > My courses > 121 - ITSP2B > 08 Deep Diving into Cryptography: Types of Cipher > Lesson Proper for Week 8

Lesson Proper for Week 8

TYPES OF CIPHER

What is a cipher? To put it simply, a cipher is the method in which data is converted from plaintext to cipher text format. In cryptography, there are many different methods. Each method is known as a cipher suite and has its own advantages and disadvantages. In this section, we'll discuss the different types of ciphers used to encode and decode messages.

1. Substitution Cipher

In a substitution cipher, also known as a **Caesar Cipher**, the secret key is the replacement of certain or all of the plaintext with another character, thus creating the cipher text. For example, let's say you are writing the sentence, "the quick brown fox jumps over the lazy dog." We, as humans, will see it in its natural form, plaintext. If we were to use a key such as A=Z, B=Y, C=X and so on, we would have the following:

Normal Sequence	A	B	C	D	E	F	G	H	I	J	K	L	M
Key	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Normal Sequence	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key	M	L	K	J	I	H	G	F	E	D	C	B	A

If we encrypt the message: the quick brown fox jumps over the lazy dog, the ciphertext will result in: gsv jfrxp yildm ulc qfnkh levi gsv ozab wlt. Reversing the ciphertext using the preceding chart will result in the plaintext.

2. Transposition Cipher

A transposition cipher simply manipulates the order or sequence of the message instead of trying to hide the message itself. There are many different transposition methods, one of which is known as columnar transposition. This variation uses the words of the message without spaces, where the width of the column itself is a fixed size.



if there are any spaces remaining at the end of the last row, random characters are added to ensure the rows and columns are equal.

An example of columnar transposition while using the message *the quick brown fox jumps over the lazy dog* would result in the following: thequi

ckbrow

nfoxju

mpsove

rthela

zydogz

Another version of a transposition cipher is the rail fence cipher. This version hides some of the characters of a message. Once again, we'll use the *sentence the quick brown fox jumps over the lazy dog* to demonstrate how the rail fence cipher works. The following is the result of the rail fence cipher: t . . . u . . . b . . . n . . . j . . . s . . . r . . . l . . . d . .

Notice that there is a consistent thread where three characters are missing and there are no spaces between words. Each period (.) represents that a character is missing.

3. Block Ciphers

Block ciphers encrypt a fixed size (block) of data at a time. If you're sending a message and your computer is using a block cipher encryption algorithm, it would create blocks of a fixed size such as 64-bits or even 128-bits and encrypt all the data inside each block. Some examples of block cipher algorithms are: Data Encryption Standard, Triple Data Encryption Standard, and Advanced Encryption Standard, to name just a few.

4. Stream Ciphers

In a stream cipher, the algorithm encrypts each bit individually, therefore creating a continuous stream. An example of a stream cipher encryption algorithm is the **Rivest Cipher 4 (RC4)** cipher suite.

5. Key

A key, also referred to as the secret or even the secret key, is used to reorder the contents of a cipher text back to its original form. A simple analogy we can use is a room with a single deadbolt lock. To secure the contents of the room, we would need to lock the door using a specific key. This would be considered to be the encryption aspect. Once the room is locked, only people with the appropriate key can unlock the room to view its contents. This would be considered decryption.



ENCRYPTION ALGORITHMS

Furthering our discussion, we will dive a little bit deeper into understanding the different algorithms and how they are used to provide confidentiality.

1. Data Encryption Standard

The **Data Encryption Standard (DES)** is a symmetric encryption algorithm which uses the same key to both encrypt and decrypt data. It does this by encrypting a block of 64-bits in size using a 56-bit key. The size of the key makes a difference in the strength of the encryption itself; in this case, a 56-bit key is used per block. The smaller the key, the weaker and more vulnerable the encryption/algorithm is to being deciphered by a hacker.

2. Triple Data Encryption Standard (3DES)

The successor to the DES algorithm is the Triple DES (3DES), and this upgrade applies the DES three times to messages. The 3DES algorithm uses key sizes of 56-bits, 112-bits, and 168-bits, respectively. However, the block size still remains the same, 56-bits. To further explain how 3DES works, it uses a key to encrypt the plaintext, and the result will be ciphertext1, which is round 1. Next, it takes ciphertext1 and applies the algorithm again, resulting in ciphertext2; this is round 2. Once more, it runs the algorithm but on ciphertext2, giving the output as ciphertext3; this is the third round. The final output of the entire 3DES algorithm is ciphertext3.

3. Advanced Encryption Standard

The **Advanced Encryption Standard (AES)** has become the de facto for symmetric encryption standards due to its very strong encryption key sizes and its ability to encrypt large blocks of data at a time. AES uses various key sizes, and they are: 128-bits, 192-bits, and 256-bits, and the block size is 128-bits.

◀ Preliminary Activity for Week 8

Jump to...



Analysis, Application, and Exploration for Week 8 ▶



Navigation

Home

 Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103



121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants

 Grades

General

01 Exploring Security Threats

02 Delving into Security Toolkits

03 Intrusion Prevention System

04 Understanding Security Policies I

05 Understanding Security Policies II


06 - Preliminary Examination


07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

 Preliminary Activity for Week 8

 **Lesson Proper for Week 8**

 Analysis, Application, and Exploration for Week 8

 Generalization for Week 8

 Evaluation for Week 8

 Assignment for Week 8

09 Implementing the AAA Framework

10 Implementing the AAA Framework: Implementing A...

11 Securing the Control and Management Planes

12 - Midterm Examination

13 Protecting Layer 2 Protocols

14 Protecting the Switch Infrastructure

15 Exploring Firewall Technologies I

16 Exploring Firewall Technologies II

17 Cisco ASA

121 - WEB101 / CCS3218

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***



PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment



visit www.bcp.edu.ph

Enrollment registration is now Ongoing





For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.

"Be trained to be the best,
Be linked to success"

 bcp-inquire@bcp.edu.ph  (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources



