The formation of symmetric standards

Introduction

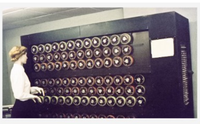
Secure communication and data exchange are critical concerns for individuals and businesses alike. One of the essential tools in ensuring secure communication is symmetric encryption, which, as you now know, involves using a single key for both data encryption and decryption.

In this reading, you will explore the formation of symmetric standards, with a focus on the Advanced Encryption Standard (AES). You'll review its various techniques and explore examples illustrating its importance in modern cryptography.

Symmetric Standards

The need for symmetric standards arose from the need for secure communication during World War II. The German Enigma machine was a cipher machine used to encrypt and decrypt messages. The Allies realized the importance of breaking the Enigma code to win the war. This led to the formation of the Government Code and Cypher School at Bletchley Park in the UK, where Alan Turing and his team developed the Bombe machine to break the Enigma code.

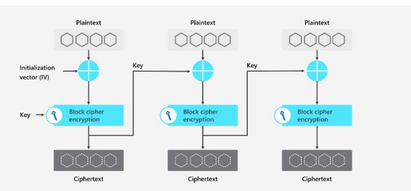
Enigma machine



Bombe machine

Symmetric encryption has been in use for decades and is a widely used technique in modern cryptography. The formation of symmetric standards started with the development of the Data Encryption Standard (DES), which was widely used until it was replaced with AES in the late 1990s.

The AES standard was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It was first published in 1998 and was adopted as a standard by the US National Institute of Standards and Technology (NIST) in 2001. AES uses a block cipher structure, which encrypts data in fixed-size blocks. The size of the block is 128 bits, and the key length can be 128, 192, or 256 bits. The key size determines the level of security provided by AES, with larger key sizes providing greater security.



Note: An Initialization Vector (IV) is a fixed-size input that is typically random or pseudorandom and used in cryptographic algorithms. It's often used in block cipher modes of operation, which are methods to apply a cipher to data that are larger than the cipher's block size.

AES techniques

AES has several advantages over DES. AES has a longer key length, making it more secure against brute-force attacks. AES is also faster and more efficient, making it suitable for use in modern computing systems. AES has become the legal standard for secure data transmission, and it is used in a wide range of applications, including online banking, e-commerce, and secure communication.

AES uses various techniques to ensure secure encryption, including key schedules, substitution-permutation networks, mix-column and shift rows operations:

- A **key schedule** is an essential tool that generates the round keys used in encryption and decryption and determines the strength of the encryption.
- A **substitution-permutation network (SPN)** structure consists of repeated rounds of substitution and permutation operations. These operations ensure that the input data is transformed in a non-linear way, making it difficult to decrypt without the key.
- A **mix-column** operation is used in the encryption and decryption process to ensure that the input data is mixed in a way that makes it difficult to decrypt without the key.
- A **shift rows** operation ensures that the data is shifted in a non-linear way.

AES modes of operations

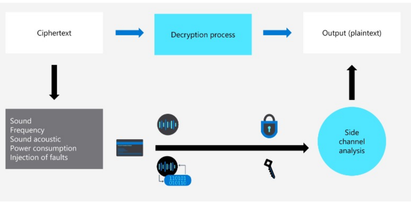
AES has several modes of operation, which are used to provide different levels of security and performance. The most commonly used mode is the Cipher Block Chaining (CBC) mode, which provides secure encryption and decryption of data blocks. Other modes include the Electronic Codebook (ECB) mode, which is used for encrypting small amounts of data, and the Counter (CTR) mode, which is used for streaming data.

Another technique used in AES is the Galois Counter Mode (GCM), which is a mode of operation for block ciphers. GCM is a combination of the Counter mode of encryption and the Galois field multiplication. GCM ensures the authenticity and confidentiality of the data being transmitted. GCM is widely used in secure communication protocols such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

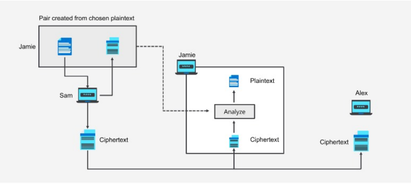
AES vulnerabilities and mitigation

AES has also been subjected to several attacks, which have led to the development of new techniques and variants of the algorithm. One such attack is the **side-channel attack** (SCA), which involves using information obtained from the physical implementation of the algorithm to extract the secret key. SCA can be prevented by using techniques such as masking and blinding, which involve adding random values to the data during encryption and decryption.

The figure illustrates a side-channel attack, a method used to extract sensitive information from a normal application workflow. This attack takes advantage of side information, including sound, frequency, power consumption, and more, to obtain the final output, such as the plaintext from a ciphertext. What this means is that even the noise your computer makes or the tiny changes in voltage your computer is using may give an attacker the edge they need to break the code.

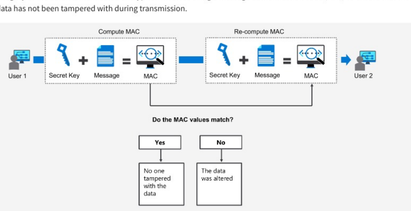


The **chosen-plaintext attack** is another vulnerability that affects AES. In this attack, the attacker can actively select the plaintext to be encrypted and deduce the key by utilizing the resulting ciphertext. For example, the image below depicts a hacker, Jamie, attempting to decrypt a message using the chosen-plaintext attack method, where she selects and encrypts specific messages between Sam and Alex to obtain information about the encryption key.



To prevent this attack, AES has been modified to use whitening techniques. These techniques involve adding a random value to the plaintext before encryption and removing it after decryption. This makes it harder for an attacker to uncover the key.

AES has also been modified to provide authenticated encryption, which not only ensures confidentiality but also the integrity of the data. Authenticated encryption involves using a message authentication code (MAC) to ensure that the data has not been tampered with during transmission.



Example

Now let's consider how Sam's Scoops can benefit from using AES encryption. Sam's business may need to exchange sensitive information such as financial data, customer information, and business plans. AES encryption can help protect this information from unauthorized access and ensure secure communication between Sam's business and its partners or clients. For example, if Sam's Scoops uses online payment systems, it can use AES encryption to protect the payment data and ensure that it is not intercepted by hackers.

Conclusion

The formation of symmetric standards has played a critical role in ensuring secure communication and data exchange in the digital world. AES is a widely adopted symmetric encryption algorithm that has become essential for securing digital communication. It uses various techniques such as the key schedule, SPN structure, mix column operation, shift rows operation, and Galois Counter Mode to ensure secure encryption.

AES encryption is flexible, efficient, and widely used in various applications, making it an essential tool for businesses and governments. However, AES encryption is not immune to side-channel attacks, and countermeasures need to be implemented to ensure its security. Overall, the AES standard has become a cornerstone of modern cryptography and will continue to play a crucial role in securing digital communication in the future.

Mark as completed