

19  
APR 2020

## WHAT IS DATA ENCRYPTION? WHICH ALL ARE THE TOP ENCRYPTION ALGORITHMS?

Created: Jan 17, 2020

Cyber Security

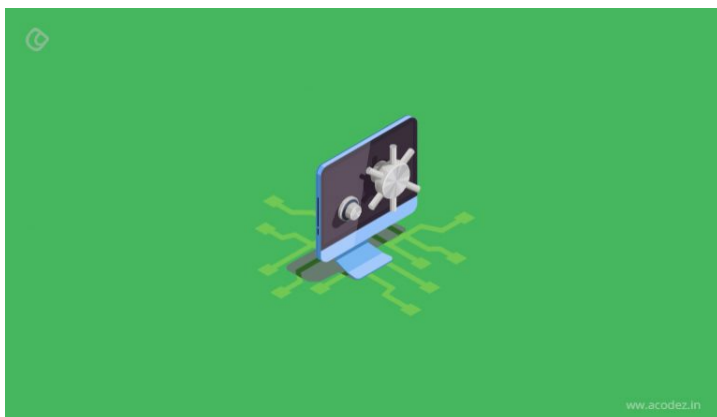
### Table of Contents

#### 1. What Is Data Encryption?

#### 2. Strongest Data Encryption Algorithms

- 2.1. Triple Data Encryption Standard (TripleDES)
- 2.2. Blowfish Encryption Algorithm
- 2.3. Twofish Encryption Algorithm
- 2.4. Advanced Encryption Standard (AES)
- 2.5. IDEA Encryption Algorithm
- 2.6. MD5 Encryption Algorithm
- 2.7. HMAC Encryption Algorithm
- 2.8. RSA Security

## What Is Data Encryption?



Secure data transfer is a paramount activity for PC users and business owners

Albeit you do not possess a lot in your personal or business account, securing the little you have is noteworthy.

Technology experts have unveiled numerous forms of securing data transfer, but data encryption is the commonest and easiest method that every PC user should be aware of and able to use.

By encryption, the data is “scrambled” such that an unintended person cannot read it.

Data encryption involves the translation of data into a format such that only the intend persons who have a decryption key, also referred to as a secret key will be able to read it.

Before encryption, the data is referred to as plaintext while after encryption the data is termed as [ciphertext](#).

Data encryption is purposely executed to secure confidential information during storage or when being transferred from one computer system to another.

Today, new encryption algorithms have been developed to replace the out-of-date DES – data encryption standard – where the former plays a very significant role in securing information and computing systems.

The modern encryption tools come with confidentiality properties such as data integrity, data authentication as well as non-cancellation features.

By authentication, the sender of the data is identified and verified; the integrity feature proves that the content of the information is not distorted while the non-cancellation property ensures that the person who sends the information cannot repudiate transferring it.

The earliest forms of data encryption were primitive; some involved changing letters in the sentence. This rendered the whole sentence absolutely unreadable and required a lot of time to figure out what the spewed characters meant.

With time, people discovered how to crack codes, and the encryption technique required more sophistication to ensure that the message was kept private.

Today, data encryption algorithms find extensive application in [File Transfer Protocol](#) (FTP) transfers and computer systems to offer protected transfers.

When the algorithms are used for transfers, the information is initially transformed into an unreadable ciphertext and sent in this format, upon which the receiver uses a secret key or a password to decode the ciphertext into its initial format.

In case an intruder accesses the file before reaching the final computer, they cannot read it as it is encrypted.

---

also  
Read

[RASP Application Security to Prevent Attacks](#)

---



There are several data encryption algorithms available:

- TripleDES
- Twofish encryption algorithm
- Blowfish encryption algorithm
- Advanced Encryption Standard (AES)
- IDEA encryption algorithm
- MD5 encryption algorithm
- HMAC encryption algorithm
- RSA security

## Triple Data Encryption Standard (TripleDES)

This form of data encryption algorithm applies block cipher algorithms thrice to all the data blocks individually.

The magnitude of the key is enlarged to provide extra protection by increasing the encryption ability.

Every individual block constitutes of 64-bit data. In this encryption algorithm, three keys are used where each key constitutes of 56 bits.

A total of three key permutations are provided under this standard:

- Option #1: the three keys are independent
- Option #2: keys 1 and 2 are independent
- Option #3: the three keys are similar

Most importantly, we call #3 triple DES whose key length consists of ( $3 \times 56$  bits = 168 bits) whereas key security consists of ( $2^{56}$  bits =

The substantially longer key length of this type of encryption algorithms overpowers other encryption techniques.

Nevertheless, after the development of the advanced encryption standard (AES), TripleDES has been rendered old-fashioned.

---

also  
Read

[Post Quantum Crptography](#)

---

## Blowfish Encryption Algorithm

Developed in 1993, the Blowfish encryption algorithm is an alternative for Data Encryption Standard (DES).

Before its creation, encryptions were performed by patents and intellectual properties of firms.

The developer placed the protocol to the public to make it readily available for any interested user.

Compared to DES, it is substantially faster and offers better encryption security.

It is an asymmetric type of encryption protocol: uses a single key for both encryption and decryption.

Like Twofish, it is a block cipher and its block size is 64-bit and the key size lies anywhere between 32 – 448 bits.

It features 18 subkeys, sixteen rounds and has four S-boxes.

Its protection capability has been examined and proved.

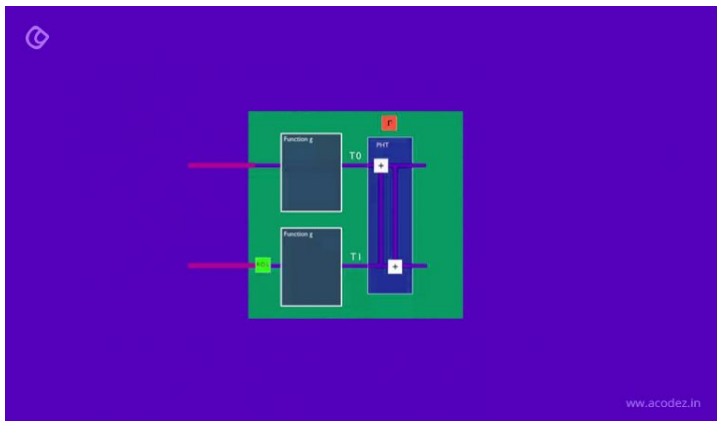
Considering blowfish standard is regarded as a [Feistel cipher](#), a single structure is used to encrypt and decrypt data provided that the reverse direction of the round keys is considered.

It is a significantly fast operation because it involves a relatively small number of rounds as well as its clarity of functionality.

Nevertheless, its key-scheduling consumes a lot of time, although it has an upper hand when it comes to protecting brute-force threats.

Also, its 64-bit block length (size) is rather small making it endangered by birthday attacks compared to AES whose block size is 128 bits and above.

## Twofish Encryption Algorithm



This form of the encryption algorithm is a [symmetric key block cipher](#) which is characterized by 128-bit block size and whose keys' size can run up to 256 bits.

This protocol uses one key for encryption and decryption.

It is a fast and flexible standard for eight-bit and thirty two-bit CPUs, and small smart cards.

The protocol works exemplarily in hardware and has numerous functionality commutations between the speed of encryption and the setup time making it distinctive amongst other protocols.

The standard shares some features with its predecessor, blowfish Encryption Algorithm and AES.

At one time, this encryption algorithm was a real contestant for the best encryption standard, but the present AES beat it out.

This algorithm bears several peculiar characteristics that distinguish it from other standards.

First, this cryptographic protocol applies substitution-boxes, S-boxes that are pre-computed and key-reliant.

This implies that despite the provision of the S-box, it relies on the cipher key for the decryption of the encrypted data.

The significance of the S-box is to conceal the key connection with the ciphertext.

Secondly, the Twofish encryption standard is accepted as a substantially secure alternative.

Encryption protocols whose keys have 128 bits and above are regarded as safe from attacks: Twofish has a block size of 128 bits.

Twofish protocol comes with several options.

To execute fast encryption, the key setup time can be made longer; this is done when the amount of data (plaintext) to be encrypted is relatively large.

The encryption can be made slower by setting a shorter key setup time when short blocks with constantly alternating keys are to be encrypted.

also  
Read[Rise of Tokenization](#)

## Advanced Encryption Standard (AES)

AES is the most popular and broadly used symmetric encryption standard today.

Due to the DES's small key size and low computing capability, a replacement was required which led to the development of AES.

Compared with TripleDES, it has been proved to be more than six times faster.

Concerning cybersecurity, the AES acronym, in particular, keeps popping up on all computer screens as it is the world's most accepted encryption standard.

It is seen while using messaging applications such as Signal and Whatsapp, computer platforms such as VeraCrypt and other technologies commonly used.

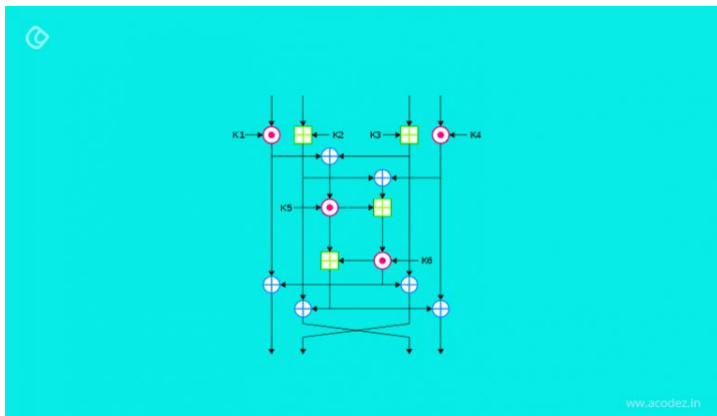
The AES standard constitutes 3 block ciphers where each block cipher uses cryptographic keys to perform data encryption and decryption in a 128-bit block.

A single key is used for encryption and decryption thus both the sender and receiver have the same key.

The sizes of the keys are considered adequate to secure the classified data to a satisfactory secret level.

also  
Read[Major Mobile App Security Issues](#)

## IDEA Encryption Algorithm



The international data encryption algorithm abbreviated as IDEA is a symmetric block cipher data encryption protocol.

Of the numerous years, this protocol has been in the market, there is no single attack that has been published in spite of the numerous trials to identify them.

The standard was patent in the US and Europe. It is used for non-commercial purposes while commercial authentication can be accessed from Ascom-Tech.

Typically, the block cipher runs in round blocks. It applies fifty-two subkeys where each has a 16-bit length.

Two subkeys are applied for a single round, four subkeys are applied prior to and after every round.

Typically, both the plain text and the ciphertext have equal sizes of 16 bytes.

---

also  
Read

[Protection for Mobile Banking and Payment Apps](#)

---

## MD5 Encryption Algorithm

This protocol was purposely developed to offer data security as it can take inputs of arbitrary size to generate a 128-bit hash value output.

Under this protocol, the encryption technique follows 5 phases where every phase features a predefined task.

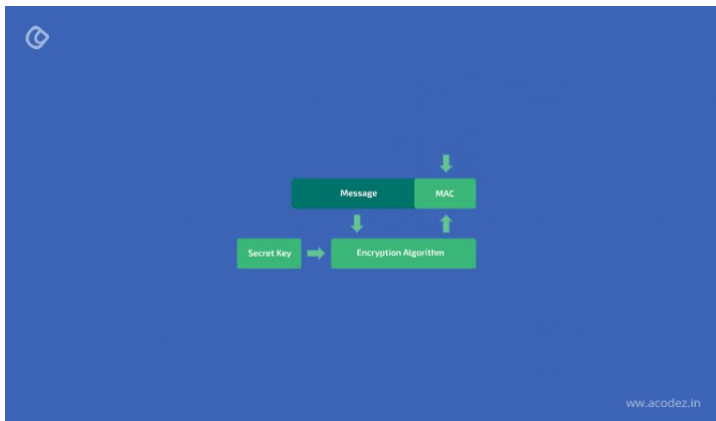
The five steps include:

- append padding (adding additional bits to the input) bits
- append the length
- initializing MD buffer
- message processing
- output

One notable advantage of MD5 is that the protocol allows the generation of a message digest using the initial message.

Nevertheless, the protocol is relatively slow.

## HMAC Encryption Algorithm



HMAC stands for hash message authentication code and it is applied to ascertain the message integrity and authenticity.

The protocol applies 2 hash computation passes and a cryptographic key.

This standard resembles most digital signatures only that symmetric keys are used in HMAC whereas asymmetric types of keys are used in digital signatures.

## RSA Security

This standard offers protection against [cyber-attacks](#) by detecting and responding to threats, preventing online fraud, management identification, et al.

Its data encryption is founded on the application of both a public key as well as a private key.

RSA algorithm generates the two keys simultaneously.

When the computer is running on a secure website, the protocol generates a public key that is available publicly for data encryption.

On the other hand, the encrypted text is decrypted using the private key. Sender identification is done with the aid of the public key.

In conclusion, whether securing your communication information or CVs on your PC, you should use some form of encryption as a protection tool. This way, your data is protected and you will have the convenience when you need to access it.

Acodez is a renowned website development and [web design company in India](#). We offer all kinds of web design and web development services to our clients using the latest technologies. We are also a leading [digital marketing company](#) providing SEO, SMM, SEM, Inbound marketing services, etc at affordable prices. For further information, please contact us.

Looking for a good team  
for your next project?

Contact us and we'll give you a preliminary free consultation  
on the web & mobile strategy that'd suit your needs best.





## Rithesh Raghavan



Rithesh Raghavan, Co-Founder, and Director at Acodez IT Solutions, who has a rich experience of 16+ years in IT & Digital Marketing. Between his busy schedule, whenever he finds the time he writes up his thoughts on the latest trends and developments in the world of IT and software development. All thanks to his master brain behind the gleaming success of Acodez.

[View all blogs](#)

### Recent Posts

### Popular Posts

Top 9 Advantages of Flutter: An Ultimate Guide

How the Black Swan Event of 2020 is Affecting eCommerce

What is Social Engineering? What are the Various Types of it?

Top Python Libraries to help you Perform Machine Learning Tasks

AWS vs Azure vs Google Cloud: A Comparison of All Platforms

## Categories

Acodez Interview Series

AI and ML

Big Data

Blockchain

Branding

Cyber Security



- Infographics
- Life At Acodez
- Mobile Application
- UX & UI Design
- Web Design
- Web Development

Archives

2020	▼
2019	▼
2018	▼
2017	▼
2016	▼
2015	▼
2014	▼
2013	▼

Get a free quote!

Brief us your requirements & let's connect

Your Name

Your Email Address

Contact Number

//

Send Message



### What is Social Engineering? What are the Various Types of it?

Posted on Jun 11, 2020 | [Cyber Security](#)



### The Cybersecurity Skills Gap – A Statistical Guide

Posted on Jun 03, 2020 | [Cyber Security](#)



### All About Cyber-Attacks on Mobile Devices and How to Protect Against Them?

Posted on May 26, 2020 | [Cyber Security](#)

Checkout our UX Design related services

Interaction Design

Information Architecture

Mobile UX Design

Leave a Comment

Your email address will not be published. Required fields are marked \*

Name \*

Email address \*

Company

Comments

Post Comments

Let's talk about what we can build together

Whatever may be your requirement - be it a simple website design, a complex data driven web application development, an ecommerce website, a native or cross platform mobile app development, a logo and brand identity design, a video production or a full fledged digital marketing campaign - we have a solution for you.

Contact us now for a free quote!

Delhi NCR

1101 - 11th Floor  
JMD Megapolis, Sector-48  
Gurgaon, Delhi NCR - India

<

Google Maps

Mumbai

1st floor, Urmi Corporate  
Park  
Solaris (D) Opp. L&T Gate  
No.6  
Powai, Mumbai- 400072

Google Maps

Bangalore

#12, 100 Feet Road  
Banaswadi,  
Bangalore 5600432


Google Maps


Calicut (S

UL CyberPark  
Nellikode (PO)  
Kerala, In >


Google Maps

Contact Us


 info@acodez.in

 acodez

+91 95 44 66 99 44



Quick Enquiry●Quick Enquiry



https://acodez.in/data-encryption-algorithms/

12/13



## Newsletter

Your Email address

Subscribe Now!

Enter your email ID above to subscribe to our newsletter.

©2020 All rights reserved to Acodez

[Terms & Conditions](#) | [Privacy Policy](#)