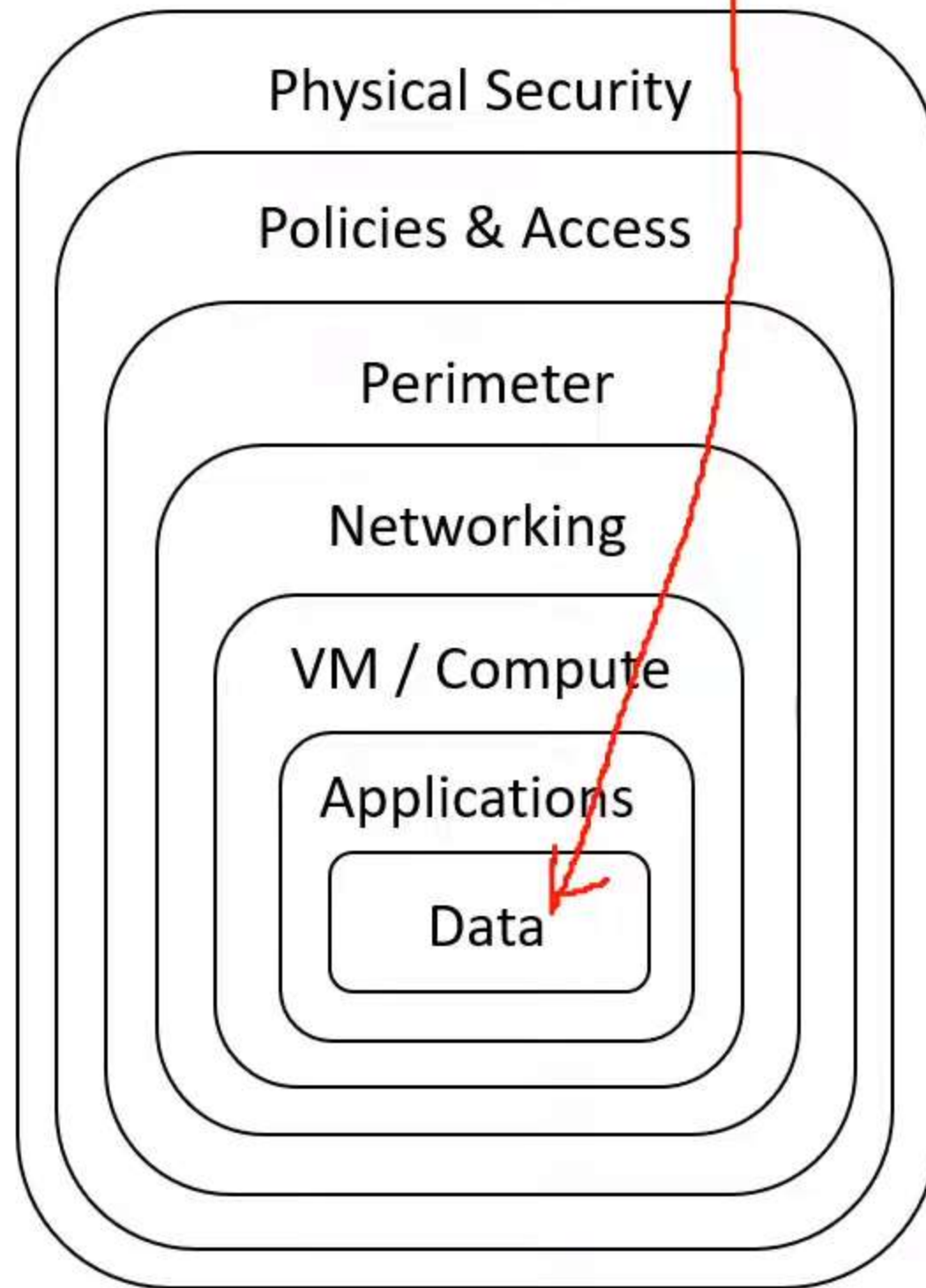


# Defense in Depth

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)



## The 7 Layers of Security

### 1. Data

access to business and customer data, and encryption to protect data.

### 2. Application

applications are secure and free of security vulnerabilities.

### 3. Compute

Access to virtual machines (ports, on-premise, cloud)

### 4. Network

limit communication between resources using segmentation and access controls.

### 5. Perimeter

distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

### 6. Identity and access

controlling access to infrastructure and change control.

### 7. Physical

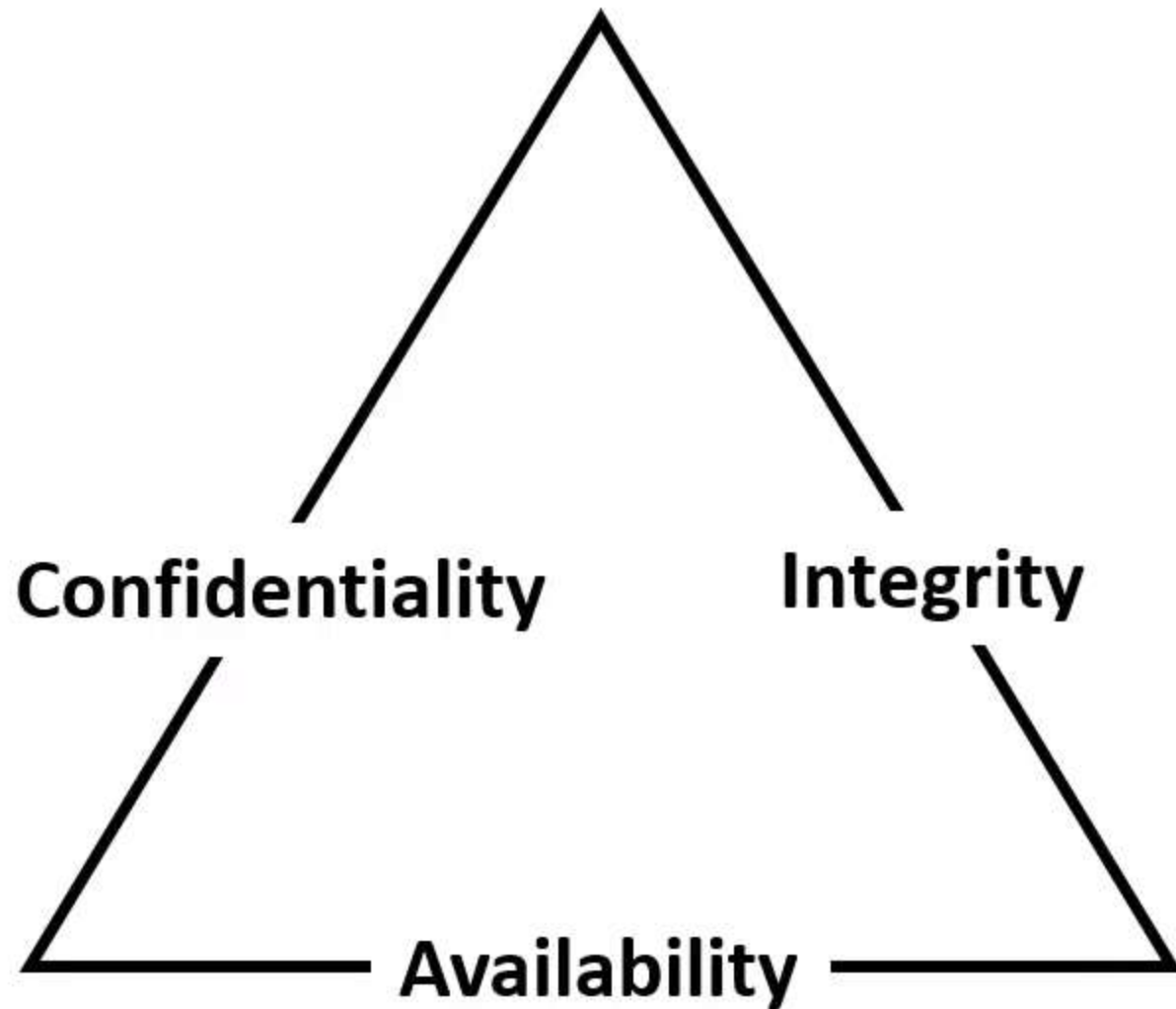
limiting access to a datacenter to only authorized personnel.



# Confidentiality, Integrity, Availability (CIA)

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](https://www.examprompro.co/clf-c01)

Confidentiality, Integrity, and Availability (CIA) triad is a model describing the foundation to security principles and their trade-off relationship.



## Confidentiality

confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. In practice this can be using cryptographic keys to encrypt our data, and using keys to encrypt our keys (envelope encryption)

## Integrity

maintaining and assuring the accuracy and completeness of data over its entire lifecycle. In Practice utilizing ACID compliant databases for valid transactions. Utilizing tamper-evident or tamper proof Hardware security modules. (HSM)

## Availability

information needs to be made be available when needed  
In Practice: High Availability, Mitigating DDoS, Decryption access

The CIA triad was first mentioned in a **NIST publication from 1977.**

There have been efforts to expand and modernize or suggest alternatives to CIA triad:

- (1998) Six Atomic Elements of Information eg. confidentiality, possession, integrity, authenticity, availability, and utility
- (2004) NIST Engineering Principles for Information Technology Security — 33 security principles



# Vulnerabilities

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## What is a vulnerability?

a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application



Allowing Domains or Accounts to Expire

### Buffer Overflow

Business logic vulnerability

CRLF Injection

CSV Injection

Catch NullPointerException

Covert storage channel

Deserialization of untrusted data

Directory Restriction Error

Doubly freeing memory

Empty String Password

Expression Language Injection

Full Trust CLR Verification issue

Heartbleed Bug

### Improper Data Validation

Improper pointer subtraction

Information exposure through query strings

Injection problem

Insecure Compiler Optimization

Insecure Randomness

Insecure Temporary File

Insecure Third Party Domain Access

Insecure Transport

Insufficient Entropy

Insufficient Session-ID Length

### Least Privilege Violation

### Memory leak

Missing Error Handling

Missing XML Validation

Multiple admin levels

Null Dereference

OWASP .NET Vulnerability Research

Overly Permissive Regular Expression

PHP File Inclusion

PHP Object Injection

PRNG Seed Error

Password Management Hardcoded Password

Password Plaintext Storage

Poor Logging Practice

Portability Flaw

Privacy Violation

Process Control

Return Inside Finally Block

Session Variable Overloading

String Termination Error

Unchecked Error Condition

Unchecked Return Value Missing Check against Null

Undefined Behavior

Unreleased Resource

Unrestricted File Upload

Unsafe JNI

Unsafe Mobile Code

Unsafe function call from a signal handler

Unsafe use of Reflection

Use of Obsolete Methods

Use of hard-coded password

### Using a broken or risky cryptographic algorithm

Using freed memory

Vulnerability template

XML External Entity (XXE) Processing



# Encryption

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## What is cryptography?

The practice and study of techniques for secure communication in the presence of third parties called adversaries

## What is encryption?

The process of encoding (scrabbling) information **using a key** and a **cypher** to store sensitive data in an unintelligible format as a means of protection. An encryption takes in plaintext and produces **ciphertext**.



The **enigma machine** was used during WW2. A different key for each day was used to set the position of the rotors. It relied on simple cypher substitution.



# Cyphers

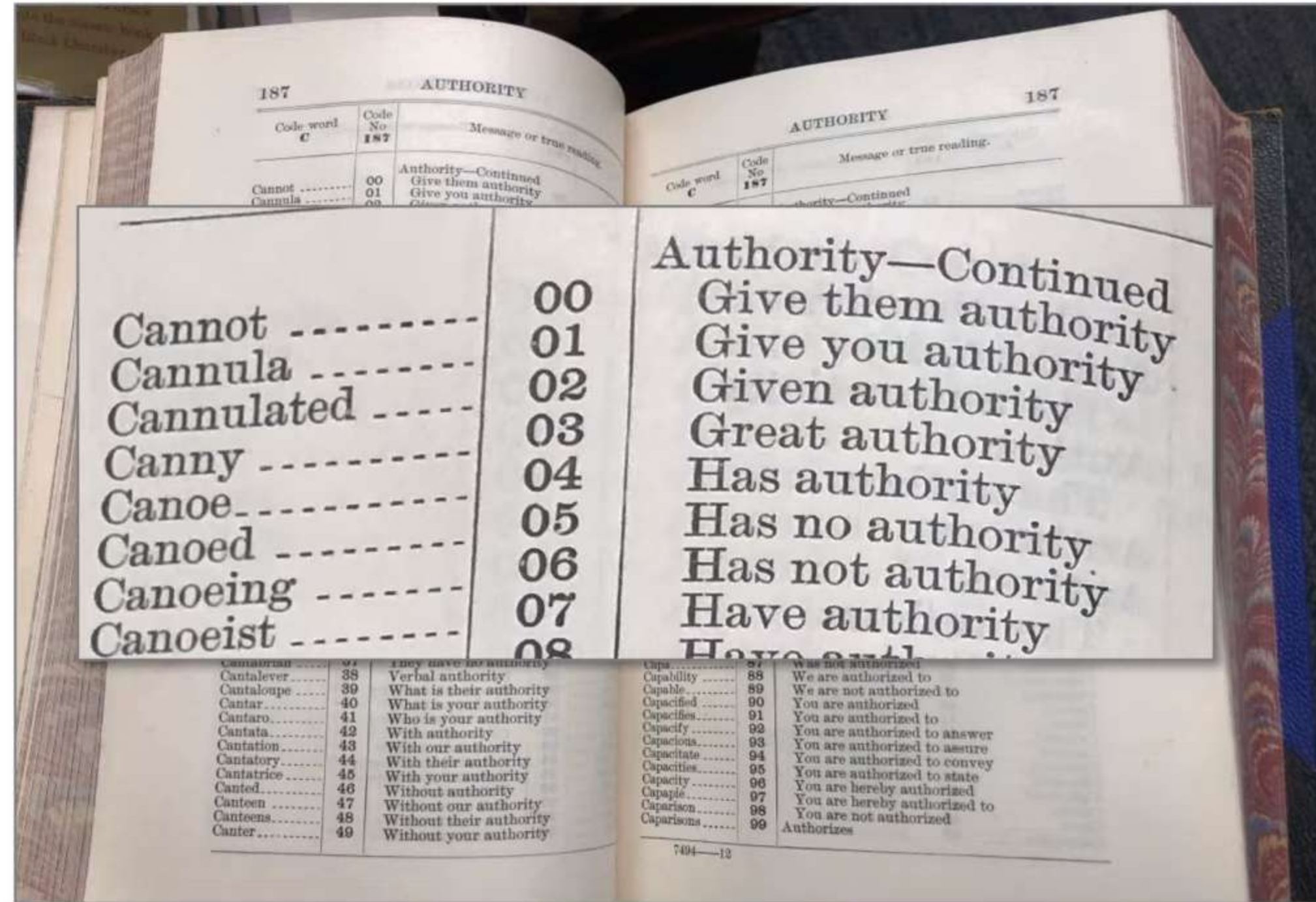
Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampuro.co/clf-c01](http://www.exampuro.co/clf-c01)

## What is a cypher?

An algorithm that performs encryption or decryption. Cipher is synonymous with “code”

## What is ciphertext

Ciphertext is the result of encryption performed on plaintext via an algorithm



A **codebook** is a type of document used for gathering and storing cryptography codes

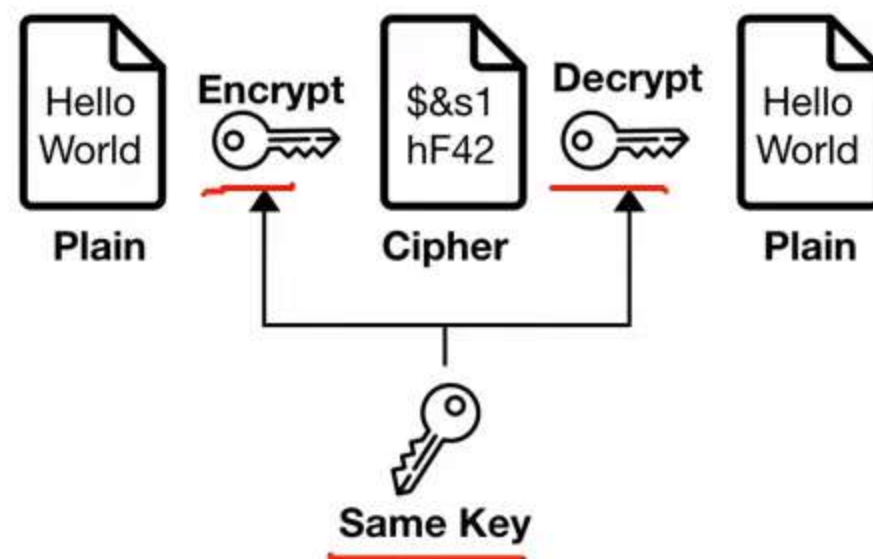


# Cryptographic Keys

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

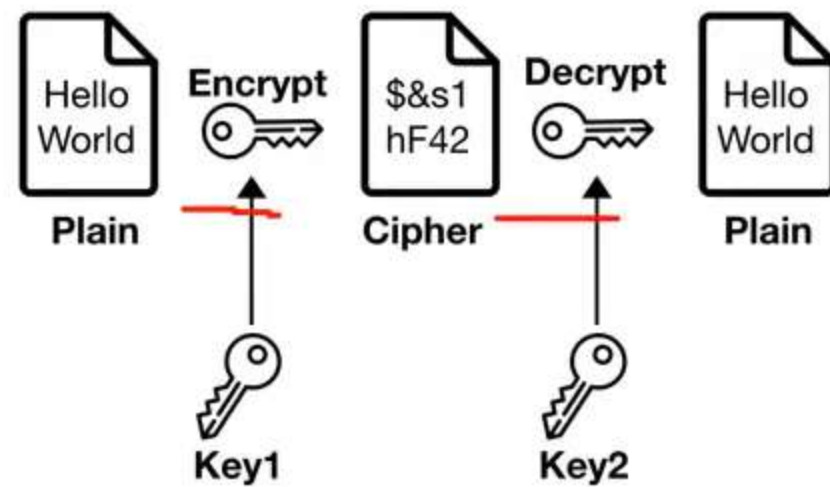
## What is a cryptographic key?

A key is a variable used in conjunction with an encryption algorithm in order to encrypt or decrypt data.



## What is symmetric encryption?

The same key is used for encoding and decoding.  
eg **Advanced Encryption Standard (AES)**

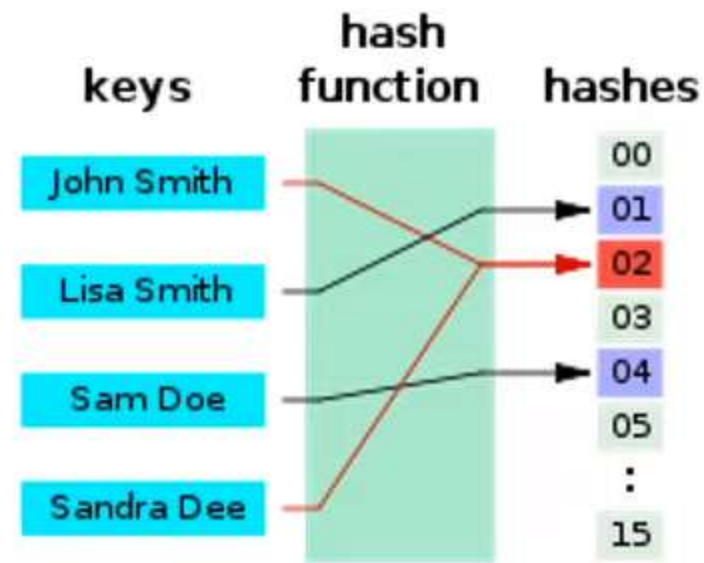


## What is asymmetric encryption?

Two keys are used. One to encode and one to decode eg. **Rivest-Shamir-Adleman (RSA)**

# Hashing and Salting

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)



## What is hashing function?

A function that accepts arbitrary size value and maps it to a fixed-size data structure. Hashing can reduce the size of the store value.

Hashing is a **one-way process** and is **deterministic**

A deterministic function always returns the same output for the same input.

## Hashing Passwords

Hashing functions are used to store passwords in database so that a password does not reside in a plaintext format.

To authenticate a user, when a user inputs their password, it is hashed, and the hash is compared to the store hashed. If they match then the user has successful logged in.

Popular hashing functions are **MD5, SHA256 and Bcrypt**

If an attacker knows what function you are using and stole your database, they could enumerate a dictionary of password to determine the password.

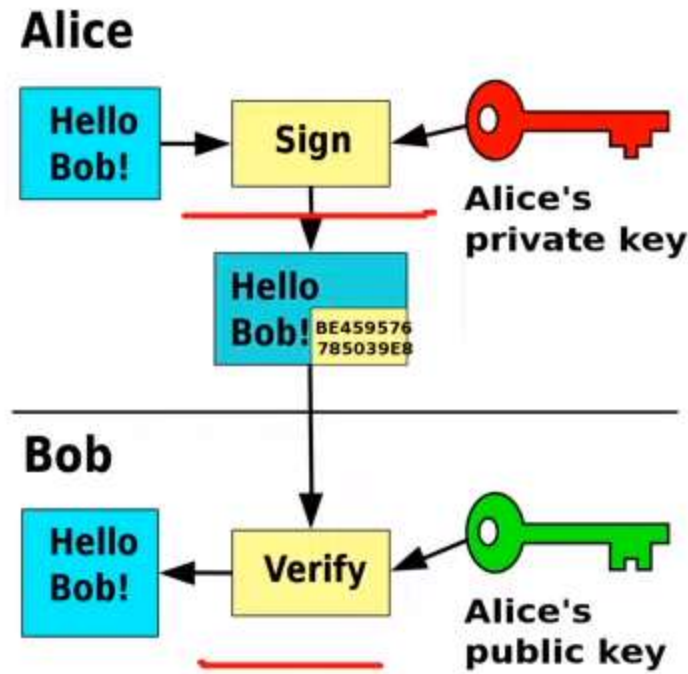
## Salting Passwords

A salt is a random string not known to the attacker that the hash function accepts to mitigate the deterministic nature of hashing functions



# Digital Signatures and Signing

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampor.co/clf-c01](http://www.exampor.co/clf-c01)



## What is a digital signature

A mathematical scheme for verifying the authenticity of digital messages or documents.

A Digital signature gives us **tamper-evidence**.

- Did someone mess (modify) the data?
- Is this data is not from the expected sender?

There are three algorithms to digital signatures:

- **Key generation** – generates a public and private key.
- **Signing** - the process of generating a digital signature with a **private key** and inputted message
- **Signing verification** – verify the authenticity of the message with a **public key**

```
ssh-keygen -t rsa
```

SSH uses a public and private key to authorize remote access into a remote machine e.g. Virtual Machine. It is common to use RSA  
ssh-keygen is a **well known command** to generate a public and private key

## What is Code Signing?

When you use a digital signature to ensure **computer code** has not been tampered



# In-Transit vs At-Rest Encryption

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](https://www.examprompro.co/clf-c01)

## Encryption In-Transit

Data that is secure when moving between locations

Algorithms: **TLS, SSL**

## Encryption At-Rest

Data that is secure when residing on storage or within a database

Algorithms: **AES, RSA**

### Transport Layer Security (TLS)

An encryption protocol for data integrity between two or more communicating computer application.

*TLS 1.0, 1.1 are deprecated. **TLS 1.2** and **1.3** is the current best practice*

### Secure Sockets Layers (SSL)

An encryption protocol for data integrity between two or more communicating computer application

*SSL 1.0, 2.0 and 3.0 are deprecated*



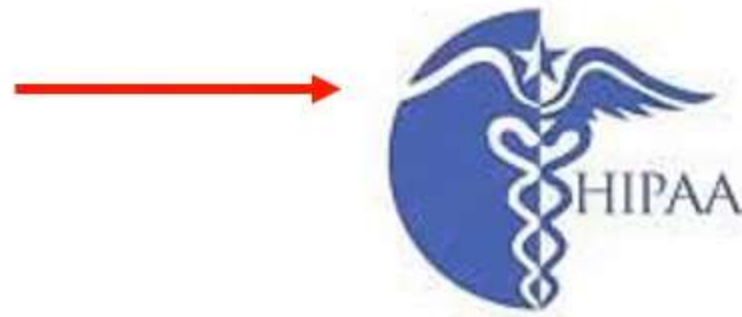
# Common Compliance Programs

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## Compliance Programs

A set of internal policies and procedures of a company to comply with laws, rules, and regulations or to uphold business reputation.

**Health Insurance Portability and Accountability Act of 1996)** is United States legislation that provides data privacy and security provisions for safeguarding medical information.



**The Payment Card Industry Data Security Standard (PCI DSS)**



When you want to sell things online and you need to handle credit card information.





# Common Compliance Programs

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampor.co/clf-c01](http://www.exampor.co/clf-c01)



## International Organization for Standardization (ISO) / International Electrotechnical Commission

ISO/IEC 27001 — control implementation guidance

ISO/IEC 27017 — enhanced focus on cloud security

ISO/IEC 27018 — protection of personal data in the cloud. eg. PII

ISO/IEC 27701 — Privacy Information Management System (PIMS) framework

- outlines controls and processes to manage data privacy and protect PII.



## System and Organization Controls (SOC)

SOC 1 — 18 standard and report on the effectiveness of internal controls (SSAE) at a service organization

- relevant to their client's internal control over financial reporting (ICFR).

SOC 2 — evaluates internal controls, policies, and procedures that directly relate to the security of a system at a service organization

SOC 3 — A report based on the Trust Services Criteria that can be freely distributed



## Payment Card Industry Data Security Standard (PCI DSS)

a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.



## Federal Information Processing Standard (FIPS) 140-2

US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.



# Common Compliance Programs

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)



## **Personal Health Information Protection Act (PHIPA)**

An Ontario provincial law (Canada) that regulates patient Protected Health Information



## **Health Insurance Portability and Accountability Act (HIPAA).**

US federal law that regulates patient Protected Health Information



## **Cloud Security Alliance (CSA) STAR Certification**

Independent third-party assessment of a cloud provider's security posture



# Common Compliance Programs

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)



FedRAMP

## **Federal Risk and Authorization Management Program (FedRAMP)**

US government standardized approach to security authorizations for Cloud Service Offerings



## **Criminal Justice Information Services (CJIS)**

Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.



## **General Data Protection Regulation (GDPR)**

A European privacy law. Imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.



# Penetration Testing

Cheat sheets, Practice Exams and Flash cards  [www.exampnro.co/clf-c01](http://www.exampnro.co/clf-c01)

## What is PenTesting?

An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.



Pen Testing **is allowed** to be performed on AWS!

### Permitted Services

- Amazon EC2 instances
- NAT Gateways
- Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

### Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- \*Subject to the **DDoS Simulation Testing policy**
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
  - Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

For **Other Simulated Events** you will need to submit a request to AWS. A reply could take up to 7 days.



# AWS Artifact

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampopro.co/clf-c01](http://www.exampopro.co/clf-c01)



**AWS Artifact** is a self-serve portal for on-demand access to **AWS compliance reports**



Choose you report

View the PDF

Reports Info

Reports (82)

Q canada X 1 match

Copy link Download report

Title	Reporting period	Category	Description
Government of Canada (GC) Partner Package	August 25, 2017 to current	Alignment Documents	The Government of Canada (GC) Partner Package is intended for use by partners and customers when building applications and solutions on AWS that need to meet the GC requirements based on the Protected B/Medium Integrity/Medium Availability (PBMM) profile. The documents available in this package include: Partner Package Playbook, Controls Implementation Summary (CIS)/Customer Responsibility Matrix (CRM), and Government of Canada PBMM Security Assessment and Letter of Attestation.



Download the Excel





# AWS Inspector

Cheat sheets, Practice Exams and Flash cards  [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## What is Hardening?

The act of eliminating as many **security** risks as possible. Hardening is common for Virtual Machines where you run a collection of security checks known as a security benchmark



AWS Inspector runs a **security benchmark** against specific EC2 instances. You can run a variety of security benchmarks. Can perform both **Network** and **Host** Assessments

### Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run once for a one-time assessment, or **Advanced setup** for custom assessments.

#### ☒ Network Assessments (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. [Learn more](#)
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. [Learn more](#)
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment. For example, for 100 instances assessed weekly, the monthly cost would be around \$61/month. [Learn more](#)

#### ☒ Host Assessments (Inspector Agent is required)

- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. [Learn more](#)
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instance. [Learn more](#) about [Inspector Agent](#) and [how to manually install agent](#).
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment. For example, for 100 instances assessed weekly, the monthly cost would be around \$120/month. [Learn more](#)

[Run weekly \(recommended\)](#)

- Install the AWS agent on your EC2 instances.
- Run an assessment for your assessment target.
- Review your findings and remediate security issues.

One very popular benchmark you can run is by CIS which has **699 checks!**



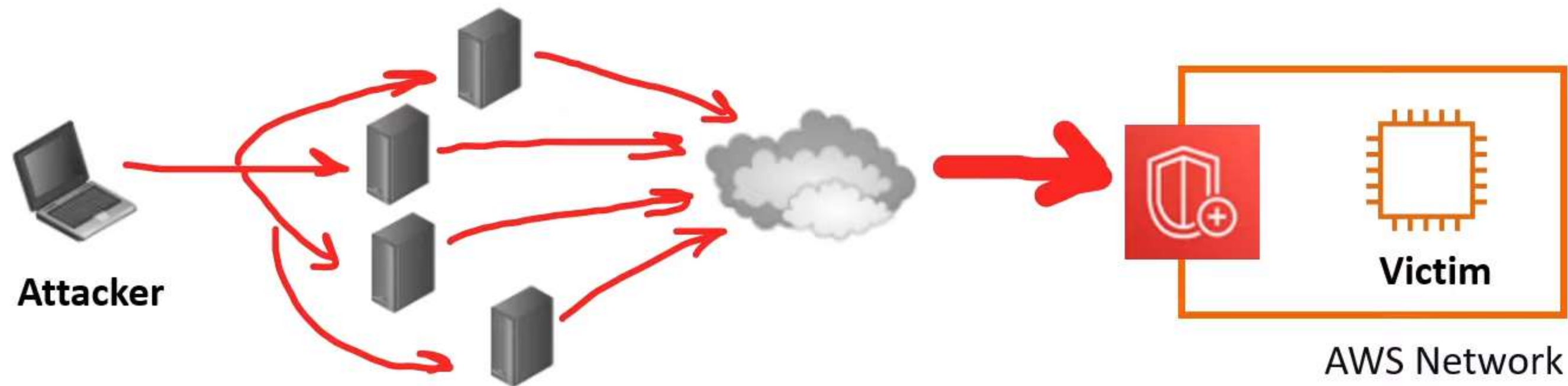


# Distributed Denial of Service (DDoS)

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## What is a DDoS (Distributed Denial of Service) Attack?

A malicious attempt to disrupt normal traffic by flooding a website with large amounts of fake traffic.





# AWS Shield

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampopro.co/clf-c01](http://www.exampopro.co/clf-c01)

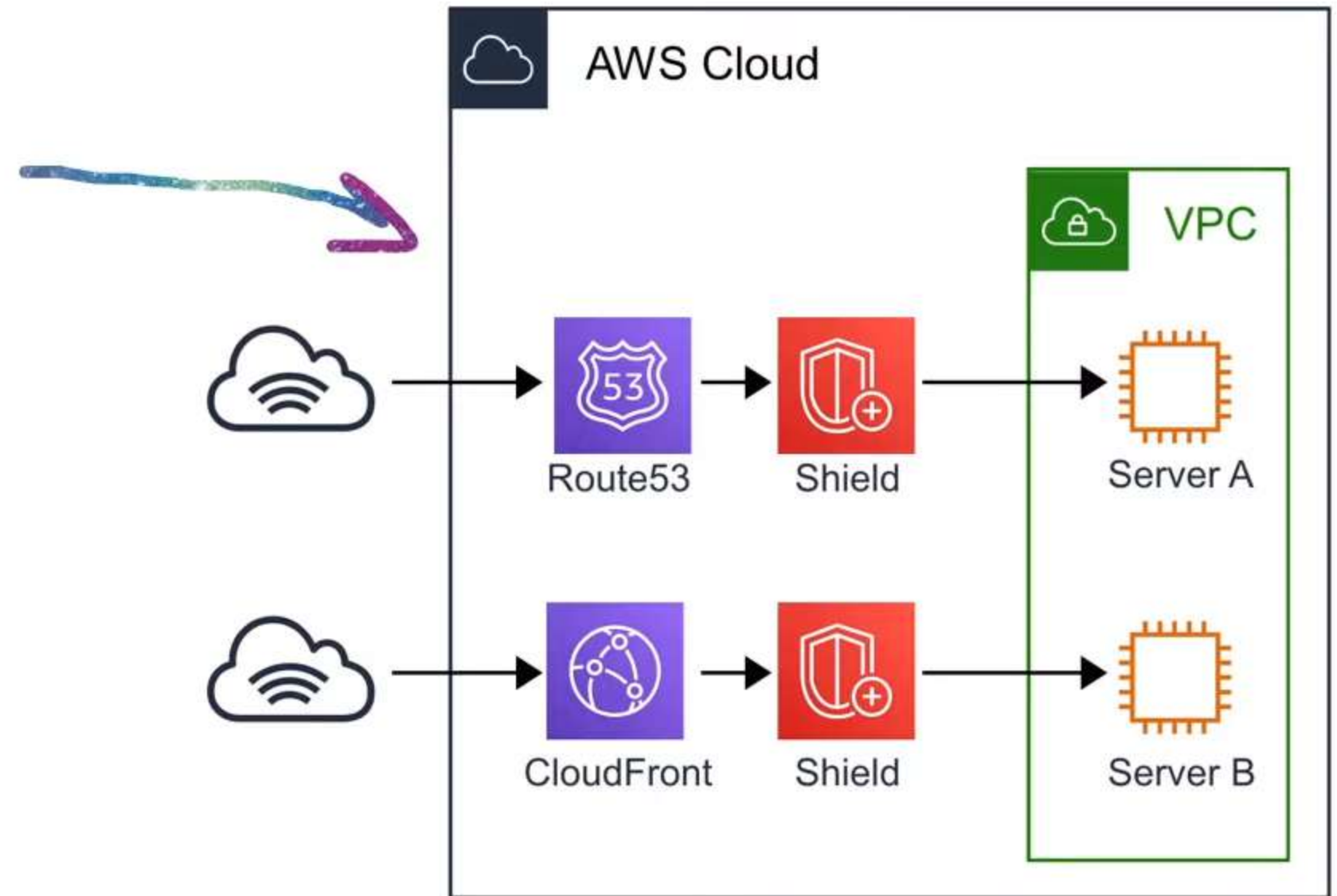


AWS Shield is a **managed** DDoS (Distributed Denial of Service) protection service that safeguards applications running on AWS

When you route your traffic through **Route53** or **CloudFront** you are using **AWS Shield Standard**

Protects you against **Layer 3, 4 and 7** attacks

- 7 Application
- 4 Transport
- 3 Network





# AWS Shield

Cheat sheets, Practice Exams and Flash cards  [www.examprompro.co/clf-c01](http://www.examprompro.co/clf-c01)

## Shield Standard FREE

### protection against most common DDoS attacks

- access to tools and best practices to build a DDoS resilient architecture.
- Automatically available on all AWS services.

## Shield Advanced \*3000 USD / Year

### additional protection against larger and more sophisticated attacks

#### Available On

- Amazon Route 53
- Amazon CloudFront
- Elastic Load Balancing
- AWS Global Accelerator
- Elastic IP (Amazon EC1 and Network Load Balancer)

#### Notable Features

- Visibility and Reporting on Layer 3,4 and 7
- Access to Team and Support (with Business or Enterprise Support)
- DDoS Cost Protection
- Comes with SLA



Both plans integrate with AWS Web Application Firewall (WAF) to give you Layer 7 (Application) protection





# Amazon Guard Duty

Cheat sheets, Practice Exams and Flash cards 🖱️ [www.exampopro.co/clf-c01](http://www.exampopro.co/clf-c01)

## What is IDS/IPS?

Intrusion Detection System and Intrusion Protection System.

A device or software application that monitors a network or systems for malicious activity or policy violations.



**Guard Duty** is a **threat detection service** that continuously monitors for malicious, suspicious activity and unauthorized behavior. It uses Machine Learning to analyze the following AWS logs:

- CloudTrail Logs
- VPC Flow Logs
- DNS logs

It will alert you of **Findings** which you can automate a incident response via CloudWatch Events or with 3rd Party Services

Policy: IAMUser/RootCredentialUsage 🔍 ⌵  
Finding ID: dcbe0ca20e68085ad8a0c8e049659217 [Feedback](#)

**Low** API DescribeAccount was invoked using root credentials from IP address 104.194.51.113. [Info](#)

[Investigate with Detective](#)

**Overview**

Severity	LOW	🔍 ⌵
Region	us-east-1	
Count	36	
Account ID	123456789012	🔍 ⌵
Resource ID	No information available	
Created at	09-24-2021 15:24:26 (a month a...	
Updated at	09-24-2021 16:59:21 (a month a...	