Teach Computer Science

teachcomputerscience.com/encryption

KS3 Computer Science

11-14 Years Old

48 modules covering EVERY Computer Science topic needed for KS3 level.

View KS3 Resources →

GCSE Computer Science

14-16 Years Old

45 modules covering EVERY Computer Science topic needed for GCSE level.

View GCSE Resources →

A-Level Computer Science

16-18 Years Old

66 modules covering EVERY Computer Science topic needed for A-Level.

View A-Level Resources →
Home / Internet / Encryption

The evolution of technology brought individuals and industries on a unique link. Anybody can visit and proceed with transactions using networks. The internet is one of the key sources to link all the agencies on a single platform. Clients using networking facilities have a great belief that their private information and transactions are secure. This is all due to the significant impact of “encryption”.

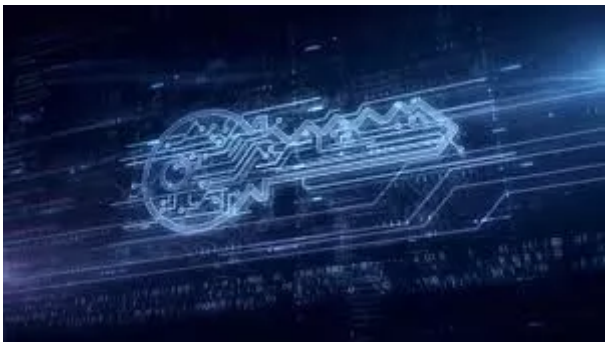

Figure 1: Data Encryption

Encryption Working:

The purpose of the encryption is to scramble the information as it can only be accessed or understood by authorized parties. The data is altered from ordinary text to ciphertext.

We can make it more clear by a real-life example. Suppose a person contains a box with few documents inside it. The person takes care of the box and puts this box into a lock. After a few days, the person dispatches this box of documents to his/her friend. The friend also retains the same key. This means that the sender and receiver both contain a similar key. The friend now has the authority to open the box and access the document. The process of encryption is the same as we have discussed in the example. Nevertheless, encryption is done on digital signals. This electronic process aims to keep the third party away from understanding the hidden information in the signal.

Online consumers perform transactions for product purchasing. Millions of online services are available to facilitate various skilled personnel to accomplish their tasks. Moreover, most of the websites require a significant identity to access these services that require personal details. Keeping such information safe and sound is one of the prevalent approaches known as “encryption”.

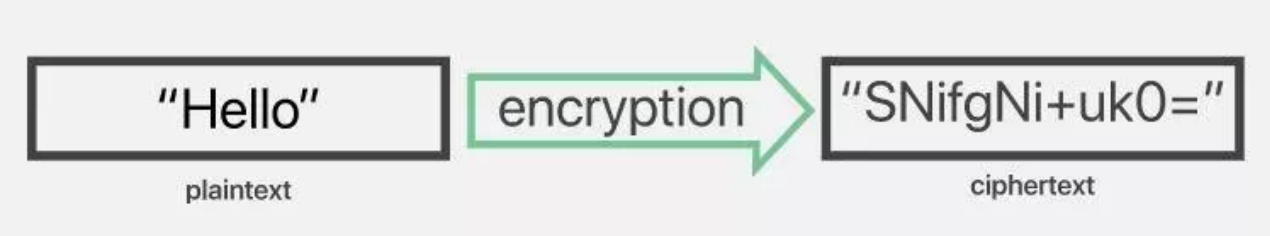

Figure 2: Encryption Processing

Encryption directly relates to the security of the networks. Encryption is helpful to hide data, information, and contents that a normal human cannot understand. The encrypted information can be converted to its original state after the decryption process as both the encryption and decryption are an effective method of cryptography that is a scientific process to perform secure communication. There exist various algorithms to process encryption and decryption of data. However, “keys” are also used to avail of high-level data protection.

The encryption process contains three levels of working.

1. Normal Text
2. Text Encryption (Ciphered Text)
3. Text Decryption (Conversion of Ciphered Text to Normal Text)

Encryption Keys:

“Keys” consist of bits in a long sequence employed for the process of encryption and decryption. An encrypted form of data consists of a sequence of bits (keys) and the message’s content that is passed through a mathematical algorithm. One or more keys are used to restore the encrypted message utilizing a decryption algorithm.

1. Symmetric Encryption:

In cryptographic algorithms, there exist a couple of techniques. Sometimes the algorithms use a unique key for encryption and decryption methods. There is a need to secure the unique key in such processes as the system or person familiar with the key has full authentication to decrypt the message for reading. In the domain of network encryption, this technique is known as “symmetric encryption”.

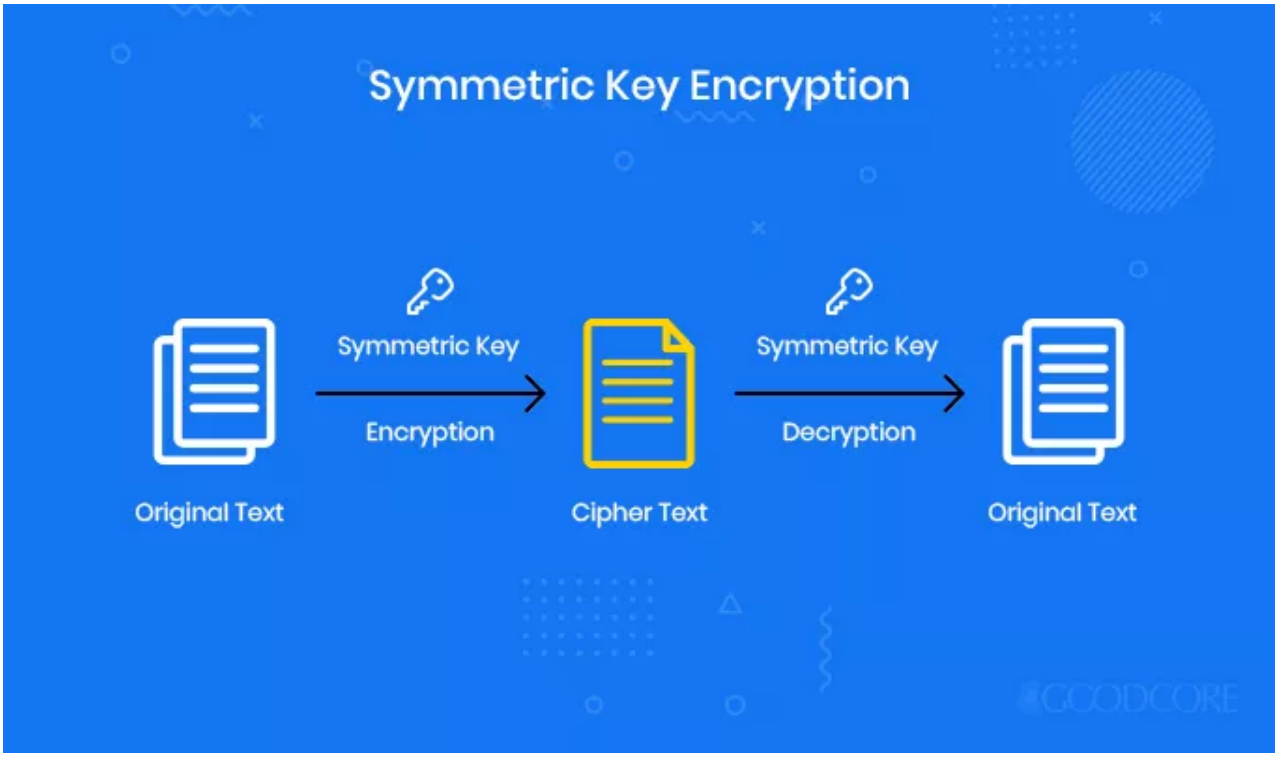

Figure 3: Symmetric Encryption Framework

2. Asymmetric Encryption:

However, some cryptography approaches use one key for encryption of the data and another key for the decryption of the data. So, keeping such a public message is of no means for anyone to decrypt or read that specific message. Most of the prevalent protocols related to security on the internet employ this kind of cryptography known as “public-key” encryption. This kind of encryption holds another name that is known as “asymmetric encryption”.

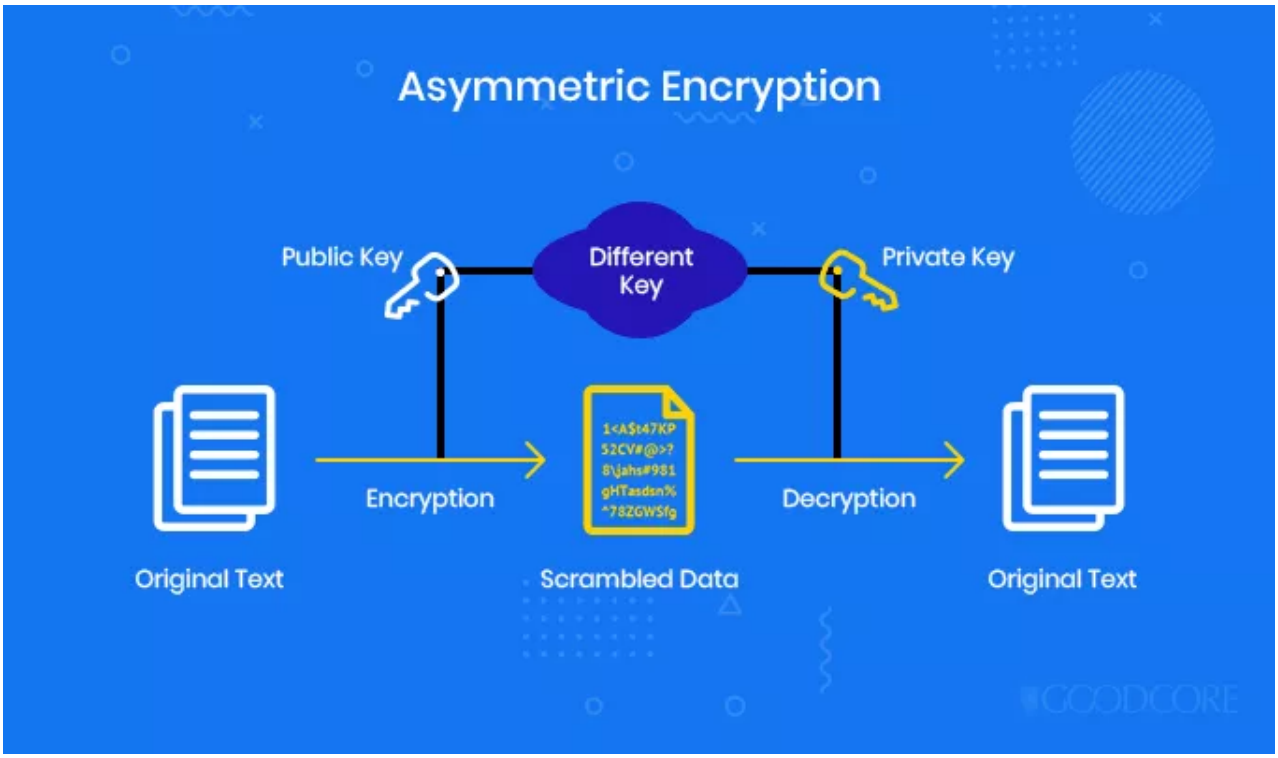

Figure 4: Asymmetric Encryption Framework

Encryption Categories:

1. Triple DES (TDES):

Triple DES is a typical name of the technique; however, its official name is the Triple Data Encryption Algorithm (TDEA). Symmetric encryption is employed for the smooth operation of Triple DES. The modern version of the Triple-DES is evolved on the DES block cipher. This encryption technique uses a 56-bit key. These keys are used triple times or thrice that makes it a 168-bit key. Functional operation of the Triple-DES algorithm is done in three different phases.

1. Data Encryption
2. Data Decryption
3. Re-Encryption of the data

Similarly, **decryption** of the three-phase encrypted data is performed as given below.

1. Data Decryption
2. Data Encryption
3. Repetition of Decryption

Triple DES is the most effective approach used for cryptography, but as encryption and decryption are carried out thrice, it consumes more time than the other approaches to encryption. Moreover, encryption in this approach is carried out in a small chunk, also known as shorter blocks, that can easily be decrypted during encryption or before completing the entire process of encryption. So, this encryption method is a bit risky, and

data thieving is easy. The approach was widely used and recommended before the evolution of other significant techniques. Triple DES is still part of a few organizations for the protection of data.

2. Advanced Encryption Standard (AES):

AES uses the phenomenon of symmetric encryption. This form of encryption is based on the Rijndael algorithm. The algorithm is developed by the National Institute of Standards & Technology in the United States. Therefore, AES has assumed a robust cryptography algorithm that gives the data's efficient security because it operates using a single private key.

In a single time, it deals with a fixed size of the data block and adopts the block-cipher technique for data encryption. The functionality of the algorithm is valid with 128-bit and considers ten rounds for data encryption. For 192-bit of data, there exist 12 rounds for encrypting the data. However, it can support up to 256-bit keys in extended mode.

3. Rivest–Shamir–Adleman (RSA):

RSA uses an asymmetric cryptography technique that operates with two keys.

1. Encryption with a public key.
2. Decryption with a private key.

It gives operation with 1024-bit; therefore, it is one of the best cryptography techniques. Key length can be extended up to 2048-bit. A higher value of key size will be more time consuming for encryption processing. RSA is considered the strongest algorithm for data encryption. Moreover, it is a certain type of encryption that is widely used over the internet. Compared with other encryption kinds, RSA retains a secured bond due to higher bits of keys; therefore, hackers cannot breach the boundary easily to access the data.

4. Blowfish:

Blowfish is used as a replacement for a data encryption algorithm (DES). This technique uses symmetric block cryptography. The operation is performed on varying numbers of key length that ranges from 32 – 448 bits. Data is divided into chunks of 64 – bit blocks as it uses the block cipher technique, so encryption and decryption are carried out accordingly.

Blowfish is developed for robust operation as well as publicly available without any cost. As the encryption algorithm is free, most researchers and agencies have tested its efficiency, data rate, and security and reported that the data had not been hacked using this approach. So, it is prevalent among e-commerce organizations to secure and secure payment processing and deal with private credentials.

5. Twofish:

Twofish uses an asymmetric form of the approach based on a block cipher. An algorithm is a modern form of the Blowfish method. The Twofish algorithm's block sizes are 128 – the bit that enables extension up to 256 – bit key. The data in this encryption type is also distributed into a specific length of chunks or blocks. To complete the encryption process, it performs 16 rounds on the data, nevertheless considering its length. It is a flexible algorithm that allows adjusting the keying setup greater for higher security and encryption process slow and vice versa. The kind of encryption is also freely available as well as performs fast performance during encryption. One of the significant features of this technique is a user control that is not available in any other kind of encryption. Advanced encryption standards (AES) have powerful data encryption features, but Twofish is also an asset for data encryption for plenty of users and industries.

6. Format Preserving Encryption (FPE):

This type of encryption is used to secure the format of the data. The encryption model (ciphertext) and the given text (plaintext) are uniforms. FPE is employed in the financial and economic organization like banking, audit firms and retail systems, etc.

Encryption Applications:

Till now, we have briefly discussed the basics and patterns of encryption. We will now briefly discuss data encryption applications that assure the content's health; the sent and received messages are not changed anywhere in the route.

1. Hashes:

After selecting a valid data encryption type, the client must notify the data's authenticity and verification. For this purpose, hashes are required. The one-way operation collects a large amount of data and makes smaller chunks of standard size. A unique fingerprint is created to verify the purity of data between the encryption levels. Results of the hashing technique are known as a hash value. If there is any doubt of alteration during data encryption, the original fingerprint can be matched with the one as the systems do not produce different hashes of the same data.

Using "username" and "password" for different web services are common examples. Servers monitor the associated hash values. A client enters a password hashed with a similar algorithm through which it was encrypted. The system will validate the authentication on that portal if the hash matches the previously saved hashed value.

2. Internet Encryption:

Advanced internet browsers employ the SSL protocol to perform a secure transaction. This type of secure protocol accomplishes the process of encryption by a public key; however, the process of decryption is done by a private key. The significant indicator of secure protocol or SSL resides in the prefix of a web URL that is written as HTTPS; this means that secure encryption is working on a website.

3. Home Networks Encryption:

Home networks have their unique protocols of security. The secure Wi-fi network uses WPA and WPA2 for encryption of data. Although these protocols are not as strong but are adequate for protecting the home networks. Home network encryption form can be analysed by checking broadband router configuration.

Encryption Challenges:

Today, brute force, or attempting random keys until the correct one is identified, is the most popular attacking encryption procedure. Of course, the duration of the key defines the potential number of keys and influences this form of attack's authenticity. It is necessary to remember that the encryption intensity directly relates to the key size, but the amount of resources needed to execute the calculation rises as the key size expands.

Side-channel assaults and cryptanalysis provide alternate means to cracking a cipher. Side-channel threats, rather than the real cipher itself, go for the cipher's implementation. Where there is a flaw in device architecture or implementation, these assaults appear to work. Similarly, cryptanalysis involves discovering and manipulating a flaw in the cipher. Where there is a weakness in the cipher itself, cryptanalysis is more likely to occur.

Encryption solutions:

Encryption of smartphones, addresses, and data may be supported through data security technologies for data encryption. These security operations are often faced with computer, email, and data access functionality in certain examples. As workers utilize external computers, removable files, and online apps increasingly frequently as part of their everyday business practices, businesses and organizations face the task of preserving records and avoiding data loss. When personnel transfer data to portable computers or transfer it to the cloud, confidential data can no longer be under the organization's supervision and security. Consequently, data leakage and the implementation of ransomware from removable and external computers and network and cloud software were avoided by the best data loss protection technologies. Therefore, they must ensure all computers and software are used correctly to do so and that knowledge is protected by auto-encryption even after it exits the company.

Although data encryption can sound like an overwhelming, complex task, it is done efficiently every day by endpoint security tools. Data encryption must not be like that the company is working on its own to overcome. Choose a top data loss protection program that provides computer, email, and application access with data encryption to ensure that the data is secure.

Encryption Advantages:

Everyone is nervous about the transition of confidential data to the cloud because several businesses consider that the cloud is not as reliable as their own data centre. It is feasible for outsiders to access it while data is in the cloud, but clients' and competitors' data

remain stored in the same storage place.

Due to the extreme cost and versatility, companies need the benefit of the cloud. The capacity to spin up or decommission servers when market requirements shift is part of this benefit. So, what happens if the service company asks to leave?

The virtualized contexts can provide multi-tenancy that includes greater flexibility and reduction in cost.

The service providers can access the data if they both contain encrypted data and keys used for encryption. To overcome this issue, processing data encryption in the cloud and preserving the encryption keys at the users' end make sense. Although certain companies, no matter how simple the key security solution is, do not consider handling encryption keys. They have queries about backup, affordability, and rehabilitation from disasters.

Consumers use Payment cards for various transactions and require protection of the card and its related data. Most card consumers understand that their information and data related to this card are safe and secure. Therefore, encryption is one of the effective approaches used by PCI DSS (Payment Card Industry Data Security Standard).

If a data breach exists and personal data is destroyed, the compromised group must contact the individuals who are affected. Any jurisdictions have public notice with a safe harbour provision if the intercepted data is secured and if the security keys are not breached. Therefore, in an infringement, installing encryption and comprehensive key protection might save plenty of revenue.

Plenty of businesses are now giving online services that contain virtual offices, which are not protected by their very existence. There is a very real possibility for the robbery of machines and storage. Many of these companies have insecure confidential data residing on these servers. Data encryption protects against data manipulation or unintentional destruction, and there are also greater capabilities for today's security technologies. Imagine sending cryptographic keys to remote data only during working hours, meaning that if the lights go out, the code is unusable to everyone.

Encryption Disadvantages:

Dealing with encryption is a well-known technique to keep the data secure from unauthorized individuals and agencies. One of the major benefits of encryption is to provide data access for such an agency that is familiar with the keys and passwords used for the encryption of data. However, below are the few disadvantages of data encryption that require special attention.

The user would be unable to explore the encrypted file if the password or key got the loss. However, using simpler keys in data encryption makes the data insecure, and randomly, anyone can access it.

Data encryption is a useful data security technique; therefore, it requires plenty of resources like data processing, time consumption, usage of various algorithms for encryption, and decryption. Therefore, it is a bit of an expensive technique.

It is possible to establish arbitrary expectations and specifications that might jeopardize data encryption protection if an enterprise may not recognize any of the limitations enforced by encryption techniques.

When the user layers it for current systems and software, data protection techniques can be challenging. This may adversely impact routine processes inside the device.

Summary and Facts:

What does data encryption mean?

Encryption directly relates to the security of the networks. Encryption is helpful to hide data, information, and contents that a normal human cannot understand. The encrypted information can be converted to its original state after the decryption process.

Write a line defining the purpose of the data encryption?

The purpose of the encryption is to scramble the information as it can only be accessed or understood by authorized parties. The data is altered from normal text to ciphertext.

What are the levels, occur in the working of data encryption?

The encryption process contains three levels of working.

1. Normal Text
2. Text Encryption (Ciphered Text)
3. Text Decryption (Conversion of Ciphered Text to Normal Text)

What are the two major types of data encryption?

1. Symmetric Encryption

2. Asymmetric Encryption

Write down the various categories of data encryption?

1. Triple DES (TDES)
2. Advanced Encryption Standard (AES)
3. Rivest–Shamir–Adleman (RSA)
4. Blowfish
5. Twofish
6. Format Preserving Encryption (FPE):

Write down the highlights of data encryption advantages?

1. Encryption helps move to the cloud
2. Easy access to decommission
3. Encryption aims to achieve stable cloud multi-tenancy
4. Encryption keys are a solid reason to secure data access from service providers.
5. Encryption assists the clients to meet regulations.
6. Encryption offers a secure shelter from warnings of attacks.
7. Encryption facilities data security for remote businesses

Write down the highlights of data encryption disadvantages?

1. Remembering or recording key/passwords when accessing the data
2. Consumes plenty of resources
3. Sometimes needs unrealistic requirements
4. Issue of compatibility

References: