

# Protecting Secrets

# Sections & Objectives

## Cryptography

Explain how encryption techniques protect confidentiality.

## Access Control

Describe access control techniques used to protect confidentiality.

## Obscuring Data

Describe the concept of obscuring data.

# Cryptography

# Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition
- Substitution
- One-time pad

# Overview (Cont.)

## Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins.
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

# Private-Key Encryption

**Symmetrical Encryption Process** - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.

# Public-Key Encryption

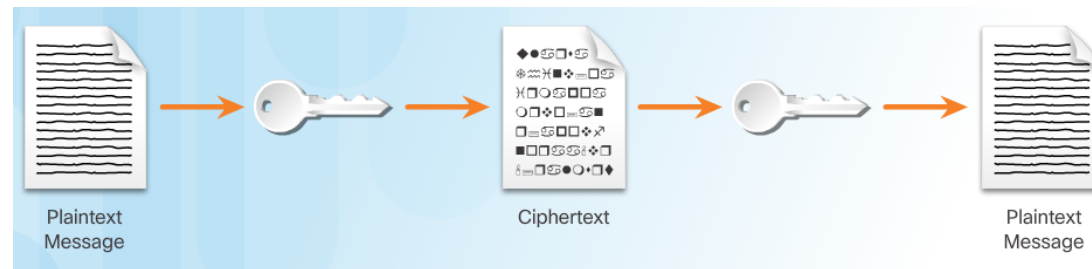
**Asymmetrical Encryption Process** - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest-Shamir-Adleman)** - uses the product of two very large prime numbers. **Browsers use RSA to establish a secure connection.**
  - [Factorization of a 768-bit RSA modulus](#)
  - [RSA Factoring Challenge](#)
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

# Symmetrical versus Asymmetrical Encryption

## Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.





# Symmetrical versus Asymmetrical Encryption

## Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.

# Symmetrical versus Asymmetrical Encryption

## Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

# Symmetrical versus Asymmetrical Encryption

## Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.

## 4.2 Access Control

# Types of Access Control

**Physical Access Controls** - actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).

**Logical Access Controls** - hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

**Administrative Access Controls** - policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices.

# Access Control Strategies

**Mandatory access control (MAC)** - restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.

**Discretionary access control (DAC)** - DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.

**Role-based access control (RBAC)** - is based on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role. RBAC can work in combination with DAC or MAC by enforcing the policies of either one.

**Rule-based access control** - uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.

# Identification

Identification enforces the rules established by the authorization policy:

- A subject requests access to a system resource.
- Every time the subject requests access to a resource, the access controls determine whether to grant or deny access.
- Cybersecurity policies determine which identification controls should be used.
- The sensitivity of the information and information systems determine how stringent the controls.
- The increase in data breaches has forced many organizations to strengthen their identification controls.



# Authentication Methods

**What You Know** - Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication.

**What You Have** - Smart cards and security key fobs are both examples of something that users have in their possession.

**Who You Are** - A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics.

**Multi-factor Authentication** - Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob.





# Authorization

Authorization controls what a user can and cannot do on the network after successful authentication:

- After a user proves his or her identity, the system checks to see what network resources the user can access and what the users can do with the resources.
- Authorization uses a set of attributes that describes the user's access to the network.
- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
- Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.



# Accountability

–Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data:

- The organization can use this data for such purposes as auditing or billing.
- The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed.
- This allows an organization to trace actions, errors, and mistakes during an audit or investigation.
- Implementing accountability consists of technologies, policies, procedures, and education.
- Log files provide detailed information based on the parameters chosen.

# Types of Security Controls

**Preventative Controls** - Prevent means to keep something from happening. Preventative access controls stop unwanted or unauthorized activity from happening.

**Deterrent Controls** - A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior. Deterrents do not always stop these actions.

**Detective Controls** - Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system.



# Types of Security Controls

**Corrective Controls** - Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

**Recovery Controls** - Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

**Compensative Controls** - Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

## Obscuring Data

# Data Masking

Data Masking is a technology that secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities.

In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis.

There are data masking techniques that can ensure that data remains meaningful but changed enough to protect it:

- **Substitution** - replaces data with authentic looking values to apply anonymity to the data records.
- **Shuffling** - derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.

# Steganography

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.

There are several components involved in hiding data:

- There is the embedded data, which is the secret message.
- Cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio).
- A stego-key controls the hiding process.

# Data Obfuscation

**Data obfuscation** - is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession:

- Obfuscation is the art of making the message confusing, ambiguous, or harder to understand.
- A system may purposely scramble messages to prevent unauthorized access to sensitive information.
- Software watermarking protects software from unauthorized access or modification.
- Software watermarking inserts a secret message into the program as proof of ownership.
- The secret message is the software watermark. If someone tries to remove the watermark, the result is nonfunctional code.



# Ensuring Integrity

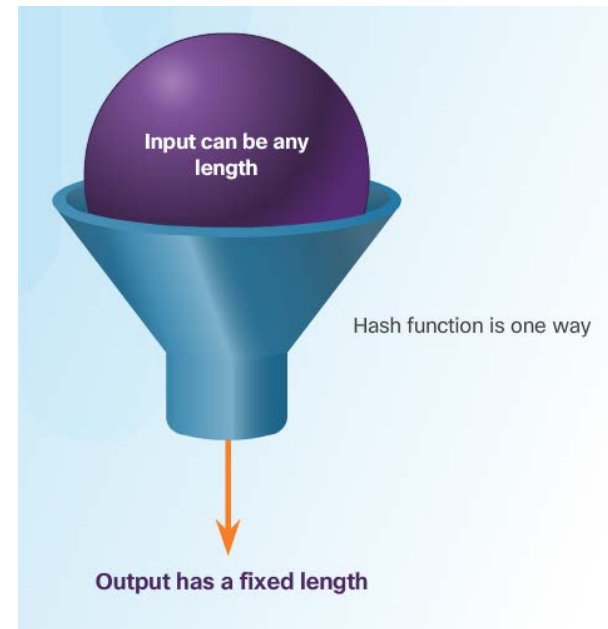
# Hashing Algorithms

- 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.

# Hashing Algorithms

There are many modern hashing algorithms widely used today.

- **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)
- **Message-Digest algorithm(MD5)** – The probability of just two hashes accidentally colliding is approximately:  $1.47 \times 10^{-29}$ .



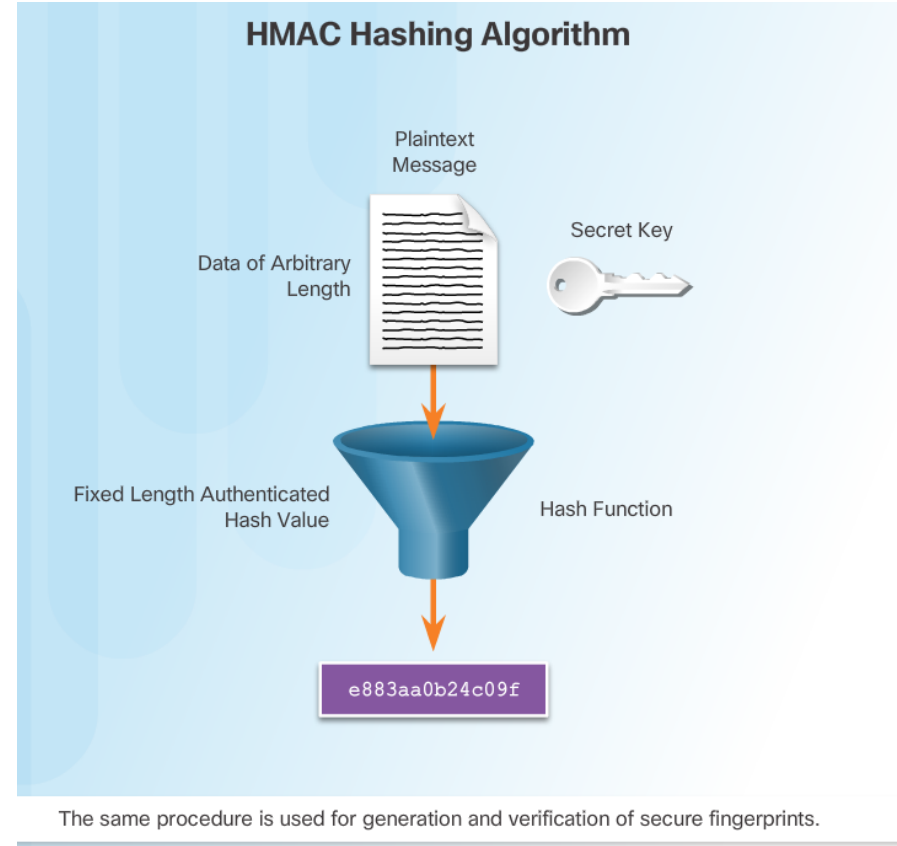
# Salting

- 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

# HMAC (Hash-based Message Authentication Code)

- 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.



# Digital Signatures

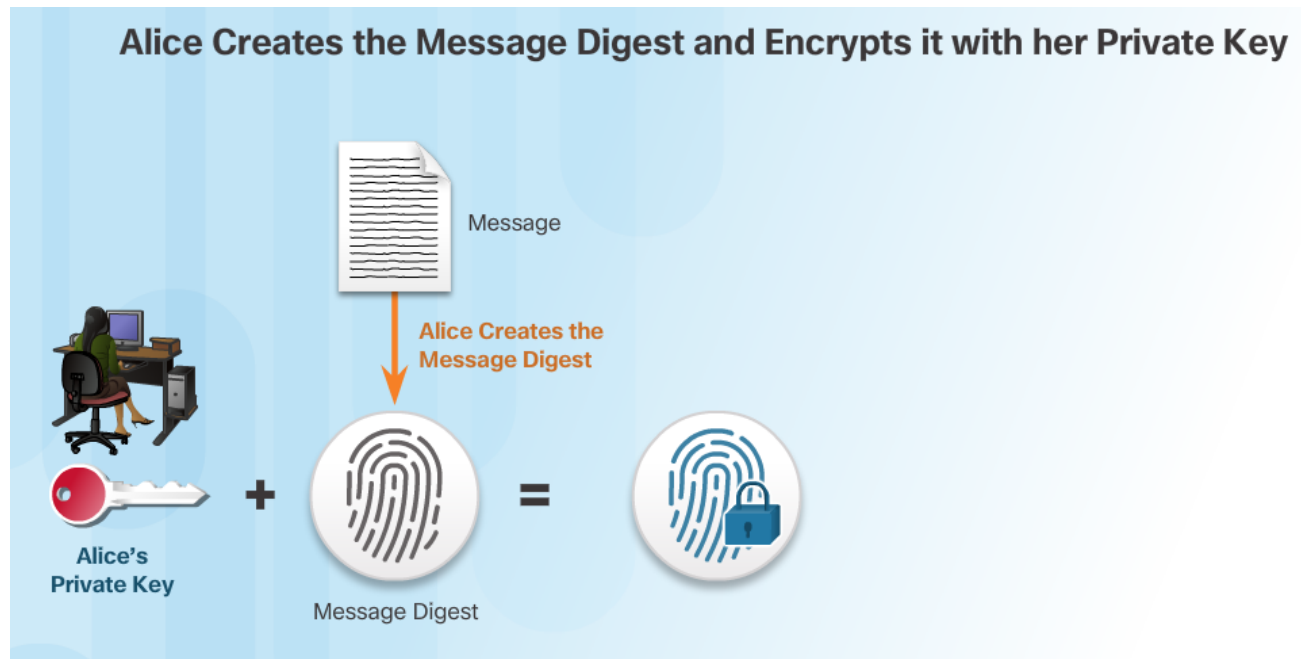
# Signatures and the Law

- 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.
- [OpenSSL cryptographic software library](#)



# 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.





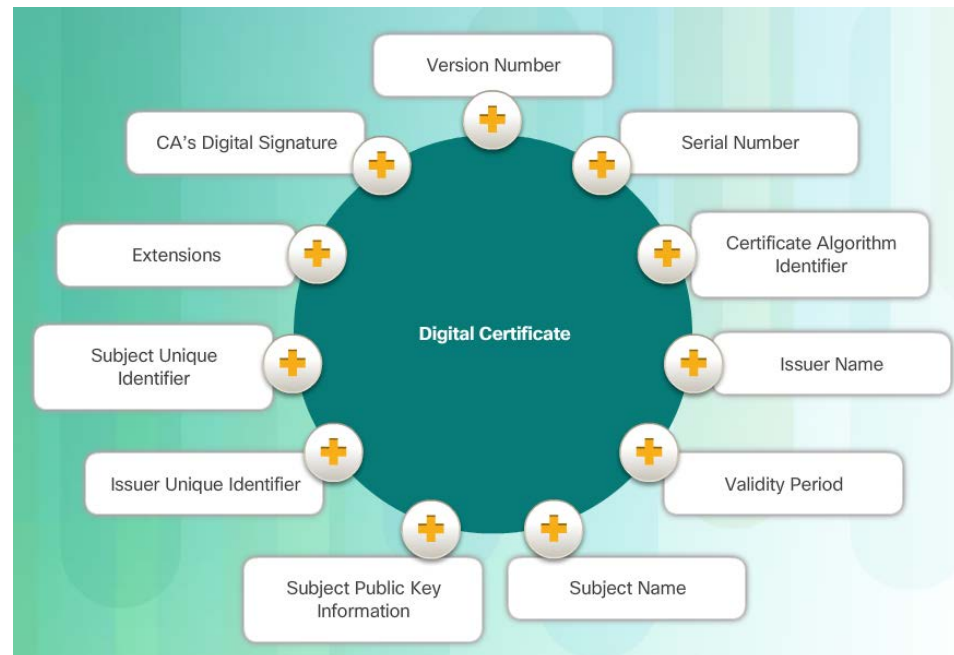
# Certificates

# The Basics of Digital Certificates

- 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.
- [Wildcard Certificates May Lead to TLS Vulnerabilities](#)

# Constructing a Digital Certificate

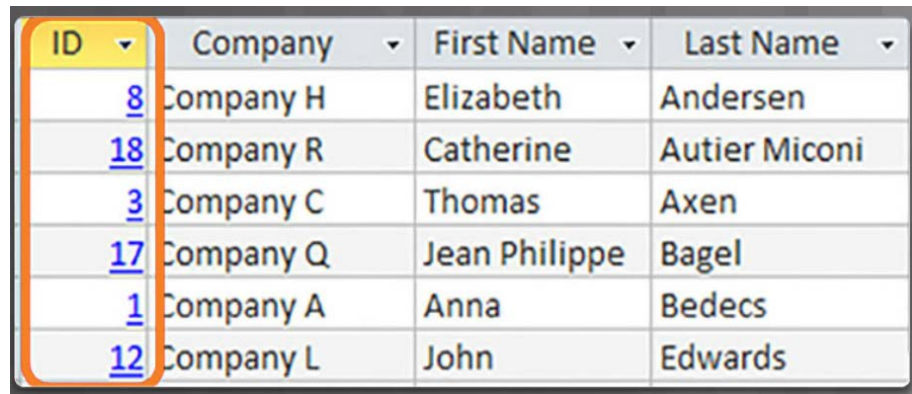
- Digital certificate must follow a standard structure so that any entity can read and understand it regardless of the issuer.
- The X.509 is the standard for construction of digital certificates and the public key infrastructure (PKI) used to manage digital certificates.
- PKI is the policies, roles,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



# 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.

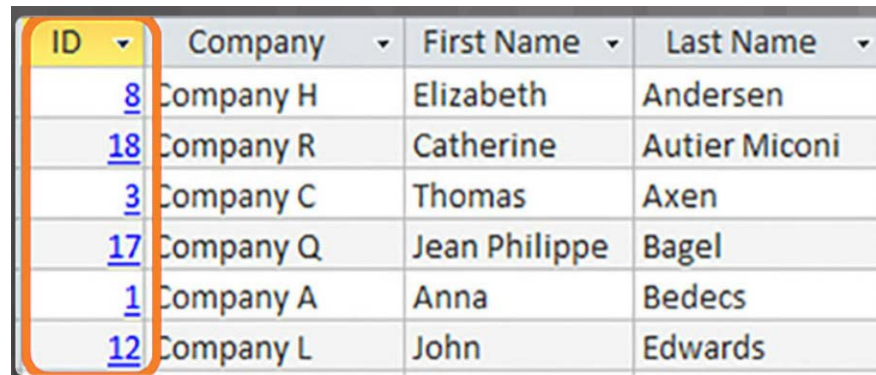
A screenshot of a database table with four columns: ID, Company, First Name, and Last Name. The ID column is highlighted with an orange border. The data rows are as follows:

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

# 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.

A screenshot of a database table with four columns: ID, Company, First Name, and Last Name. The ID column is highlighted with an orange box, indicating its role as a primary key. The data rows show various companies and their associated first and last names.

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 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.

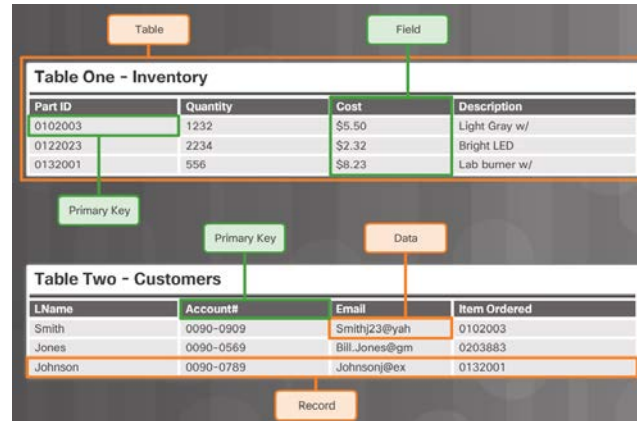
The diagram illustrates the process of calculating the check digit for the ISBN 1587143739. It features a green background with a light blue gradient. The ISBN number is displayed in purple at the top. A bracket labeled 'Check Digit' points to the final digit '9'. Below the ISBN, three numbered steps are listed in white boxes with orange plus icons:

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.

To the right of these steps, a list of calculations is shown:

$$\begin{aligned} 1 \times 10 &= 10 \\ 5 \times 9 &= 45 \\ 8 \times 8 &= 64 \\ 7 \times 7 &= 49 \\ 1 \times 6 &= 6 \\ 4 \times 5 &= 20 \\ 3 \times 4 &= 12 \\ 7 \times 3 &= 21 \\ 3 \times 2 &= 6 \end{aligned}$$

# Database Integrity Requirements



- 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 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/

Primary Key

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

Foreign Key

- 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 Requirements (Cont.)

SSN 243-27-3361	<ul style="list-style-type: none"><li>• Must have nine integers</li><li>• Format xxx-xx-xxxx</li><li>• Entered or modified by customer only</li><li>• Must be validated</li></ul>
Credit Card Number 4539 4769 0728 4479	<ul style="list-style-type: none"><li>• Must have sixteen integers</li><li>• Format xxxx-xxxx-xxxx-xxxx</li><li>• Entered or modified by customer only</li><li>• Must be validated</li></ul>
Email Address tortor@odio.com	<ul style="list-style-type: none"><li>• Must have no more that 128 characters</li><li>• Format xxxx@xxxx.xxx</li><li>• Entered or modified by customer only</li><li>• Validated by email response</li></ul>

- 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.