Instructor Materials Chapter 5: The Art of Ensuring Integrity

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5: The Art of Ensuring Integrity

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5 - Sections & Objectives

5.1 Types of Data Integrity Controls

Explain the processes used to ensure integrity.

5.2 Digital Signatures

Explain the purpose of digital signatures.

5.3 Certificates

Explain the purpose of digital certificates.

5.4 Database Integrity Enforcement

Explain the need for database integrity enforcement.

5.1 Types of Data Integrity Controls

Cisco | Networking Academy®
Mind Wide Open™

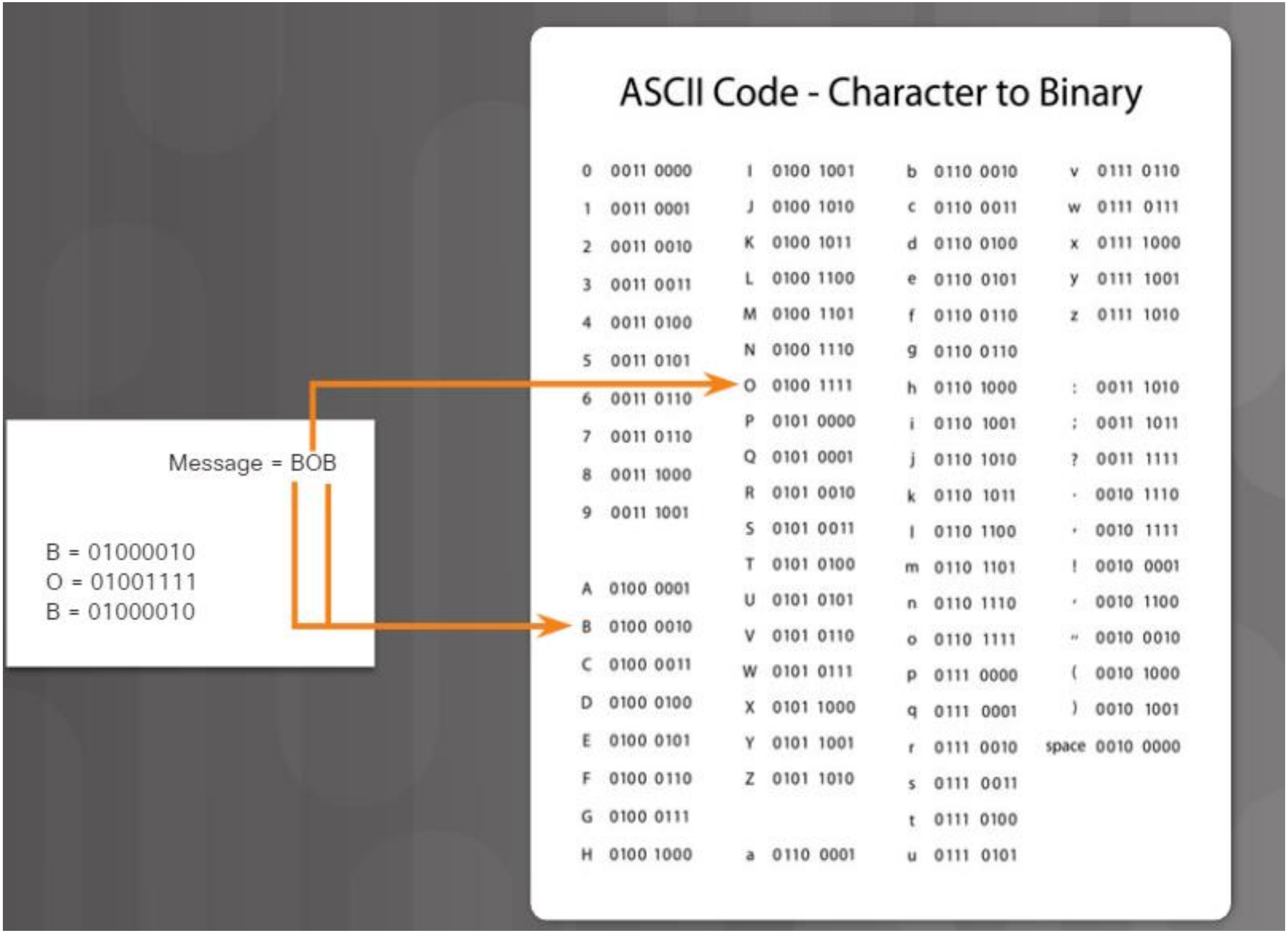
Types of Data Integrity Controls

Hashing Algorithms

- Hashing is a tool that ensures data integrity by taking binary data (the message) and producing a fixed-length representation called the hash value or message digest.
- Hashing is a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse. Grinding coffee beans is a good analogy of a one-way function. It is easy to grind coffee beans, but it is almost impossible to put all of the tiny pieces back together to rebuild the original beans.

  A cryptographic hash function has the following properties:

  - The input can be any length.
  - The output has a fixed length.
  - The hash function is one way and is not reversible.
  - Two different input values will always result in different hash values.



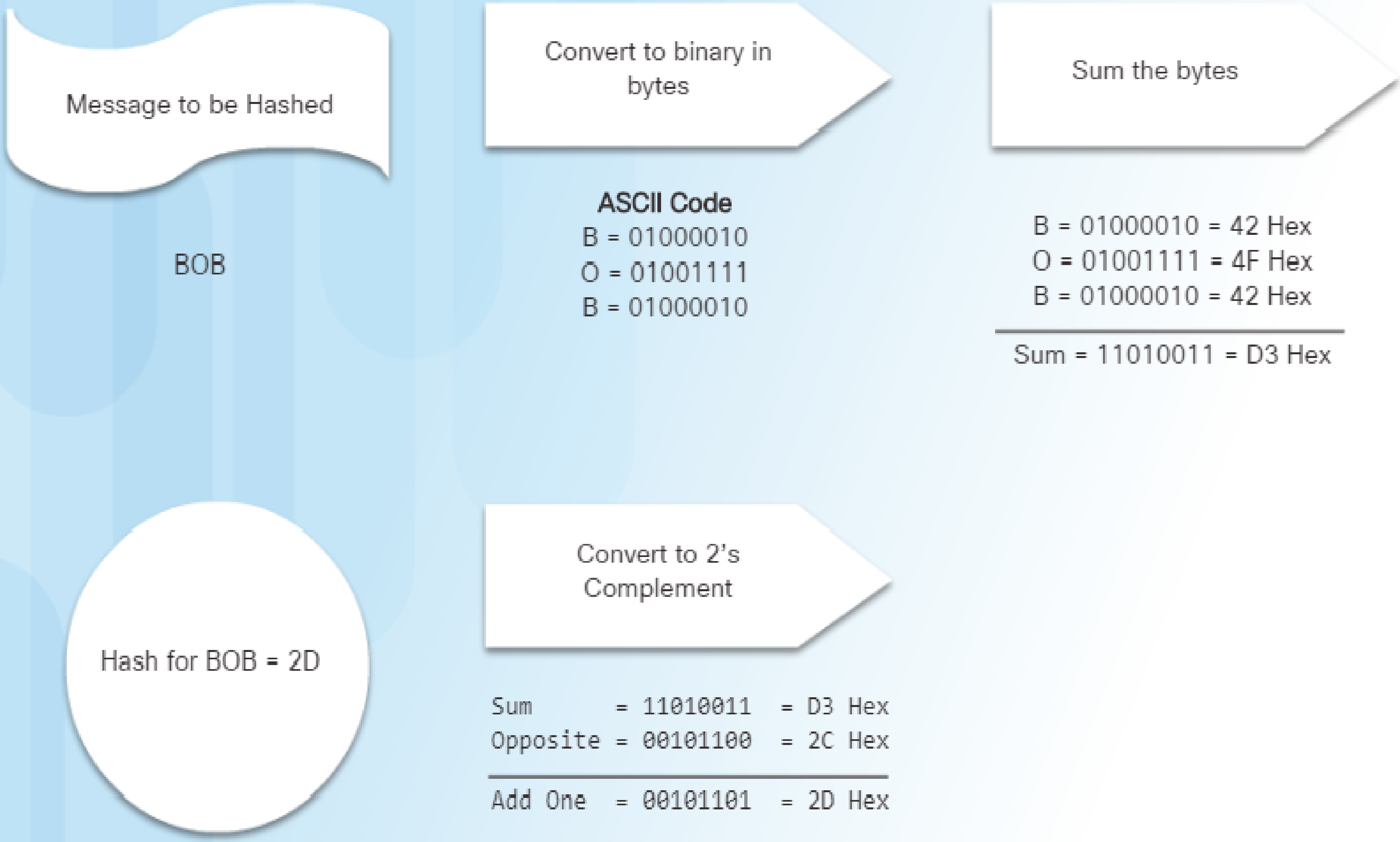
Message = BOB

B = 01000010
O = 01001111
B = 01000010

ASCII Code - Character to Binary

0	0011 0000	I	0100 1001	b	0110 0010	v	0111 0110
1	0011 0001	J	0100 1010	c	0110 0011	w	0111 0111
2	0011 0010	K	0100 1011	d	0110 0100	x	0111 1000
3	0011 0011	L	0100 1100	e	0110 0101	y	0111 1001
4	0011 0100	M	0100 1101	f	0110 0110	z	0111 1010
5	0011 0101	N	0100 1110	g	0110 0110		
6	0011 0110	O	0100 1111	h	0110 1000	:	0011 1010
7	0011 0110	P	0101 0000	i	0110 1001	;	0011 1011
8	0011 1000	Q	0101 0001	j	0110 1010	?	0011 1111
9	0011 1001	R	0101 0010	k	0110 1011	.	0010 1110
		S	0101 0011	l	0110 1100	/	0010 1111
		T	0101 0100	m	0110 1101	!	0010 0001
A	0100 0001	U	0101 0101	n	0110 1110	,	0010 1100
B	0100 0010	V	0101 0110	o	0110 1111	"	0010 0010
C	0100 0011	W	0101 0111	p	0111 0000	(	0010 1000
D	0100 0100	X	0101 1000	q	0111 0001	)	0010 1001
E	0100 0101	Y	0101 1001	r	0111 0010	space	0010 0000
F	0100 0110	Z	0101 1010	s	0111 0011		
G	0100 0111			t	0111 0100		
H	0100 1000	a	0110 0001	u	0111 0101		

Simple Hash Algorithm: 8-bit Checksum



Message to be Hashed

BOB

Convert to binary in bytes

ASCII Code
B = 01000010
O = 01001111
B = 01000010

Sum the bytes

B = 01000010 = 42 Hex
O = 01001111 = 4F Hex
B = 01000010 = 42 Hex

Sum = 11010011 = D3 Hex

Convert to 2's Complement

```
Sum      = 11010011  = D3 Hex
Opposite = 00101100  = 2C Hex

Add One  = 00101101  = 2D Hex
```

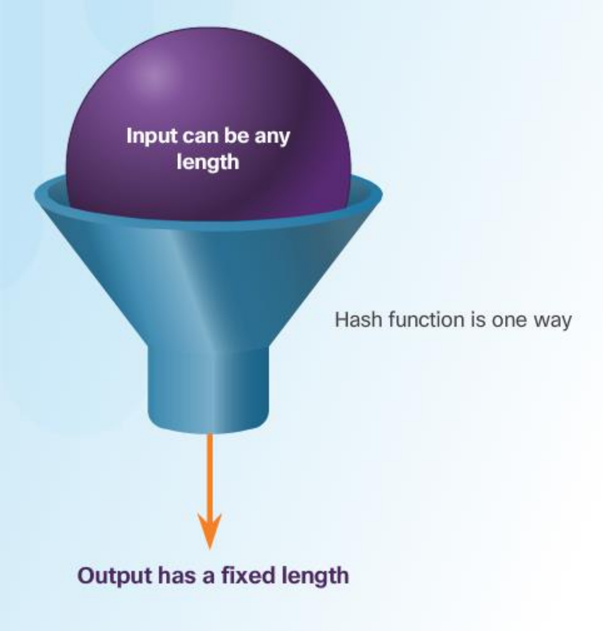
Hash for BOB = 2D

Types of Data Integrity Controls

Hashing Algorithms

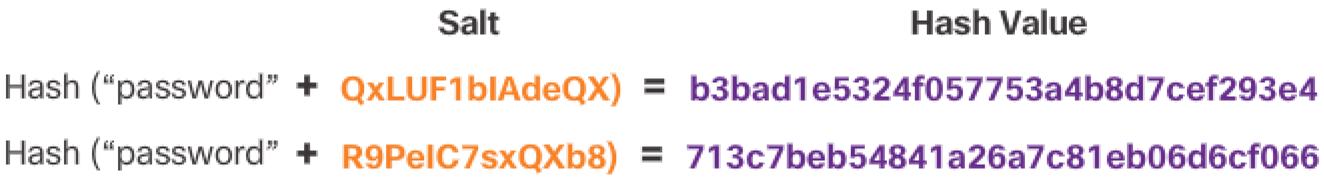
There are many modern hashing algorithms widely used today. Two of the most popular are MD5 and SHA.

- **Message Digest 5 (MD5) Algorithm -** is a hash algorithm developed by Ron Rivest that produces a 128-bit hash value.
- **Secure Hash Algorithm (SHA) –** was developed by the U.S. National Institute of Standards and Technology (NIST) and can be implemented in different strengths:
- SHA-224 (224 bit)
- SHA-256 (256 bit)
- SHA-384 (384 bit)
- SHA-512 (512 bit)



Types of Data Integrity Controls
Salting

- Salting is used to make hashing more secure. If two users have the same password, they will also have the same password hashes. A salt, which is a random string of characters, is an additional input to the password before hashing.
- This creates a different hash result for the two passwords as shown in the figure. A database stores both the hash and the salt.

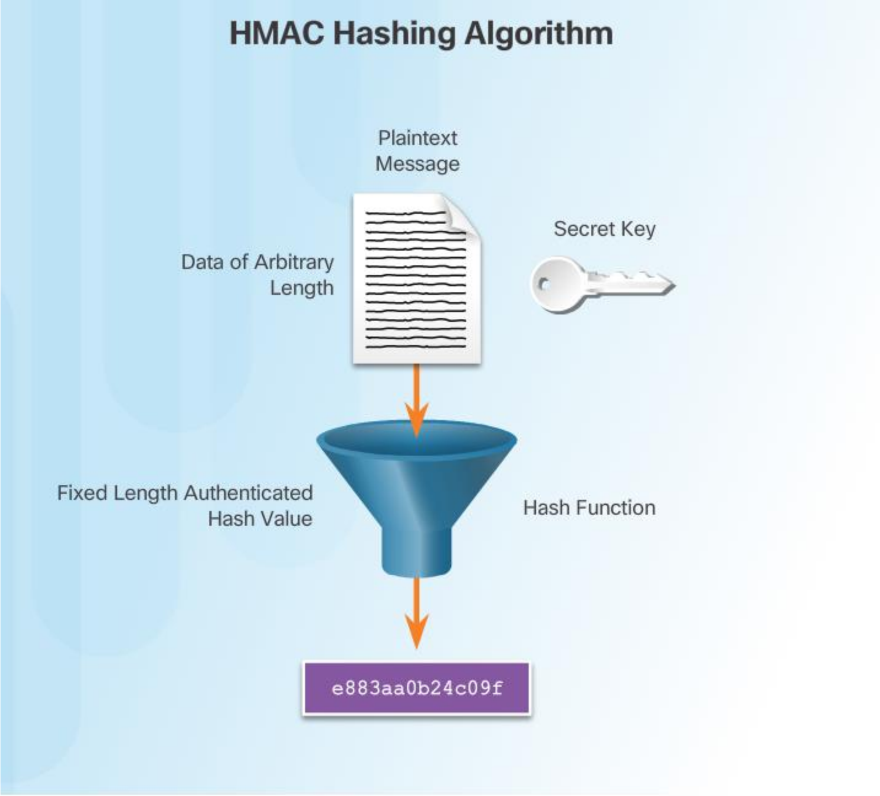


	Salt		Hash Value
Hash (“password” +	QxLUF1bIAdeQX)	=	b3bad1e5324f057753a4b8d7cef293e4
Hash (“password” +	R9PeIC7sxQXb8)	=	713c7beb54841a26a7c81eb06d6cf066

Types of Data Integrity Controls

HMAC

- HMACs strengthens hashing algorithms by using an additional secret key as input to the hash function.
- The use of HMAC goes a step further than just integrity assurance by adding authentication.
- An HMAC uses a specific algorithm that combines a cryptographic hash function with a secret key, as shown in the figure.



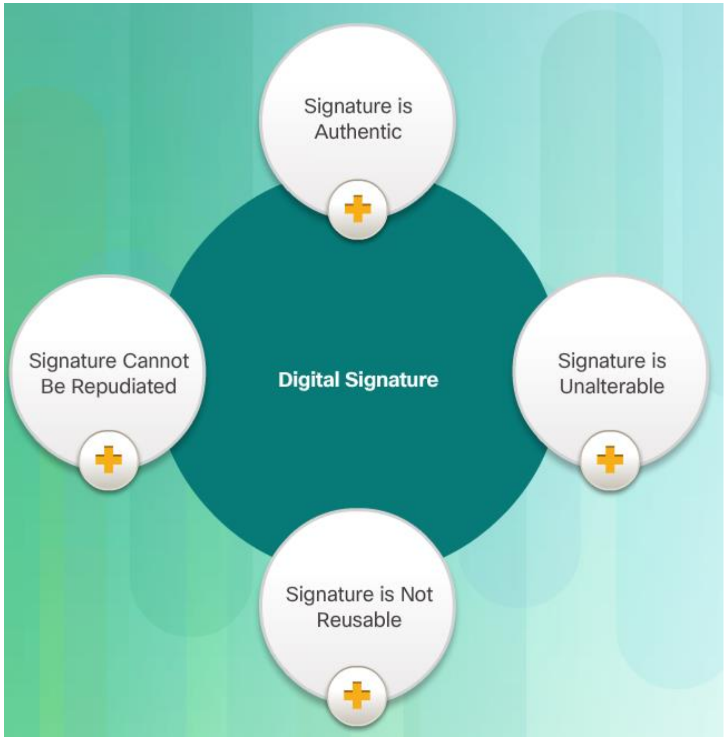
The same procedure is used for generation and verification of secure fingerprints.

5.2 Digital Signatures

Digital Signatures

Signatures and the Law

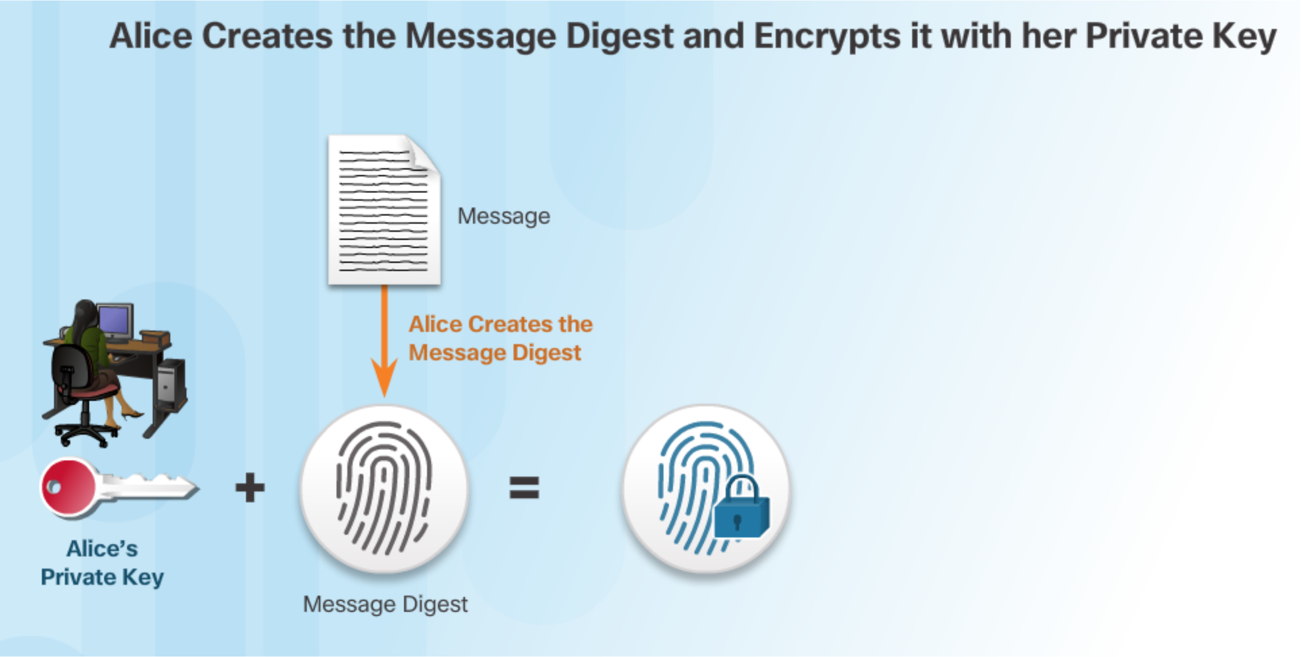
- Digital signatures provide the same functionality as handwritten signatures for electronic documents.
- A digital signature is used to determine if someone edits a document after the user signs it.
- A digital signature is a mathematical method used to check the authenticity and integrity of a message, digital document, or software.
- In many countries, digital signatures have the same legal importance as a manually signed document.
- Digital signatures also provide repudiation.



Digital Signatures

How Digital Signature Technology Works

Asymmetric cryptography is the basis for digital signatures. A public key algorithm like RSA generates two keys: one private and the other public. The keys are mathematically related.



Alice Creates the Message Digest and Encrypts it with her Private Key
Message
Alice Creates the Message Digest
Alice's Private Key
+
Message Digest
=

5.3 Certificates

Cisco | Networking Academy®
Mind Wide Open™

Certificates

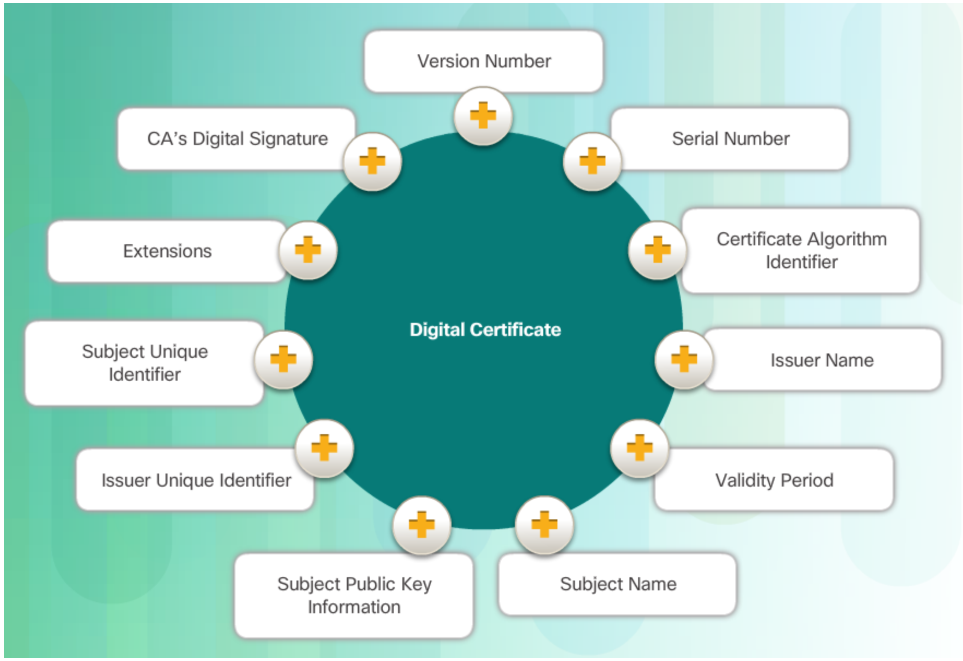
The Basics of Digital Certicates

- A digital certificate is equivalent to an electronic passport.
- Digital certificates enable users, hosts, and organizations to exchange information securely over the Internet.
- A digital certificate authenticates and verifies that users sending a message are who they claim to be.
- Digital certificates can also provide confidentiality for the receiver with the means to encrypt a reply.

Certificates

Constructing a Digital Certificate

- Digital certificate must follow a standard structure so that any entity can read and understand it regardless of the issuer.
- TheX.509 is the standard for construction of digital certificates and the public key infrastructure (PKI) used to manage digital certificates.
- PKI is the policies, roles, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.



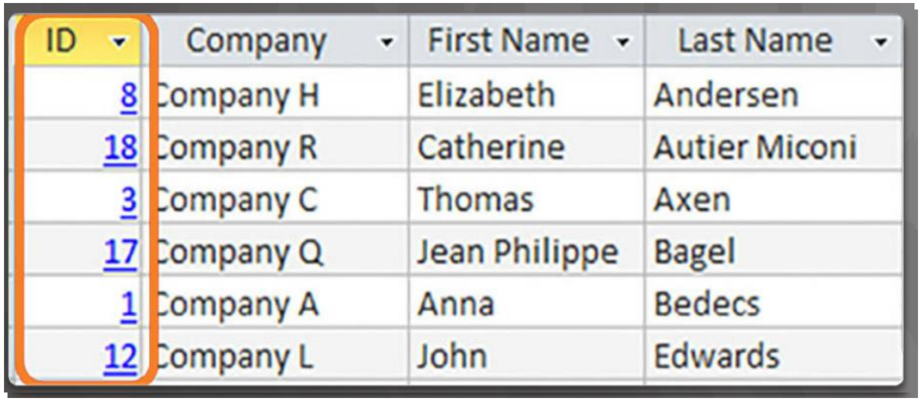
5.4 Database Integrity Enforcement

Cisco | Networking Academy®
Mind Wide Open™

Database Integrity Enforcement

Database Integrity

- Databases provide an efficient way to store, retrieve, and analyze data.
- As data collection increases and data becomes more sensitive, it is important for cybersecurity professionals to protect the growing number of databases.
- Data integrity refers to the accuracy, consistency, and reliability of data stored in a database.



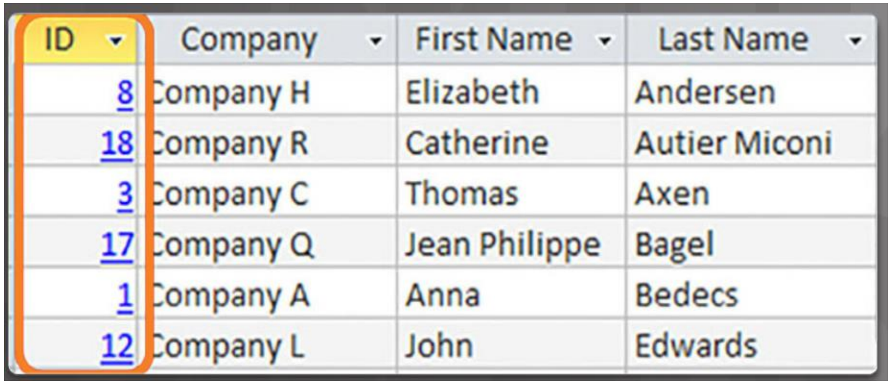
ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

Database Integrity Enforcement

Database Integrity (Cont.)

The four database integrity rules or constraints are as follows:

- **Entity Integrity**: All rows must have a unique identifier called a Primary Key.
- **Domain Integrity**: All data stored in a column must follow the same format and definition.
- **Referential Integrity**: Table relationships must remain consistent. Therefore, a user cannot delete a record which is related to another one.
- **User-defined Integrity**: A set of rules defined by a user which does not belong to one of the other categories. For example, a customer places a new order. The user first checks to see if this is a new customer. If it is, the user adds the new customer to the customers table.



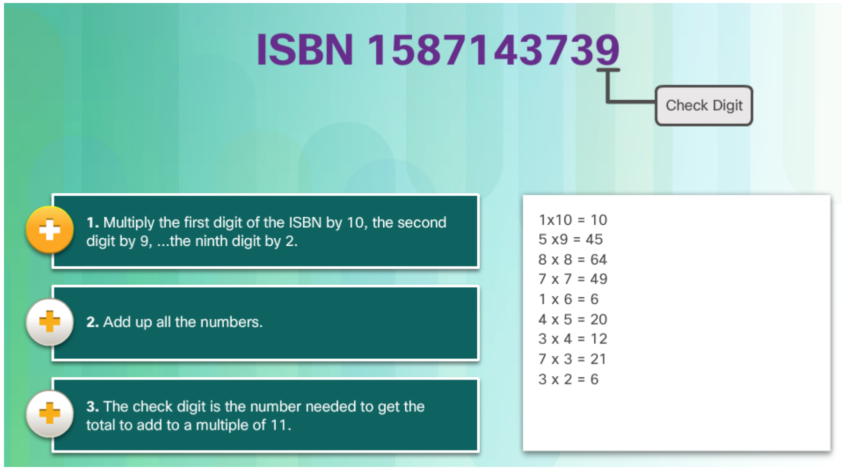
ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

Database Integrity Enforcement

Database Validation

A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy and consistency of data. The criteria used in a validation rule include the following:

- Size – checks the number of characters in a data item
- Format – checks that the data conforms to a specified format
- Consistency – checks for the consistency of codes in related data items
- Range – checks that data lies within a minimum and maximum value
- Check digit – provides for an extra calculation to generate a check digit for error detection.



ISBN 1587143739

1. Multiply the first digit of the ISBN by 10, the second digit by 9, ...the ninth digit by 2.

2. Add up all the numbers.

3. The check digit is the number needed to get the total to add to a multiple of 11.

```
1x10 = 10
5 x9 = 45
8 x 8 = 64
7 x 7 = 49
1 x 6 = 6
4 x 5 = 20
3 x 4 = 12
7 x 3 = 21
3 x 2 = 6
```

Database Integrity Enforcement

Database Integrity Requirements

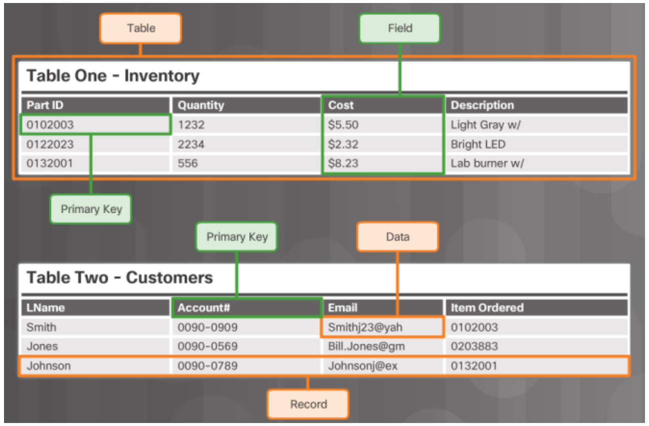


Table One - Inventory

Part ID	Quantity	Cost	Description
0102003	1232	$5.50	Light Gray w/
0122023	2234	$2.32	Bright LED
0132001	556	$8.23	Lab burner w/

Table Two - Customers

LName	Account#	Email	Item Ordered
Smith	0090-0909	Smithj23@yah	0102003
Jones	0090-0569	Bill.Jones@gm	0203883
Johnson	0090-0789	Johnsonj@ex	0132001

- Maintaining proper filing is critical in maintaining the trustworthiness and usefulness of the data within the database.
- Tables, records, fields, and data within each field make up a database.
- In order to maintain the integrity of the database filing system, users must follow certain rules.
- Entity integrity is an integrity rule, which states that every table must have a primary key and that the column or columns chosen to be the primary key must be unique and not NULL.
- Null in a database signifies missing or unknown values. Entity integrity enables proper organization of data for that record.

Database Integrity Enforcement

Database Integrity Requirements (Cont.)

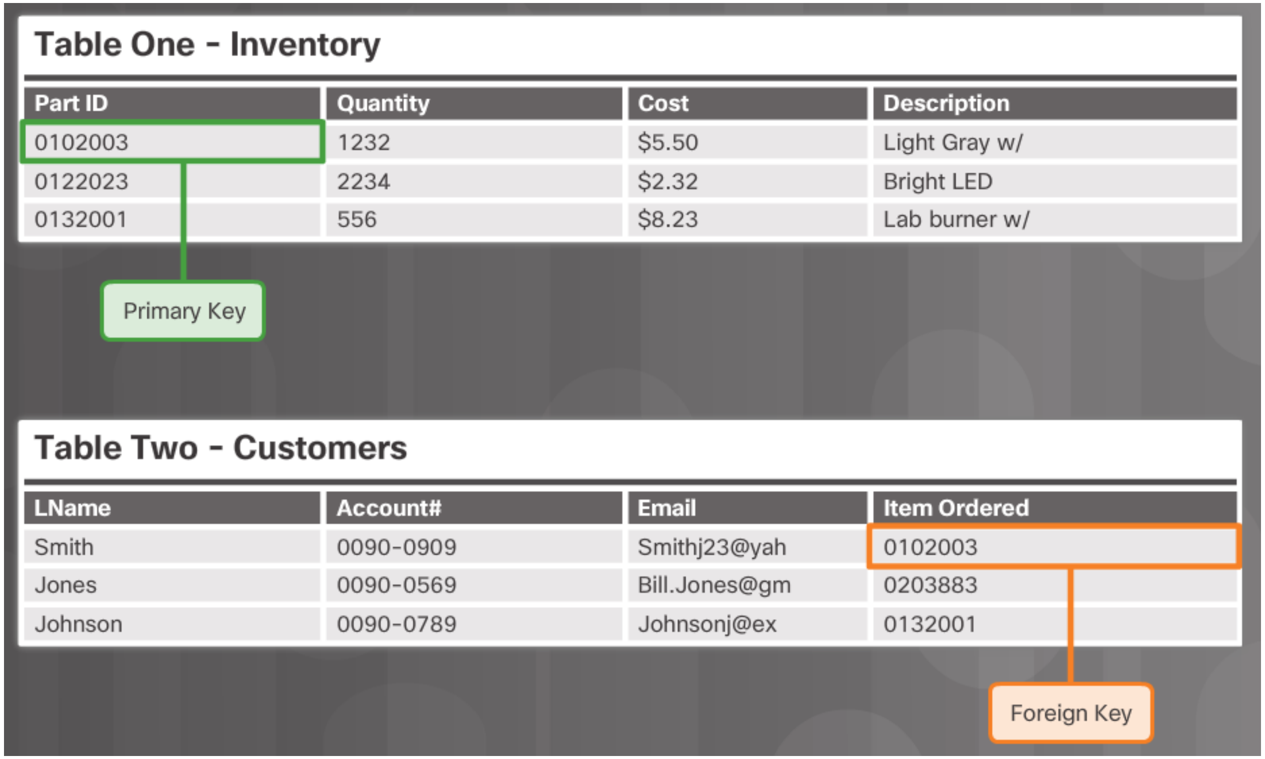


Table One - Inventory

Part ID	Quantity	Cost	Description
0102003	1232	$5.50	Light Gray w/
0122023	2234	$2.32	Bright LED
0132001	556	$8.23	Lab burner w/

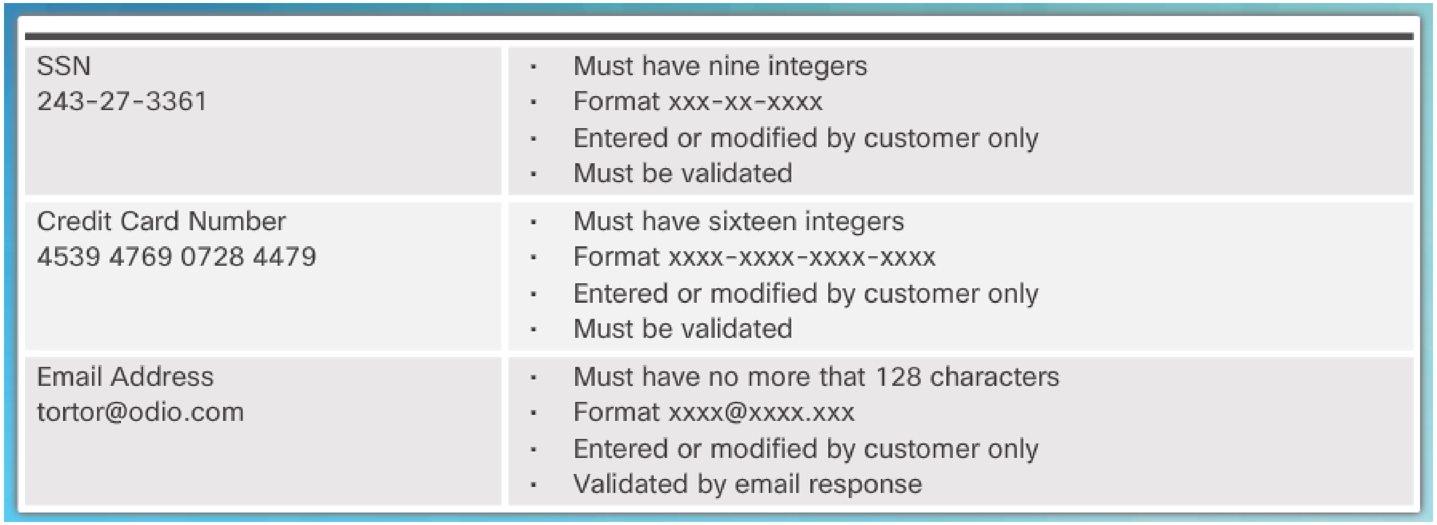
Table Two - Customers

LName	Account#	Email	Item Ordered
Smith	0090-0909	Smithj23@yah	0102003
Jones	0090-0569	Bill.Jones@gm	0203883
Johnson	0090-0789	Johnsonj@ex	0132001

- Another important integrity check is referential integrity which deals with foreign keys. A foreign key in one table references a primary key in a second table. The primary key for a table uniquely identifies entities (rows) in the table. Referential integrity maintains the integrity of foreign keys.

Database Integrity Enforcement

Database Integrity Requirements (Cont.)



SSN 243-27-3361	▪ Must have nine integers ▪ Format xxx-xx-xxxx ▪ Entered or modified by customer only ▪ Must be validated
Credit Card Number 4539 4769 0728 4479	▪ Must have sixteen integers ▪ Format xxxx-xxxx-xxxx-xxxx ▪ Entered or modified by customer only ▪ Must be validated
Email Address tortor@odio.com	▪ Must have no more that 128 characters ▪ Format xxxx@xxxx.xxx ▪ Entered or modified by customer only ▪ Validated by email response

- Domain integrity ensures that all the data items in a column fall within a defined set of valid values. Each column in a table has a defined set of values, such as the set of all numbers for credit card numbers, social security numbers, or email addresses. Limiting the value assigned to an instance of that column (an attribute) enforces domain integrity. Domain integrity enforcement can be as simple as choosing the correct data type, length and or format for a column.

5.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary
Summary

- Chapter five presented the art of integrity which is used to ensure that data remains unchanged by anyone or anything over its entire life cycle.
- The chapter introduced types of data integrity controls including:
  - hashing algorithms
  - password salting
  - keyed-hash message authentication code (HMAC)
- These tools provide a way for cybersecurity specialists to verify the authenticity of messages and documents.
- The chapter concluded with a discussion of database integrity enforcement.
- Having a well-controlled and well-defined data integrity system increases the stability, performance, and maintainability of a database system.

Cisco | Networking Academy®

Mind Wide Open™