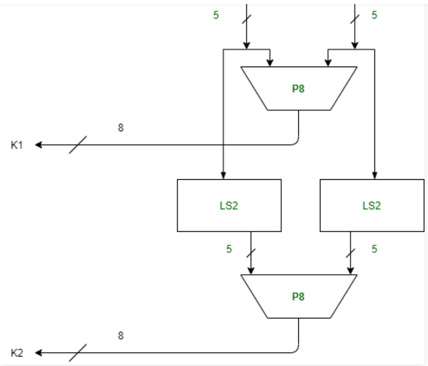
Simplified Data Encryption Standard Key Generation

Last Updated : 27 Sep, 2021

Simplified Data Encryption Standard (S-DES) is a simple version of the DES Algorithm. It is similar to the DES algorithm but is a smaller algorithm and has fewer parameters than DES. It was made for educational purposes so that understanding DES would become simpler. It is a block cipher that takes a block of plain text and converts it into ciphertext. It takes a block of 8 bit.

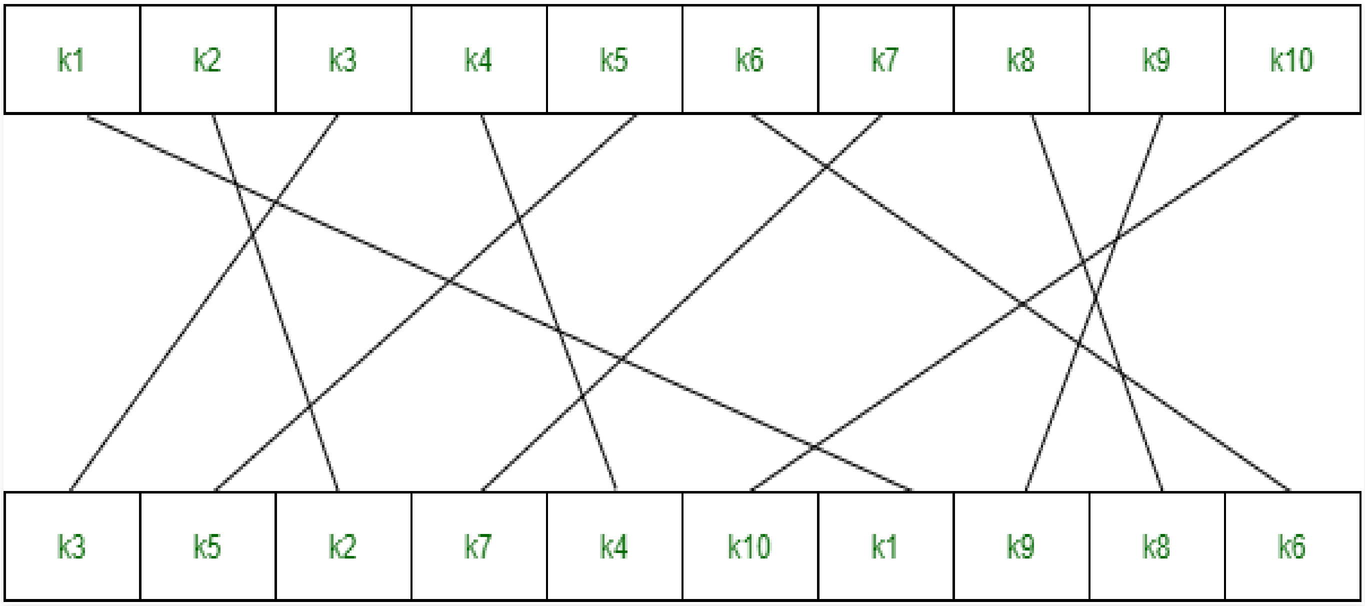
It is a symmetric key cipher i.e. they use the same key for both encryption and decryption. In this article, we are going to demonstrate key generation for s-des encryption and decryption algorithm. We take a random 10-bit key and produce two 8-bit keys which will be used for encryption and decryption.

Key Generation Concept: In the key generation algorithm, we accept the 10-bit key and convert it into two 8 bit keys. This key is shared between both sender and receiver.



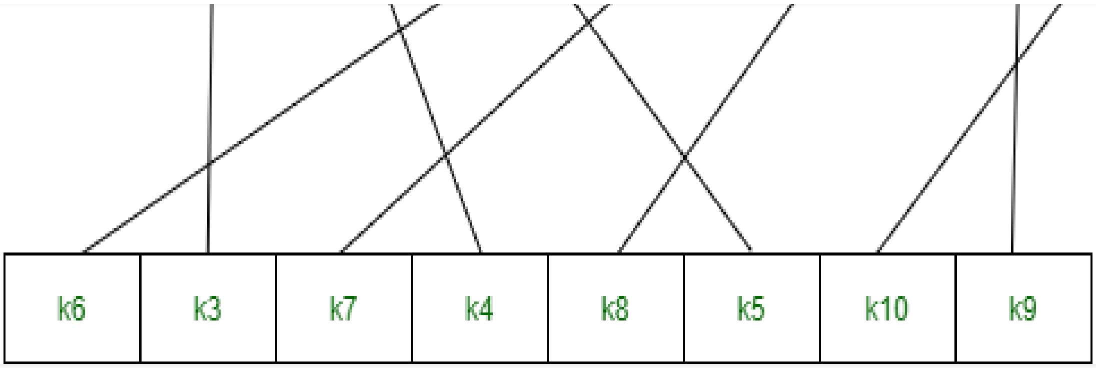
In the key generation, we use three functions:

1. Permutation P10

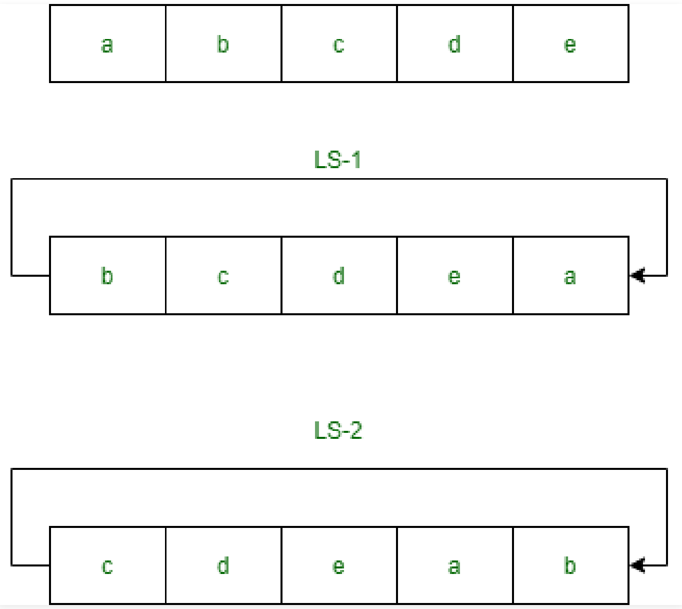


k1	k2	k3	k4	k5	k6	k7	k8	k9	k10
k3	k5	k2	k7	k4	k10	k1	k9	k8	k6

2. Permutation P8



3. Left Shift



Step 1: We accepted a 10-bit key and permuted the bits by putting them in the P10 table.

```
Key = 1 0 1 0 0 0 0 0 1 0
(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (1, 0, 1, 0, 0, 0, 0, 0, 1, 0)

P10 Permutation is: P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5,
After P10, we get 1 0 0 0 0 0 1 1 0 0
```

Step 2: We divide the key into 2 halves of 5-bit each.

```
l = 0 0 0 0 1, r = 1 1 0 0 0
```

Step 4: Combine both keys after step 3 and permute the bits by putting them in the P8 table. The output of the given table is the first key K1.

```
After LS-1 combined, we get 0 0 0 0 1 1 1 0 0 0
P8 permutation is: P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k
After P8, we get Key-1 : 1 0 1 0 0 1 0 0
```

Step 5: The output obtained from step 3 i.e. 2 halves after one bit left shift should again undergo the process of two-bit left shift.

```
Step 3 output - l = 0 0 0 0 1, r = 1 1 0 0 0
After two bit shift - l = 0 0 1 0 0, r = 0 0 0 1 1
```

Step 6: Combine the 2 halves obtained from step 5 and permute them by putting them in the P8 table. The output of the given table is the second key K2.

```
After LS-2 combined = 0 0 1 0 0 0 0 0 1 1
P8 permutation is: P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k
After P8, we get Key-2 : 0 1 0 0 0 0 1 1
```

Final Output:

```
Key-1 is: 1 0 1 0 0 1 0 0
Key-2 is: 0 1 0 0 0 0 1 1
```

Like 4

Previous

Next

RECOMMENDED ARTICLES

Page : 1 2 3

01 Simplified Data Encryption Standard | Set 2
01, Mar 21

02 Simplified International Data Encryption Algorithm (IDEA)
17, Jan 20

03 Difference between Software Encryption and Hardware Encryption
05, Feb 21

04 Data encryption standard (DES) | Set 1
17, Aug 18

05 Strength of Data encryption standard (DES)
31, Jan 20

06 Advanced Encryption Standard (AES)
15, Oct 21

07 Public Key Encryption
28, May 19

08 Difference Between Symmetric and Asymmetric Key Encryption
29, Jan 20

Article Contributed By :

devangj9689
@devangj9689

Vote for difficulty

Easy Normal Medium Hard Expert

Improved By : guptaaman9981

Article Tags : cryptography, Computer Networks

Practice Tags : cryptography, Computer Networks

Improve Article Report Issue

Writing code in comment? Please use ide.geeksforgeeks.org, generate link and share the link here.

Load Comments

GeeksforGeeks
5th Floor, A-118,
Sector-136, Noida, Uttar Pradesh - 201305

feedback@geeksforgeeks.org

Start Your Coding Journey Now!

Login

Register

Company

About Us

Careers

Privacy Policy

Contact Us

Copyright Policy

Learn

Algorithms

Data Structures

Languages

CS Subjects

Video Tutorials

Web Development

Web Tutorials

HTML

CSS

JavaScript

Bootstrap

Contribute

Write an Article

Write Interview Experience

Internships

Videos