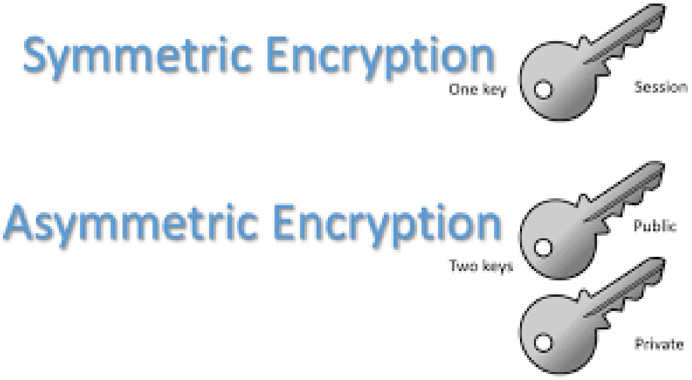
MODULE-2: Symmetric and Asymmetric key Cryptography

VIT | Vidyalankar Institute of Technology

Accredited A+ by NAAC


Symmetric Encryption

Asymmetric Encryption

Prepared by Prof. Amit K. Nerurkar

Module 2 DES and AES

THE DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES), a system developed for the U.S. gov¬ernment, was intended for use by the general public. It has been officially accepted as a cryptographic standard both in the United States and abroad. Moreover, many hard¬ware and software systems have been designed with the DES. However, recently its ad¬equacy has been questioned.

Background and History

In the early 1970s, the U.S. National Bureau of Standards (NBS) recognized that the general public needed a secure encryption technique for protecting sensitive informa¬tion. Historically, the U.S. Department of Defense and the Department of State had had continuing interest in encryption systems; it was thought that these departments were home to the greatest expertise in cryptology. However, precisely because of the sensi¬tive nature of the information they were encrypting, the departments could not release any of their work. Thus, the responsibility for a more public encryption technique was delegated to the NBS.

At the same time, several private vendors had developed encryption devices, using either mechanical means or programs that individuals or firms could buy to protect their sensitive communications. The difficulty with this commercial proliferation of encryption techniques was exchange: Two users with different devices could not exchange encrypted information. Furthermore, there was no independent body capable of testing the devices extensively to verify that they properly implemented their algorithms.

It soon became clear that encryption was ripe for assessment and standardization, to promote the ability of unrelated parties to exchange encrypted information and to provide a single encryption system that could be rigorously tested and publicly certified. As a result, in 1972 the NBS issued a call for proposals for producing a public encryption algorithm.

The call specified desirable criteria for such an algorithm :

- able to provide a high level of security
- specified and easy to understand
- publishable, so that security does not depend on the secrecy of the algorithm
- available to all users
- adaptable for use in diverse applications
- economical to implement in electronic devices
- efficient to use
- able to be validated
- exportable

Overview of the DES Algorithm

The DES algorithm is a careful and complex combination of two fundamental building blocks of encryption: substitution and transposition. The algorithm derives its strength from repeated application of these two techniques, one on top of the other, for a total of 16 cycles. The sheer complexity of tracing a single bit through 16 iterations of substitu¬tions and transpositions has so far stopped researchers in the public from identifying more than a handful of general properties of the algorithm.

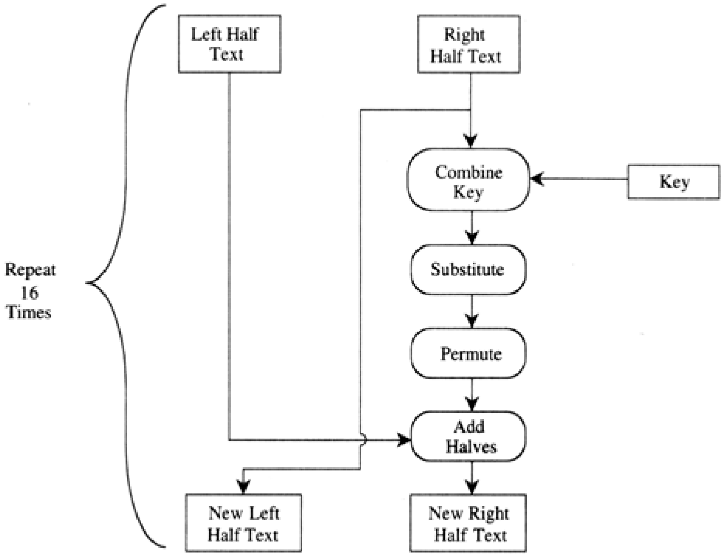


Fig : Cycles of Substitution and Permutation

The algorithm begins by encrypting the plaintext as blocks of 64 bits. The key is 64 bits long, but in fact it can be any 56-bit number. (The extra 8 bits are often used as check digits and do not affect encryption in normal implementations.) The user can change the key at will any time there is uncertainty about the security of the old key.

Substitution provides the confusion, and transposition provides the diffusion. In general, plaintext is affected by a series of cycles of a substitution then a permutation. The iterative substitutions and permutations are performed as outlined in following figure.

DES uses only standard arithmetic and logical operations on numbers up to 64 bits long, so it is suitable for implementation in software on most current computers. Al¬though complex, the algorithm is repetitive, making it suitable for implementation on a single-purpose chip. In fact, several such chips are available on the market for use as basic components in devices that use DES encryption in an application.

THE AES ENCRYPTION ALGORITHM

The AES is likely to be the commercial-grade symmetric algorithm of choice for years, if not decades. Let us look at it more closely.

The AES Contest

In January 1997, NIST called for cryptographers to develop a new encryption system. As with the call for candidates from which DES was selected, NIST made several important restrictions. The algorithms had to be unclassified

- publicly disclosed
- available royalty-free for use worldwide
- symmetric block cipher algorithms, for blocks of 128 bits
- usable with key sizes of 128, 192, and 256 bits

In August 1998, fifteen algorithms were chosen from among those submitted; in August 1999, the field of candidates was narrowed to five finalists. The five then underwent extensive public and private scrutiny. The final selection was made on the basis not only security but also of cost or efficiency of operation and ease of implementation in software. The winning algorithm,

submitted by two Dutch cryptographers, was Rijndael.

Overview of Rijndael

Rijndael is a fast algorithm that can be implemented easily on simple processors. Although it has a strong mathematical foundation, it primarily uses substitution, transposition, and the shift, exclusive OR, and addition operations. Like DBS, AES uses repeat cycles. There are 9, 11, or 13 cycles for keys of 128, 192, and 256 bits, respectively. In Rijndael, the cycles are called "rounds."

Each cycle consists of four steps.

- Byte substitution: This step uses a substitution box structure similar to the DBS, substituting each byte of a 128-bit block according to a substitution table. This is a straight confusion operation.
- Shift row: A transposition step. For 128- and 192-bit block sizes, row n is shifted left circular (n - 1) bytes; for 256-bit blocks, row 2 is shifted 1 byte and rows 3 and 4 are shifted 3 and 4 bytes, respectively. This is a straight confusion operation.
- Mix column: This step involves shifting left and exclusive-ORing bits with themselves. These operations provide both confusion and diffusion.
- Add subkey: Here, a portion of the key unique to this cycle is exclusive-ORed with the cycle result. This operation provides confusion and incorporates the key.

Bits from the key are combined with intermediate result bits frequently, so key bits arc also well diffused throughout the result. Furthermore, these four steps are extremely fast. The AES algorithm is depicted in the following Figure.

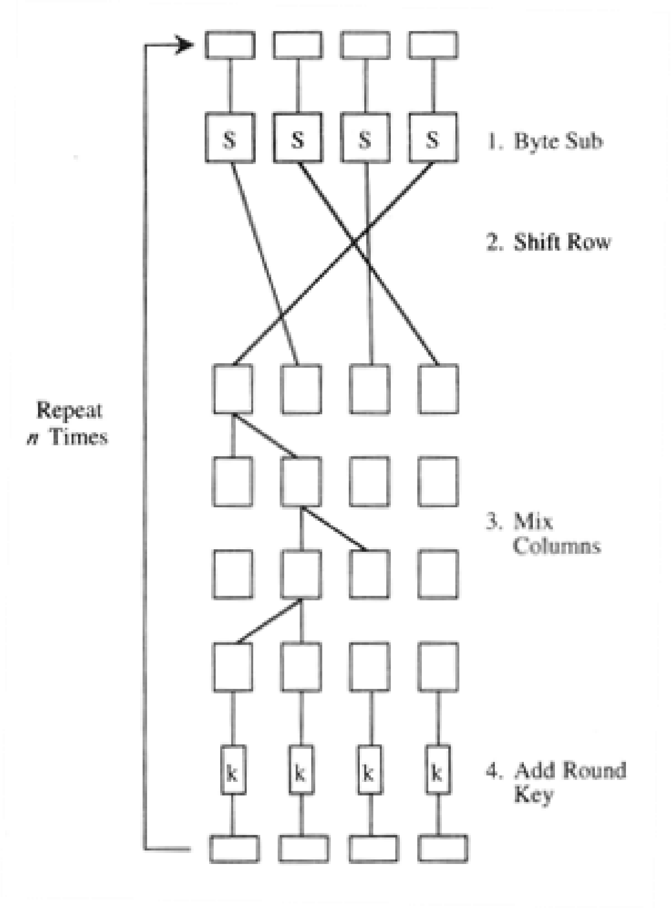


Fig : AES Algorithm

Comparison of DES and AES

The characteristics of DES and AES are compared in Table following Table :

When Rijndael's predecessor, DES, was adopted, two questions arose quickly:

1. How strong is it, and in particular, are there any backdoors?
2. How long would it be until the encrypted code could be routinely cracked?

With over 20 years of use, suspicions of weakness (intentional or not) and backdoors have pretty much been quashed. Not only have analysts failed to find any significant flaws, but in fact research has shown that seemingly insignificant changes weaken the strength of the algorithm that is, the algorithm is the best it can be. The second question, about how long DES would last, went unanswered for a long time but then

	DES	AES
Date	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length)	128, 192, 256 (and possibly more) bits
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accepted open public comment
Source	IBM, enhanced by NSA	Independent Dutch cryptographers