

[Home](#) > [Resources](#) > [Cyber Security](#) > What Is AES Encryption and How Does It Work?

What Is AES Encryption and How Does It Work?

By [Simplilearn](#)

Last updated on May 30, 2022

 32316



Table of Contents

[Why Was the AES Encryption Algorithm necessary?](#)

[What is the Advanced Encryption Standard?](#)

[What are the Features of AES?](#)

[How Does AES Work?](#)

[What Are the Applications of AES?](#)

[View More](#)



daily life applications. So far, the Advanced Encryption Standard has achieved the targets placed during its inception. And it has a long way to grow.

Why Was the AES Encryption Algorithm necessary?

When the [Data Encryption](#) Standard algorithm, also known as the DES algorithm, was formed and standardized, it made sense for that generation of computers. Going by today's computational standards, breaking into the [DES algorithm](#) became easier and faster with every year, as seen in the image below.



A more robust algorithm was the need of the hour, with longer key sizes and stronger ciphers to break into. They created the triple DES to fix this problem, but it never became mainstream because of its relatively slower pace. Thus, the Advanced Encryption Standard came into existence to overcome this drawback.

PGP in Cyber Security With Modules From MIT SCC

Your Cyber Security Career Success Starts Here!

[VIEW COURSE](#)

What is the Advanced Encryption Standard?

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext.

It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).



What are the Features of AES?

1. **SP Network:** It works on an SP network structure rather than a Feistel cipher structure, as seen in the case of the DES algorithm.
2. **Key Expansion:** It takes a single key up during the first stage, which is later expanded to multiple keys used in individual rounds.
3. **Byte Data:** The AES encryption algorithm does operations on byte data instead of bit data. So it treats the 128-bit block size as 16 bytes during the encryption procedure.
4. **Key Length:** The number of rounds to be carried out depends on the length of the key being used to encrypt data. The 128-bit key size has ten rounds, the 192-bit key size has 12 rounds, and the 256-bit key size has 14 rounds.

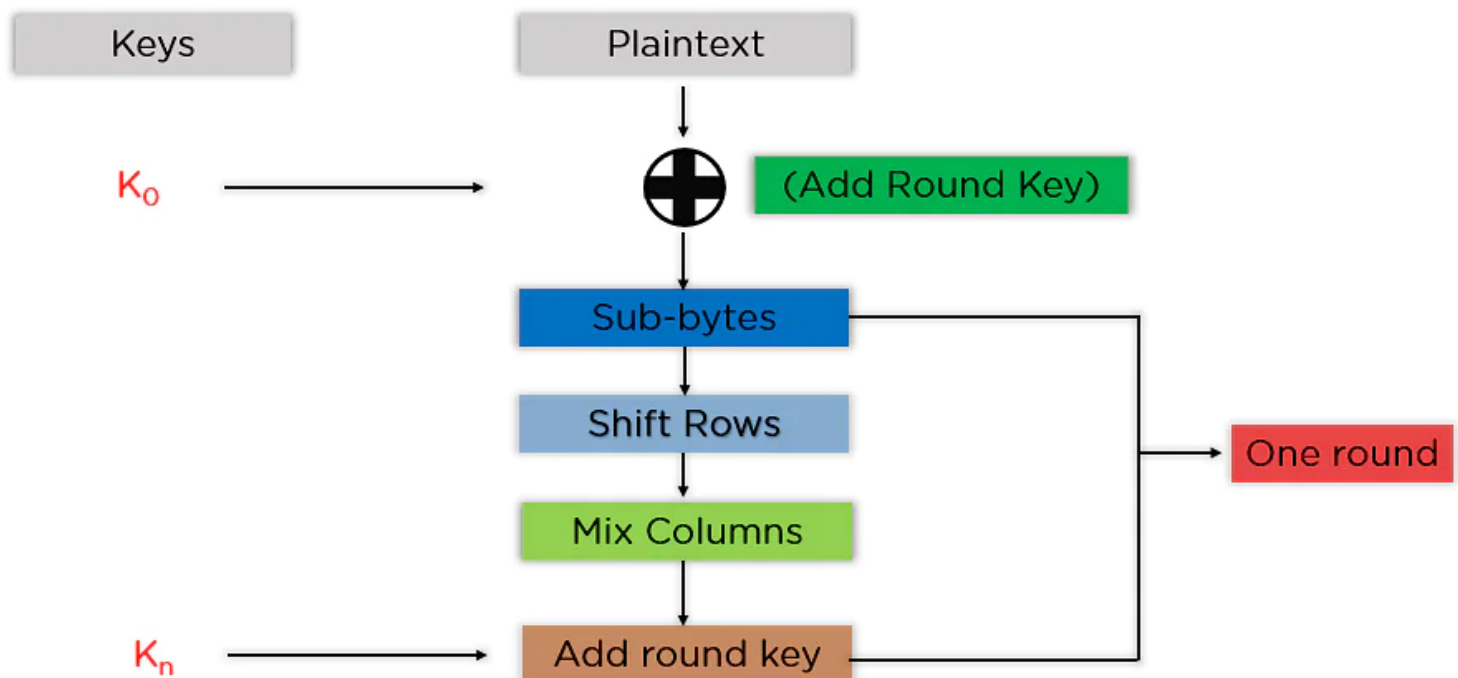
How Does AES Work?

To understand the way AES works, you first need to learn how it transmits information between multiple steps. Since a single block is 16 bytes, a 4x4 matrix holds the data in a single block, with each cell holding a single byte of information.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

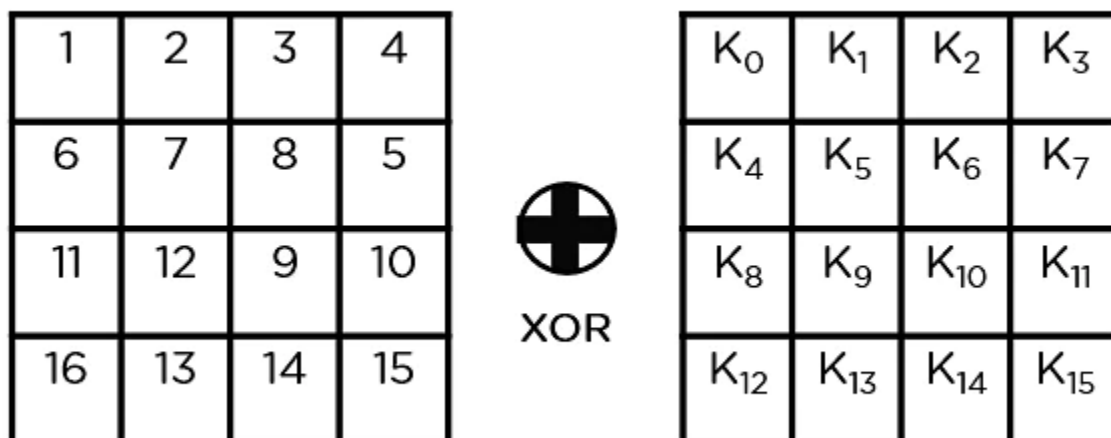


The steps to be followed in AES are in the below image.



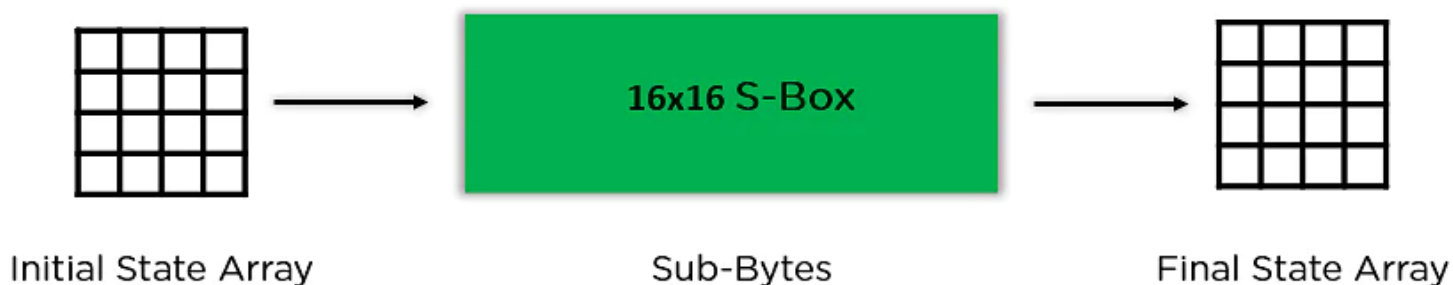
The mentioned steps are to be followed for every block sequentially. Upon successfully encrypting the individual blocks, it joins them together to form the final ciphertext. The steps are as follows:

- **Add Round Key:** You pass the block data stored in the state array through an XOR function with the first key generated (K_0). It passes the resultant state array on as input to the next step.



- **Sub-Bytes:** In this step, it converts each byte of the state array into hexadecimal, divided into two equal



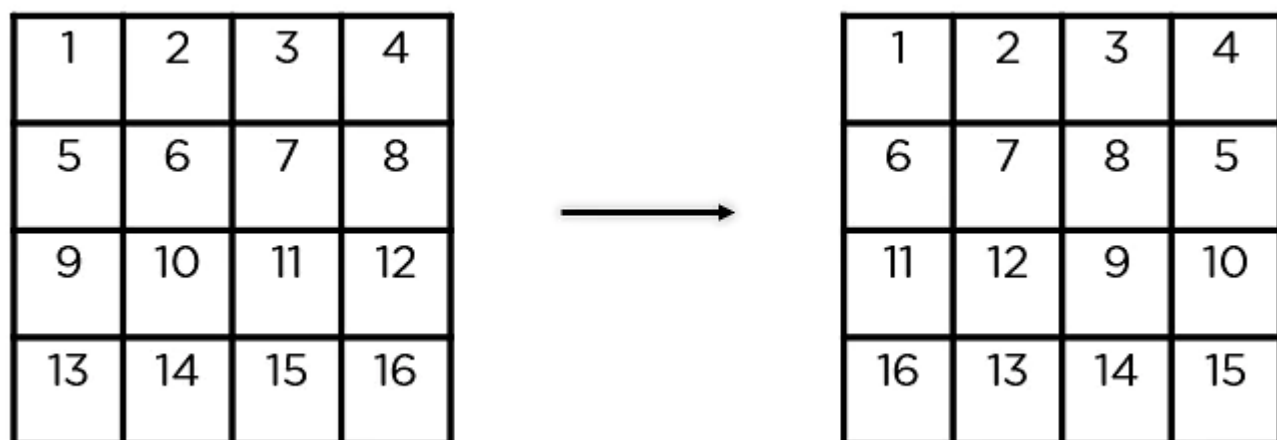


FREE Course: Introduction to Cyber Security

Learn and master the basics of cybersecurity

ENROL NOW

- **Shift Rows:** It swaps the row elements among each other. It skips the first row. It shifts the elements in the second row, one position to the left. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.



- **Mix Columns:** It multiplies a constant matrix with each column in the state array to get a new column for the subsequent state array. Once all the columns are multiplied with the same constant matrix, you get your new state array for the next step. This particular step is not to be done in the last round.



$$\begin{array}{|c|c|c|c|} \hline 5 & 6 & 7 & 8 \\ \hline 9 & 10 & 11 & 12 \\ \hline 13 & 14 & 15 & 16 \\ \hline \end{array} \times \begin{array}{|c|} \hline C_1 \\ \hline C_2 \\ \hline C_3 \\ \hline \end{array} = \begin{array}{|c|} \hline NC_1 \\ \hline NC_2 \\ \hline NC_3 \\ \hline \end{array}$$

Constant Matrix Old Column New Column

- **Add Round Key:** The respective key for the round is XOR'd with the state array is obtained in the previous step. If this is the last round, the resultant state array becomes the ciphertext for the specific block; else, it passes as the new state array input for the next round.

$$\begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 6 & 7 & 8 & 5 \\ \hline 11 & 12 & 9 & 10 \\ \hline 16 & 13 & 14 & 15 \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|} \hline K_0 & K_1 & K_2 & K_3 \\ \hline K_4 & K_5 & K_6 & K_7 \\ \hline K_8 & K_9 & K_{10} & K_{11} \\ \hline K_{12} & K_{13} & K_{14} & K_{15} \\ \hline \end{array}$$

XOR

Now that you understand the basic steps needed to go through the encryption procedure, understand this example to follow along.

Plaintext – Two One Nine Two

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	43	69	6E	25	20	54	77	6F

Plaintext in Hex Format

54 77 6F 20 4F 6E 65 20 43 69 6E 25 20 54 77 6F



P	l	a	i	n	t	s		m	a	k	i	n	g		P	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75	

Encryption Key in Hex Format

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

As you can see in the image above, the plaintext and encryption convert keys to hex format before the operations begin. Accordingly, you can generate the keys for the next ten rounds, as you can see below.

Keys generated for every round

- Round 0: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- Round 1: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
- Round 2: 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
- Round 3: D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
- Round 4: A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
- Round 5: B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
- Round 6: BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
- Round 7: CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
- Round 8: 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
- Round 9: BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
- Round 10: 28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

You need to follow the same steps explained above, sequentially extracting the state array and passing it off as input to the next round. The steps are as follows:

Cybersecurity Expert Master's Program

Master the Skills of a Cybersecurity Professional

[VIEW COURSE](#)

54	4F	4E	20
77	6E	69	54
6F	65	6E	77
20	20	65	6F

Plaintext



XOR

54	73	20	67
68	20	4B	20
61	6D	75	46
74	79	6E	75

Round 0 Key

00	3C	63	47
1F	4E	22	74
0E	08	1B	31
54	59	0B	1A

New State Array

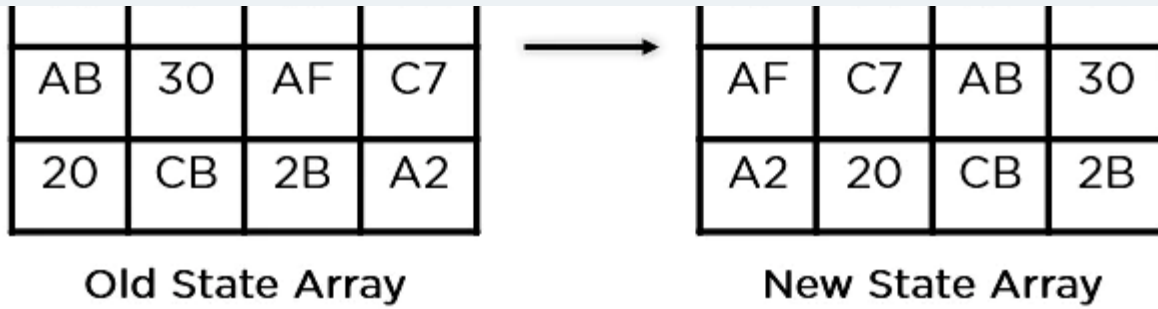
- Sub-Bytes: It passes the elements through a 16x16 S-Box to get a completely new state array.

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

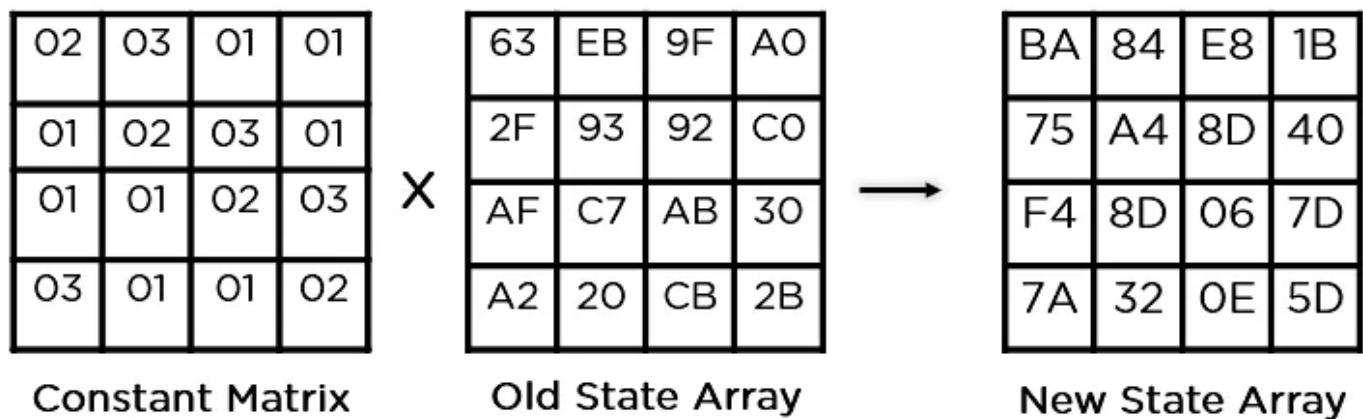
New State Array

- Shift Rows:

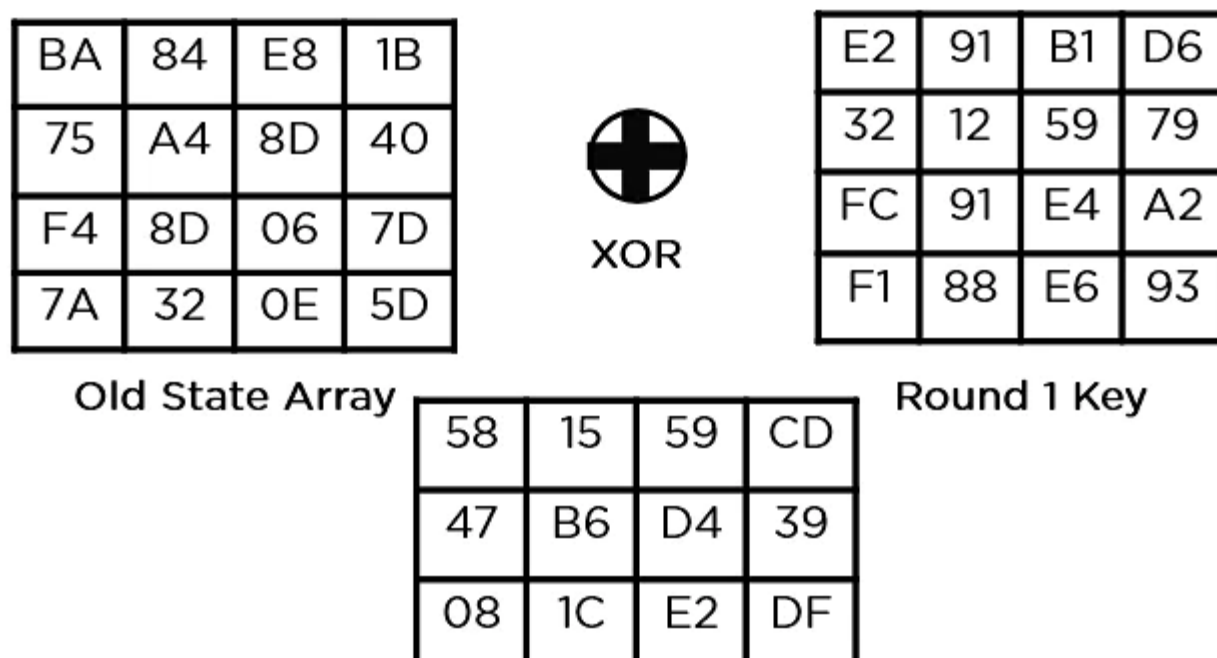




- Mix Columns:



- Add Round Key:



This state array is now the final ciphertext for this particular round. This becomes the input for the next round. Depending on the key length, you repeat the above steps until you complete round 10, after which you receive the final ciphertext.

Final State Array after Round 10

29	57	40	1A
C3	14	22	02
50	20	99	D7
5F	F6	B3	3A

AES Final Output

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A



Ciphertext

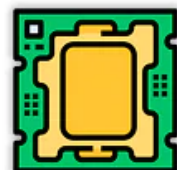
Now that you understand how AES works, go through some of the applications of this encryption algorithm.

Cybersecurity Bootcamp

Certificate and Masterclasses From UCI DCE

EXPLORE NOW



**Wireless security****Encrypted browsing****General file encryption****Processor security**

The applications of the AES Encryption algorithm are as follows:

1. **Wireless Security:** Wireless networks are secured using the Advanced Encryption Standard to authenticate routers and clients. WiFi networks have firmware software and complete security systems based on this algorithm and are now in everyday use.
2. **Encrypted Browsing:** AES plays a huge role in securing website server authentication from both client and server end. With both [symmetric](#) and [asymmetric encryption](#) being used, this algorithm helps in SSL/TLS encryption protocols to always browse with the utmost security and privacy.
3. **General File Encryption:** Apart from corporate necessities, AES is also used to transfer files between associates in an encrypted format. The encrypted information can extend to chat messages, family pictures, legal documents, etc.
4. **Processor Security:** Many processor manufacturers enable hardware-level encryption using the likes of AES encryption to bolster security and prevent meltdown failures, among other low-profile risks.

Now that you learned about the applications of AES encryption, take a look at its upgrades over its predecessor, the DES encryption algorithm.

Differences Between AES & DES



Key Length - 56 bits	Key Length - 128, 192, 256 bits	
Block Size - 64 bits	Block size - 128 bits	
Fixed no. of rounds	No. of rounds dependent on key length	
Slower and less secure	Faster and more secure	

Grab the opportunity to be a part of the MIT CSAIL Professional Programs community and interact with your peers. Attend masterclasses from MIT faculty in our [PGP in Cyber Security](#) and expedite your cybersecurity career in no time!

How Can Simplilearn Help You?

With this, you have seen the impact AES Encryption has on the global stage, with many systems needing a secure channel of authentication as DES collapsed. With many bases to cover in cybersecurity, cryptography is one of the most crucial aspects, even though several other topics are essential to excel as a cybersecurity expert.

Simplilearn offers a [“Cybersecurity Expert”](#) course designed to equip you with all the skills necessary to start or promote your career in cybersecurity. It doesn’t have any academic pre-requirements, and the introductory module will prepare beginners for the course ahead. Training for highly sought-after certifications like [CompTIA Security+](#), [CEH](#), [CISM](#), and [CISSP](#) is at the forefront of this course, preparing you for the best jobs being offered in the industry.

Conclusion



This tutorial explores the need for AES Encryption, its origin and process of encryption, all the way up to its

cybersecurity, Simplilearn’s [Cyber Security Expert Master’s](#) program should be a great fit for you. Featured as the Best Cybersecurity Bootcamp in 2021 by [Course Report](#), this program covers all the fundamental and advanced aspects of cybersecurity and provides you the right job-ready training you need to become a world-class cybersecurity expert today. Explore the program today.

Do you have any questions for us regarding this AES encryption tutorial? Please don't hesitate to mention them in the comment section of this tutorial, and we'd be happy to have our experts answer them for you.

About the Author



Simplilearn is one of the world’s leading providers of online training for Digital Marketing, Cloud Computing, Project Management, Data Science, IT, Software Development, and many other emerging ...

[View More](#)

Recommended Programs

Post Graduate Program in Cyber Security

★★★★★ | 1330 Learners

Lifetime Access*

Cyber Security Expert

★★★★★ | 6245 Learners

Lifetime Access*

*Lifetime access to high-quality, self-paced e-learning content.



NEXT ARTICLE




What Is Kerberos, How Does It Work, and What Is It Used For?

By Simplilearn

 143552


Jul 12, 2022

Recommended Resources








A Guide on How to become
A Site Reliability Engineer (SRE)


A Guide on How to Become a Site Reliability Engineer (SRE)




Data Encryption: Methods, Techniques, T...

0 Comments Simplilearn  Disqus' Privacy Policy  Melquiceded Balbi ▾

 Favorite 1  Tweet  Share Sort by Best ▾



Start the discussion... 

Disclaimer

- PMP, PMI, PMBOK, CAPM, PgMP, PfMP, ACP, PBA, RMP, SP, and OPM3 are registered marks of the Project Management Institute, Inc.

