Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment 5

Date: 14/09/2024

Name: Avadhoot Pawaskar
Rollno: 43

Title: Block cipher modes of operation using AES or DES.

Problem Definition: Compare different block cipher modes of operation by encrypting long message “Because of you, my darling, I have known how it feels actually to care and cherish someone more than anything one can ever think of in this world. I have the chance to experience the most beautiful feeling of knowing that there will always be a person who will never give up on me and always cherish and care for me no matter what happens” using online AES or DES cryptosystem.

Pre-requisite: Theory:

Block cipher modes of operation are essential cryptographic techniques that define how to apply a block cipher, a symmetric encryption algorithm that operates on fixed-size blocks of data, to encrypt and decrypt data of arbitrary lengths. There are several widely used block cipher modes of operation, each with its own strengths, weaknesses, and applications. Here are some block cipher modes of operation:

i. Electronic Codebook (ECB)
ii. Cipher Block Chaining (CBC)
iii. Cipher Feedback (CFB)
iv. Output Feedback (OFB)
v. Counter (CTR)

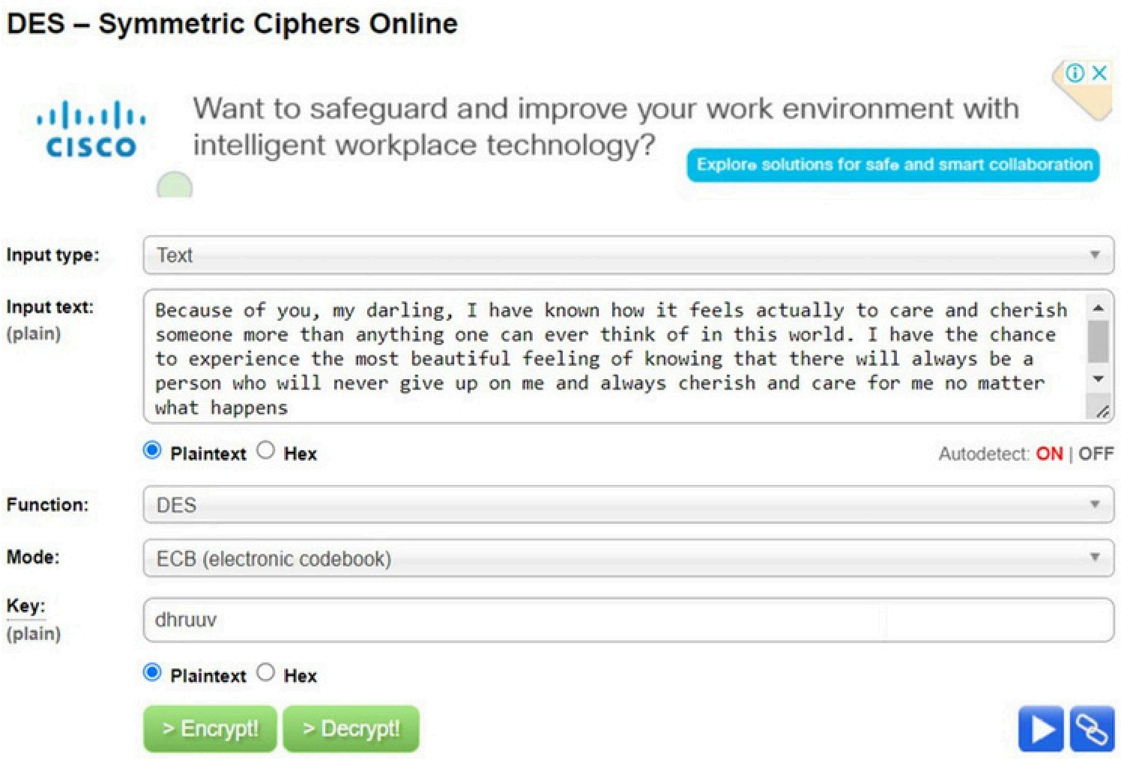
Procedure/ Algorithm:

Results:

1. Online system snapshots

1.1 ECB

Encryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
Because of you, my darling, I have known how it feels actually to care and cherish
someone more than anything one can ever think of in this world. I have the chance
to experience the most beautiful feeling of knowing that there will always be a
person who will never give up on me and always cherish and care for me no matter
what happens
```

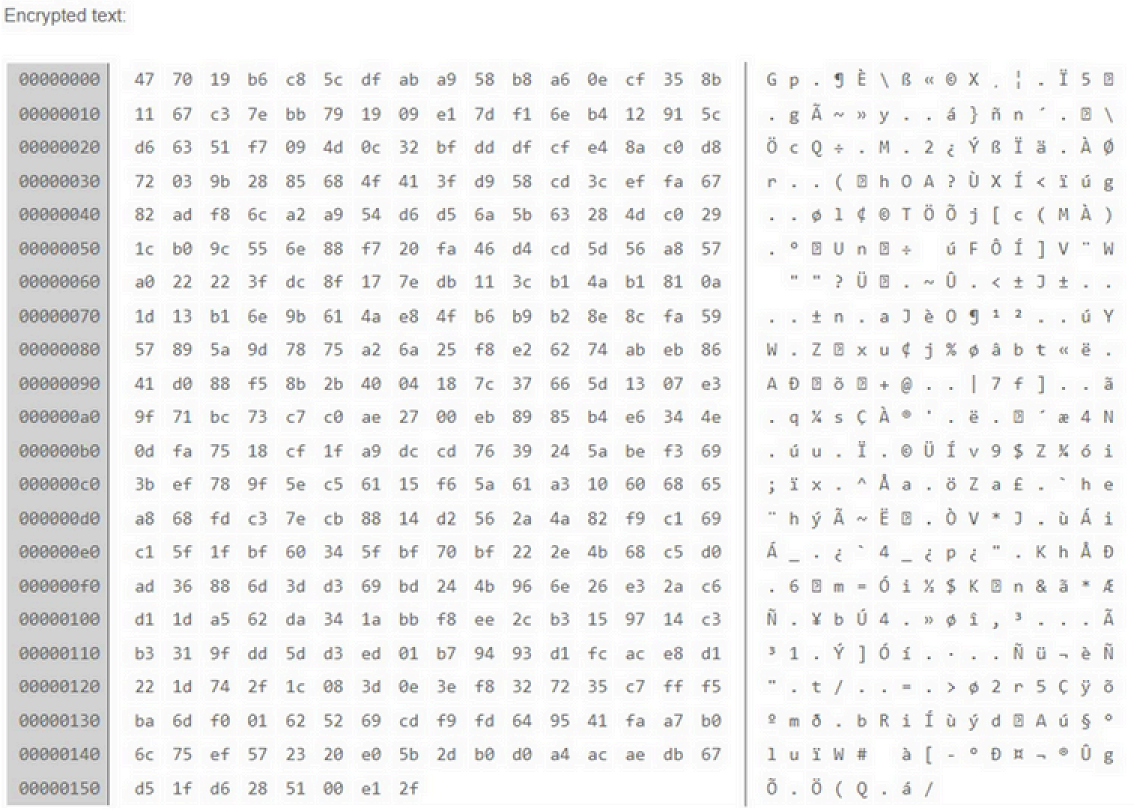
● Plaintext ○ Hex Autodetect: ON | OFF

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) dhruuv

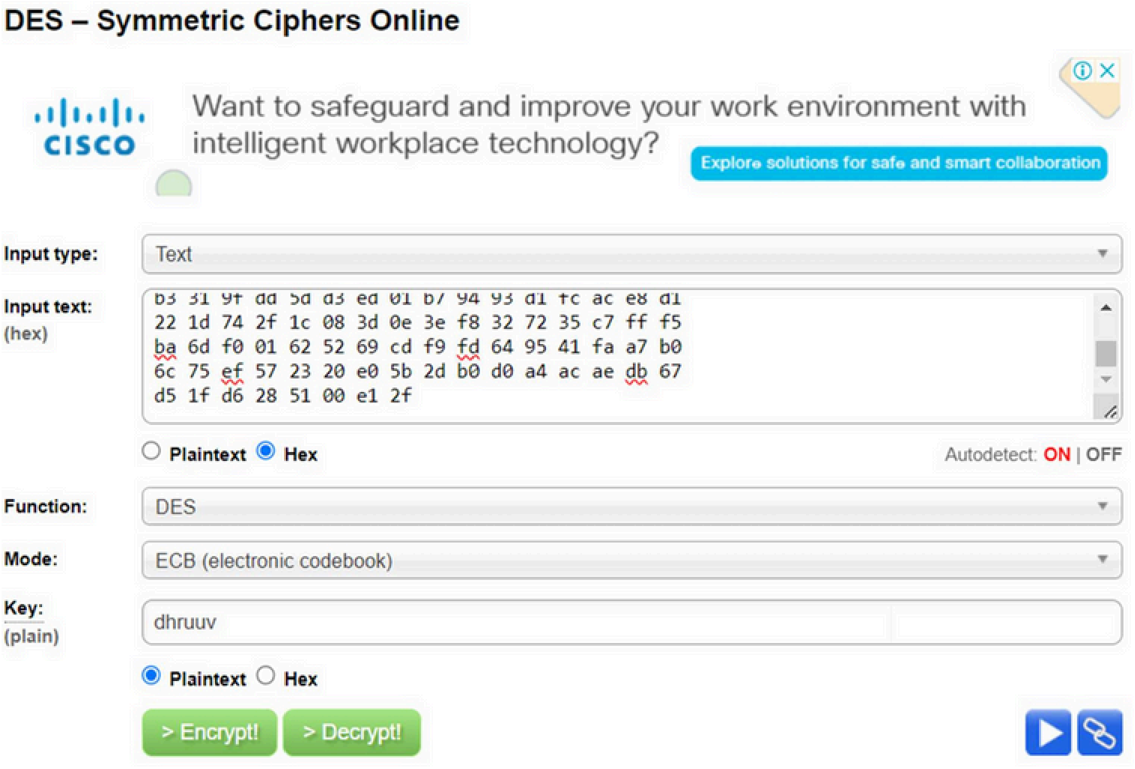
● Plaintext ○ Hex



Encrypted text:

```
00000000  47 70 19 b6 c8 5c df ab a9 58 b8 a6 0e cf 35 8b  | G p . ¶ È \ ß « © X . ¦ . Ï 5 ☒
00000010  11 67 c3 7e bb 79 19 09 e1 7d f1 6e b4 12 91 5c  | . g Ã ~ » y . . á } ñ n ´ . ☒ \
00000020  d6 63 51 f7 09 4d 0c 32 bf dd df cf e4 8a c0 d8  | Ö c Q ÷ . M . 2 ¿ Ý ß Ï ä . À Ø
00000030  72 03 9b 28 85 68 4f 41 3f d9 58 cd 3c ef fa 67  | r . . ( ☒ h O A ? Ù X Í < ï ú g
00000040  82 ad f8 6c a2 a9 54 d6 d5 6a 5b 63 28 4d c0 29  | . . ø l ¢ © T Ö Õ j [ c ( M À )
00000050  1c b0 9c 55 6e 88 f7 20 fa 46 d4 cd 5d 56 a8 57  | . ° ☒ U n ☒ ÷   ú F Ô Í ] V ¨ W
00000060  a0 22 22 3f dc 8f 17 7e db 11 3c b1 4a b1 81 0a  |   " " ? Ü ☒ . ~ Û . < ± J ± . .
00000070  1d 13 b1 6e 9b 61 4a e8 4f b6 b9 b2 8e 8c fa 59  | . . ± n . a J è O ¶ ¹ ² . . ú Y
00000080  57 89 5a 9d 78 75 a2 6a 25 f8 e2 62 74 ab eb 86  | W . Z ☒ x u ¢ j % ø â b t « ë .
00000090  41 d0 88 f5 8b 2b 40 04 18 7c 37 66 5d 13 07 e3  | A Ð ☒ õ ☒ + @ . . | 7 f ] . . ã
000000a0  9f 71 bc 73 c7 c0 ae 27 00 eb 89 85 b4 e6 34 4e  | . q ¼ s Ç À ® ' . ë . ☒ ´ æ 4 N
000000b0  0d fa 75 18 cf 1f a9 dc cd 76 39 24 5a be f3 69  | . ú u . Ï . © Ü Í v 9 $ Z ¾ ó i
000000c0  3b ef 78 9f 5e c5 61 15 f6 5a 61 a3 10 60 68 65  | ; ï x . ^ Å a . ö Z a £ . ` h e
000000d0  a8 68 fd c3 7e cb 88 14 d2 56 2a 4a 82 f9 c1 69  | ¨ h ý Ã ~ Ë ☒ . Ò V * J . ù Á i
000000e0  c1 5f 1f bf 60 34 5f bf 70 bf 22 2e 4b 68 c5 d0  | Á _ . ¿ ` 4 _ ¿ p ¿ " . K h Å Ð
000000f0  ad 36 88 6d 3d d3 69 bd 24 4b 96 6e 26 e3 2a c6  | . 6 ☒ m = Ó i ½ $ K ☒ n & ã * Æ
00000100  d1 1d a5 62 da 34 1a bb f8 ee 2c b3 15 97 14 c3  | Ñ . ¥ b Ú 4 . » ø î , ³ . . . Ã
00000110  b3 31 9f dd 5d d3 ed 01 b7 94 93 d1 fc ac e8 d1  | ³ 1 . Ý ] Ó í . · . . Ñ ü ¬ è Ñ
00000120  22 1d 74 2f 1c 08 3d 0e 3e f8 32 72 35 c7 ff f5  | " . t / . . = . > ø 2 r 5 Ç ÿ õ
00000130  ba 6d f0 01 62 52 69 cd f9 fd 64 95 41 fa a7 b0  | º m ð . b R i Í ù ý d ☒ A ú § °
00000140  6c 75 ef 57 23 20 e0 5b 2d b0 d0 a4 ac ae db 67  | l u ï W #   à [ - ° Ð ¤ ¬ ® Û g
00000150  d5 1f d6 28 51 00 e1 2f                          | Õ . Ö ( Q . á /
```

Decryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
b3 31 9f dd 5d d3 ed 01 b7 94 93 d1 fc ac e8 d1
22 1d 74 2f 1c 08 3d 0e 3e f8 32 72 35 c7 ff f5
ba 6d f0 01 62 52 69 cd f9 fd 64 95 41 fa a7 b0
6c 75 ef 57 23 20 e0 5b 2d b0 d0 a4 ac ae db 67
d5 1f d6 28 51 00 e1 2f
```

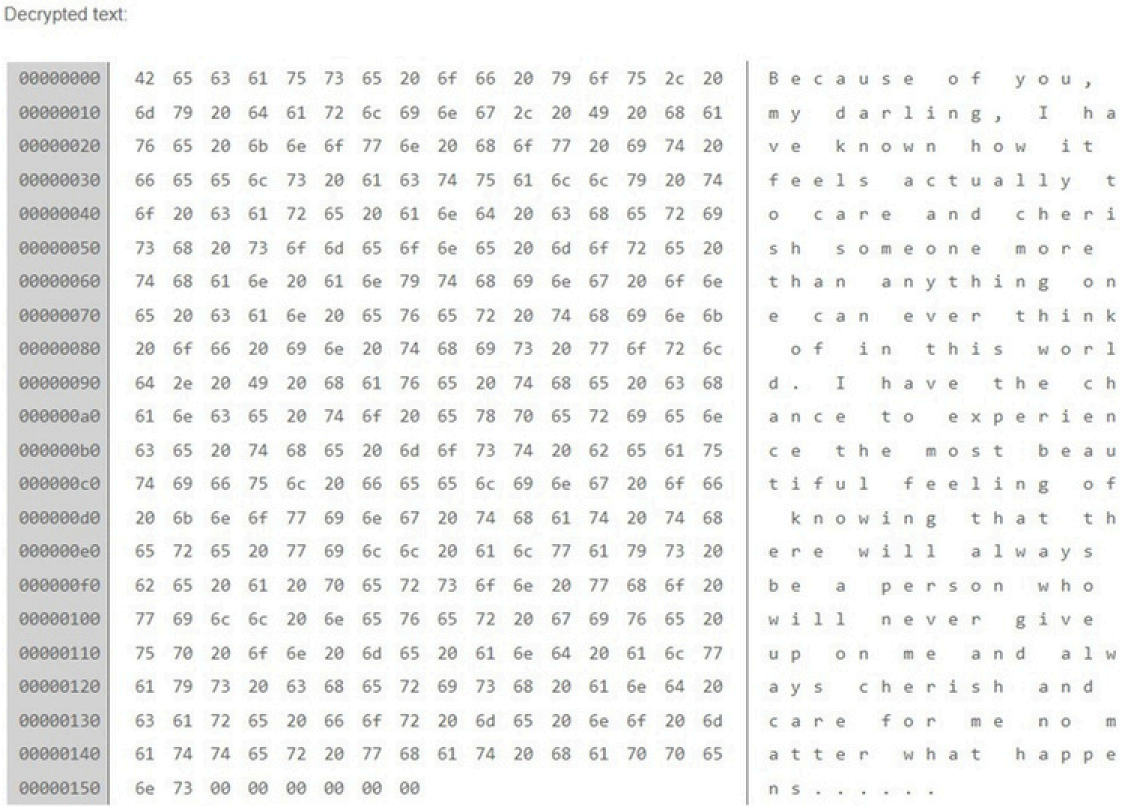
○ **Plaintext** ● **Hex**   Autodetect: ON | OFF

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) dhruuv

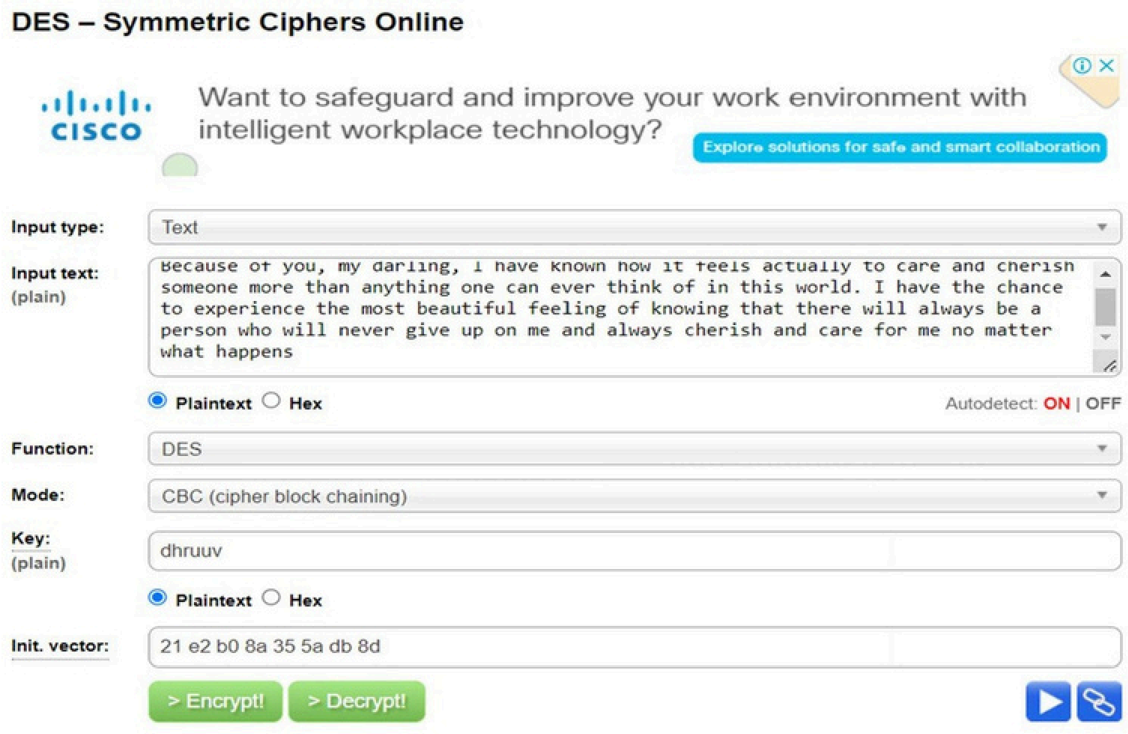
● **Plaintext** ○ **Hex**



Decrypted text:

```
00000000  42 65 63 61 75 73 65 20 6f 66 20 79 6f 75 2c 20  Because of you, 
00000010  6d 79 20 64 61 72 6c 69 6e 67 2c 20 49 20 68 61  my darling, I ha
00000020  76 65 20 6b 6e 6f 77 6e 20 68 6f 77 20 69 74 20  ve known how it 
00000030  66 65 65 6c 73 20 61 63 74 75 61 6c 6c 79 20 74  feels actually t
00000040  6f 20 63 61 72 65 20 61 6e 64 20 63 68 65 72 69  o care and cheri
00000050  73 68 20 73 6f 6d 65 6f 6e 65 20 6d 6f 72 65 20  sh someone more 
00000060  74 68 61 6e 20 61 6e 79 74 68 69 6e 67 20 6f 6e  than anything on
00000070  65 20 63 61 6e 20 65 76 65 72 20 74 68 69 6e 6b  e can ever think
00000080  20 6f 66 20 69 6e 20 74 68 69 73 20 77 6f 72 6c   of in this worl
00000090  64 2e 20 49 20 68 61 76 65 20 74 68 65 20 63 68  d. I have the ch
000000a0  61 6e 63 65 20 74 6f 20 65 78 70 65 72 69 65 6e  ance to experien
000000b0  63 65 20 74 68 65 20 6d 6f 73 74 20 62 65 61 75  ce the most beau
000000c0  74 69 66 75 6c 20 66 65 65 6c 69 6e 67 20 6f 66  tiful feeling of
000000d0  20 6b 6e 6f 77 69 6e 67 20 74 68 61 74 20 74 68   knowing that th
000000e0  65 72 65 20 77 69 6c 6c 20 61 6c 77 61 79 73 20  ere will always 
000000f0  62 65 20 61 20 70 65 72 73 6f 6e 20 77 68 6f 20  be a person who 
00000100  77 69 6c 6c 20 6e 65 76 65 72 20 67 69 76 65 20  will never give 
00000110  75 70 20 6f 6e 20 6d 65 20 61 6e 64 20 61 6c 77  up on me and alw
00000120  61 79 73 20 63 68 65 72 69 73 68 20 61 6e 64 20  ays cherish and 
00000130  63 61 72 65 20 66 6f 72 20 6d 65 20 6e 6f 20 6d  care for me no m
00000140  61 74 74 65 72 20 77 68 61 74 20 68 61 70 70 65  atter what happe
00000150  6e 73 00 00 00 00 00 00                          ns......
```

1.2 CBC
Encryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
Because of you, my darling, I have known how it feels actually to care and cherish
someone more than anything one can ever think of in this world. I have the chance
to experience the most beautiful feeling of knowing that there will always be a
person who will never give up on me and always cherish and care for me no matter
what happens
```

● Plaintext ○ Hex   Autodetect: ON | OFF

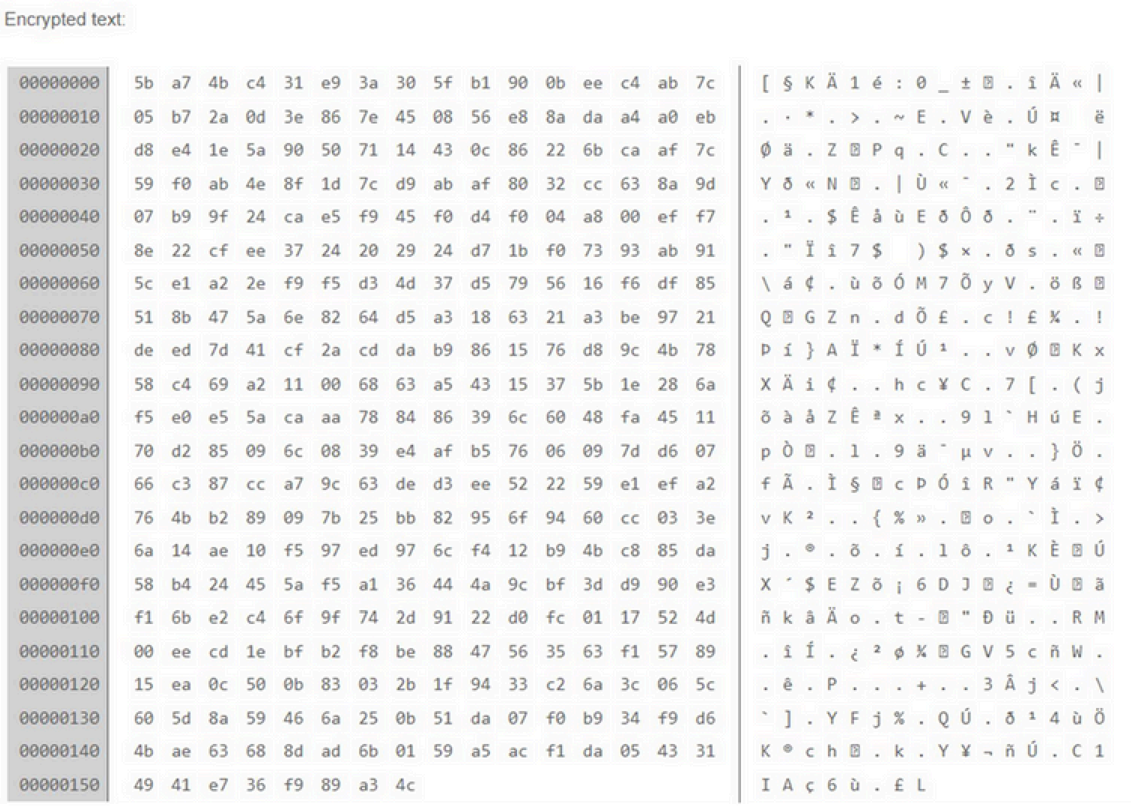
Function: DES

Mode: CBC (cipher block chaining)

Key: (plain) dhruuv

● Plaintext ○ Hex

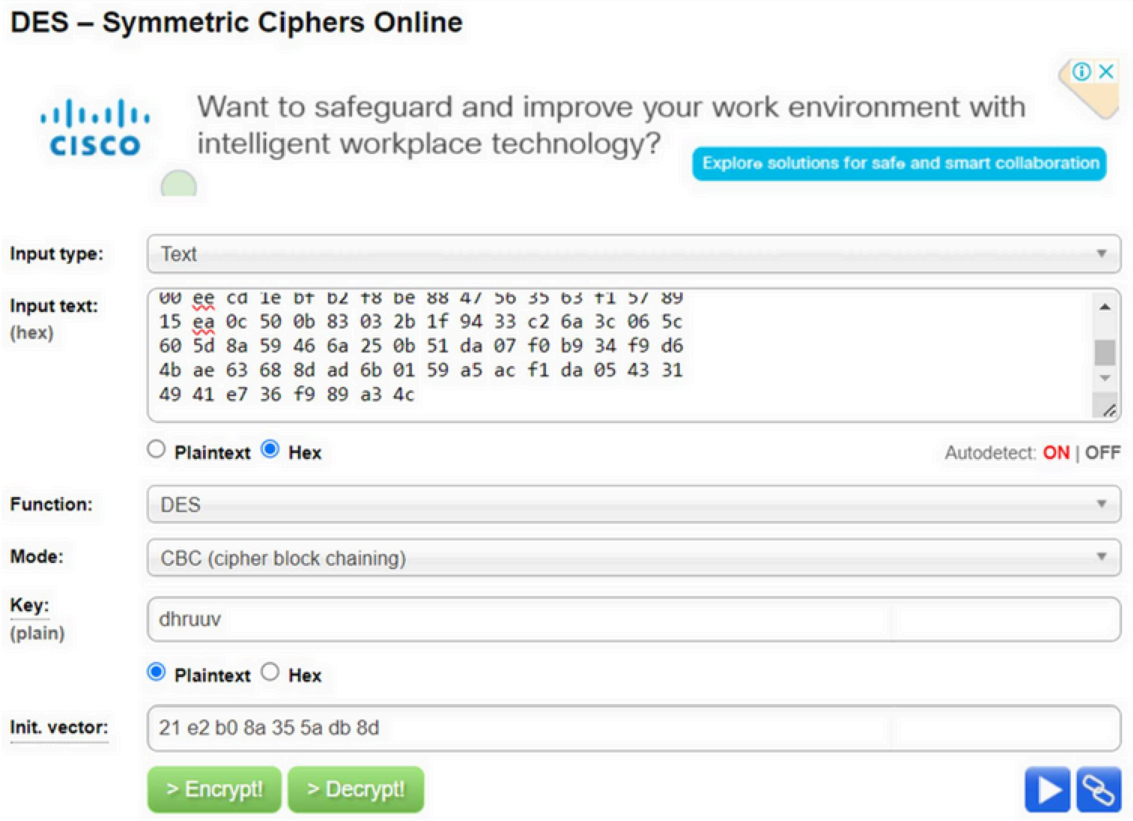
Init. vector: 21 e2 b0 8a 35 5a db 8d



Encrypted text:

```
00000000  5b a7 4b c4 31 e9 3a 30 5f b1 90 0b ee c4 ab 7c  [ § K Ä 1 é : 0 _ ± ⊠ . î Ä « |
00000010  05 b7 2a 0d 3e 86 7e 45 08 56 e8 8a da a4 a0 eb  . · * . > . ~ E . V è . Ú ¤   ë
00000020  d8 e4 1e 5a 90 50 71 14 43 0c 86 22 6b ca af 7c  Ø ä . Z ⊠ P q . C . . " k Ê ¯ |
00000030  59 f0 ab 4e 8f 1d 7c d9 ab af 80 32 cc 63 8a 9d  Y ð « N ⊠ . | Ù « ¯ . 2 Ì c . ⊠
00000040  07 b9 9f 24 ca e5 f9 45 f0 d4 f0 04 a8 00 ef f7  . ¹ . $ Ê å ù E ð Ô ð . ¨ . ï ÷
00000050  8e 22 cf ee 37 24 20 29 24 d7 1b f0 73 93 ab 91  . " Ï î 7 $   ) $ × . ð s . « ⊠
00000060  5c e1 a2 2e f9 f5 d3 4d 37 d5 79 56 16 f6 df 85  \ á ¢ . ù õ Ó M 7 Õ y V . ö ß ⊠
00000070  51 8b 47 5a 6e 82 64 d5 a3 18 63 21 a3 be 97 21  Q ⊠ G Z n . d Õ £ . c ! £ ¾ . !
00000080  de ed 7d 41 cf 2a cd da b9 86 15 76 d8 9c 4b 78  Þ í } A Ï * Í Ú ¹ . . v Ø ⊠ K x
00000090  58 c4 69 a2 11 00 68 63 a5 43 15 37 5b 1e 28 6a  X Ä i ¢ . . h c ¥ C . 7 [ . ( j
000000a0  f5 e0 e5 5a ca aa 78 84 86 39 6c 60 48 fa 45 11  õ à å Z Ê ª x . . 9 1 ` H ú E .
000000b0  70 d2 85 09 6c 08 39 e4 af b5 76 06 09 7d d6 07  p Ò ⊠ . 1 . 9 ä ¯ µ v . . } Ö .
000000c0  66 c3 87 cc a7 9c 63 de d3 ee 52 22 59 e1 ef a2  f Ã . Ì § ⊠ c Þ Ó î R " Y á ï ¢
000000d0  76 4b b2 89 09 7b 25 bb 82 95 6f 94 60 cc 03 3e  v K ² . . { % » . ⊠ o . ` Ì . >
000000e0  6a 14 ae 10 f5 97 ed 97 6c f4 12 b9 4b c8 85 da  j . ® . õ . í . 1 ô . ¹ K È ⊠ Ú
000000f0  58 b4 24 45 5a f5 a1 36 44 4a 9c bf 3d d9 90 e3  X ´ $ E Z õ ¡ 6 D J ⊠ ¿ = Ù ⊠ ã
00000100  f1 6b e2 c4 6f 9f 74 2d 91 22 d0 fc 01 17 52 4d  ñ k â Ä o . t - ⊠ " Ð ü . . R M
00000110  00 ee cd 1e bf b2 f8 be 88 47 56 35 63 f1 57 89  . î Í . ¿ ² ø ¾ ⊠ G V 5 c ñ W .
00000120  15 ea 0c 50 0b 83 03 2b 1f 94 33 c2 6a 3c 06 5c  . ê . P . . . + . . 3 Â j < . \
00000130  60 5d 8a 59 46 6a 25 0b 51 da 07 f0 b9 34 f9 d6  ` ] . Y F j % . Q Ú . ð ¹ 4 ù Ö
00000140  4b ae 63 68 8d ad 6b 01 59 a5 ac f1 da 05 43 31  K ® c h ⊠ . k . Y ¥ ¬ ñ Ú . C 1
00000150  49 41 e7 36 f9 89 a3 4c                          I A ç 6 ù . £ L
```

Decryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
00 ee cd 1e bf b2 f8 be 88 47 56 35 63 f1 57 89
15 ea 0c 50 0b 83 03 2b 1f 94 33 c2 6a 3c 06 5c
60 5d 8a 59 46 6a 25 0b 51 da 07 f0 b9 34 f9 d6
4b ae 63 68 8d ad 6b 01 59 a5 ac f1 da 05 43 31
49 41 e7 36 f9 89 a3 4c
```

○ Plaintext ● Hex

Autodetect: ON | OFF

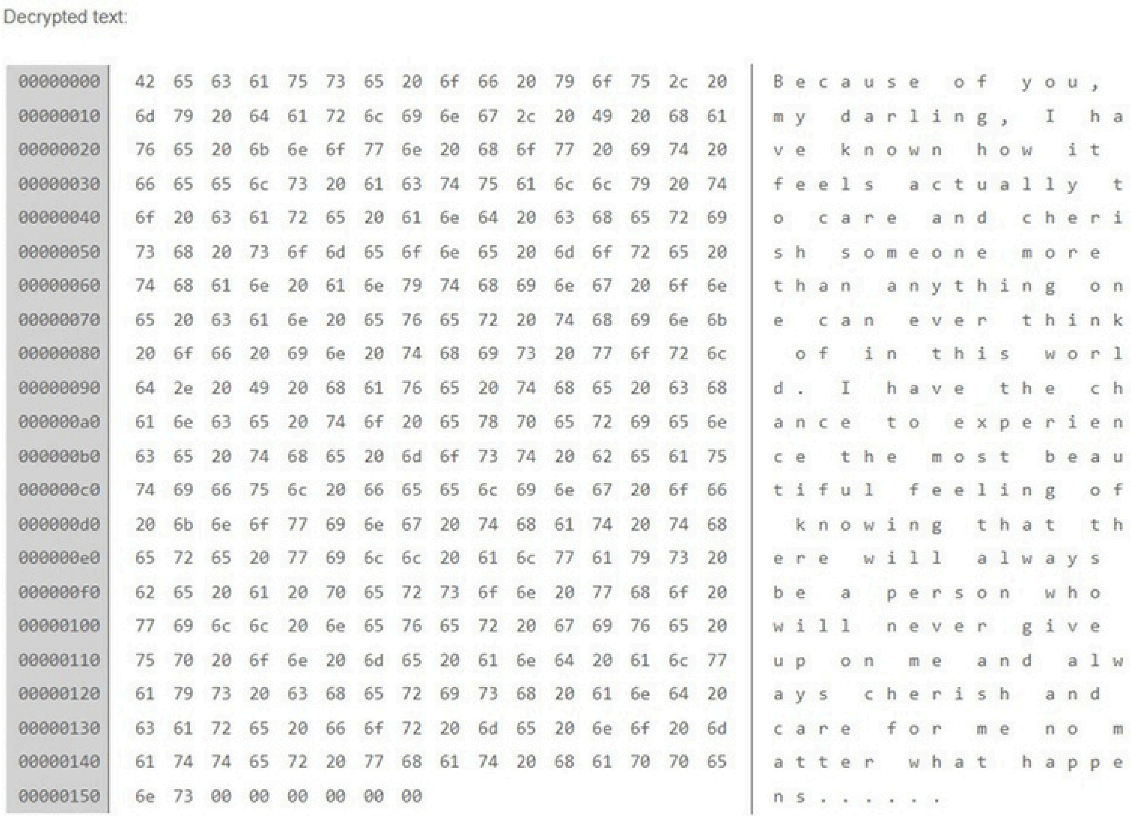
Function: DES

Mode: CBC (cipher block chaining)

Key: (plain) dhruuv

● Plaintext ○ Hex

Init. vector: 21 e2 b0 8a 35 5a db 8d

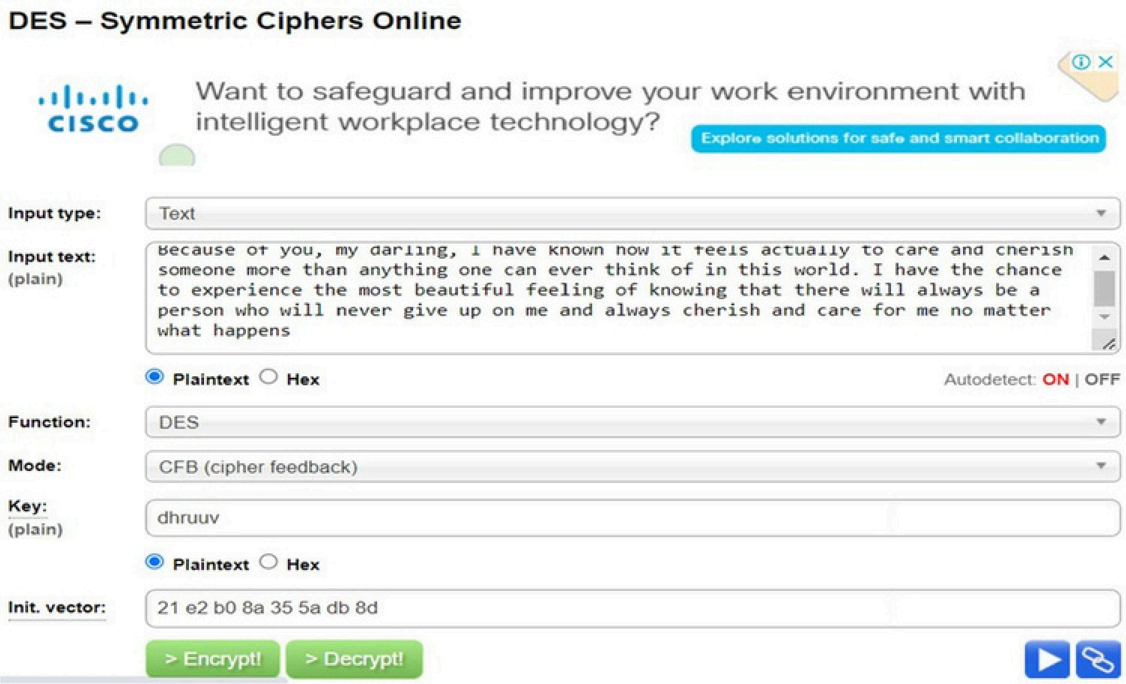


Decrypted text:

```
00000000  42 65 63 61 75 73 65 20 6f 66 20 79 6f 75 2c 20  Because of you, 
00000010  6d 79 20 64 61 72 6c 69 6e 67 2c 20 49 20 68 61  my darling, I ha
00000020  76 65 20 6b 6e 6f 77 6e 20 68 6f 77 20 69 74 20  ve known how it 
00000030  66 65 65 6c 73 20 61 63 74 75 61 6c 6c 79 20 74  feels actually t
00000040  6f 20 63 61 72 65 20 61 6e 64 20 63 68 65 72 69  o care and cheri
00000050  73 68 20 73 6f 6d 65 6f 6e 65 20 6d 6f 72 65 20  sh someone more 
00000060  74 68 61 6e 20 61 6e 79 74 68 69 6e 67 20 6f 6e  than anything on
00000070  65 20 63 61 6e 20 65 76 65 72 20 74 68 69 6e 6b  e can ever think
00000080  20 6f 66 20 69 6e 20 74 68 69 73 20 77 6f 72 6c   of in this worl
00000090  64 2e 20 49 20 68 61 76 65 20 74 68 65 20 63 68  d. I have the ch
000000a0  61 6e 63 65 20 74 6f 20 65 78 70 65 72 69 65 6e  ance to experien
000000b0  63 65 20 74 68 65 20 6d 6f 73 74 20 62 65 61 75  ce the most beau
000000c0  74 69 66 75 6c 20 66 65 65 6c 69 6e 67 20 6f 66  tiful feeling of
000000d0  20 6b 6e 6f 77 69 6e 67 20 74 68 61 74 20 74 68   knowing that th
000000e0  65 72 65 20 77 69 6c 6c 20 61 6c 77 61 79 73 20  ere will always 
000000f0  62 65 20 61 20 70 65 72 73 6f 6e 20 77 68 6f 20  be a person who 
00000100  77 69 6c 6c 20 6e 65 76 65 72 20 67 69 76 65 20  will never give 
00000110  75 70 20 6f 6e 20 6d 65 20 61 6e 64 20 61 6c 77  up on me and alw
00000120  61 79 73 20 63 68 65 72 69 73 68 20 61 6e 64 20  ays cherish and 
00000130  63 61 72 65 20 66 6f 72 20 6d 65 20 6e 6f 20 6d  care for me no m
00000140  61 74 74 65 72 20 77 68 61 74 20 68 61 70 70 65  atter what happe
00000150  6e 73 00 00 00 00 00 00                          ns......
```

1.3 CFB

Encryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
Because of you, my darling, I have known how it feels actually to care and cherish
someone more than anything one can ever think of in this world. I have the chance
to experience the most beautiful feeling of knowing that there will always be a
person who will never give up on me and always cherish and care for me no matter
what happens
```

● Plaintext ○ Hex — Autodetect: ON | OFF

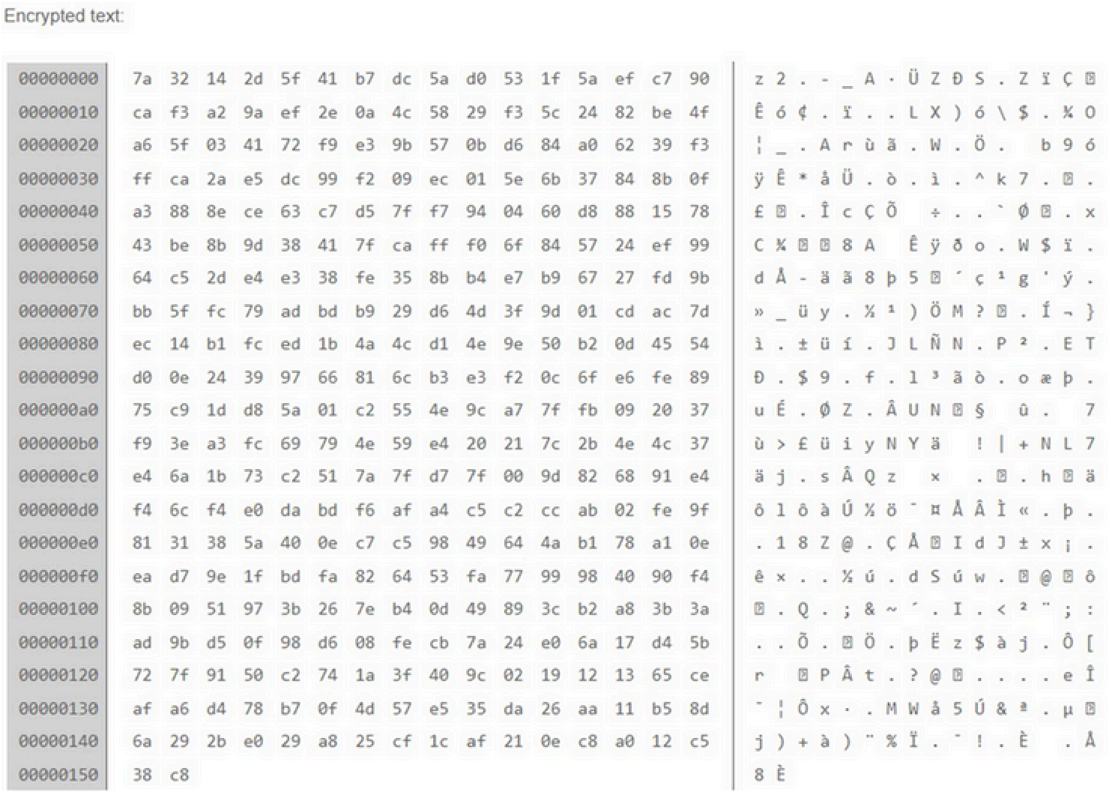
Function: DES

Mode: CFB (cipher feedback)

Key: (plain) dhruuv

● Plaintext ○ Hex

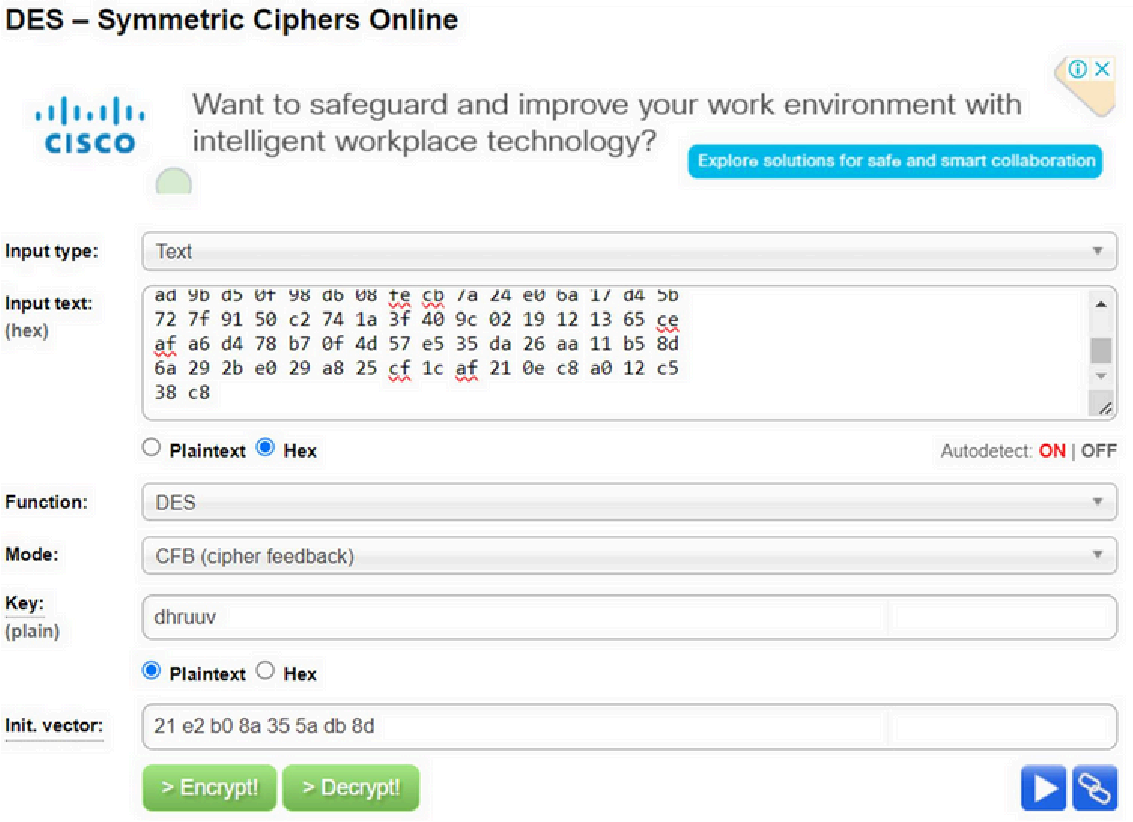
Init. vector: 21 e2 b0 8a 35 5a db 8d



Encrypted text:

```
00000000  7a 32 14 2d 5f 41 b7 dc 5a d0 53 1f 5a ef c7 90  z 2 . - _ A · Ü Z Đ S . Z ï Ç ▯
00000010  ca f3 a2 9a ef 2e 0a 4c 58 29 f3 5c 24 82 be 4f  Ê ó ¢ . ï . . L X ) ó \ $ . ¾ O
00000020  a6 5f 03 41 72 f9 e3 9b 57 0b d6 84 a0 62 39 f3  ¦ _ . A r ù ã . W . Ö .   b 9 ó
00000030  ff ca 2a e5 dc 99 f2 09 ec 01 5e 6b 37 84 8b 0f  ÿ Ê * å Ü . ò . ì . ^ k 7 . ▯ .
00000040  a3 88 8e ce 63 c7 d5 7f f7 94 04 60 d8 88 15 78  £ ▯ . Î c Ç Õ   ÷ . . ` Ø ▯ . x
00000050  43 be 8b 9d 38 41 7f ca ff f0 6f 84 57 24 ef 99  C ¾ ▯ ▯ 8 A   Ê ÿ ð o . W $ ï .
00000060  64 c5 2d e4 e3 38 fe 35 8b b4 e7 b9 67 27 fd 9b  d Å - ä ã 8 þ 5 ▯ ´ ç ¹ g ' ý .
00000070  bb 5f fc 79 ad bd b9 29 d6 4d 3f 9d 01 cd ac 7d  » _ ü y . ½ ¹ ) Ö M ? ▯ . Í ¬ }
00000080  ec 14 b1 fc ed 1b 4a 4c d1 4e 9e 50 b2 0d 45 54  ì . ± ü í . J L Ñ N . P ² . E T
00000090  d0 0e 24 39 97 66 81 6c b3 e3 f2 0c 6f e6 fe 89  Ð . $ 9 . f . l ³ ã ò . o æ þ .
000000a0  75 c9 1d d8 5a 01 c2 55 4e 9c a7 7f fb 09 20 37  u É . Ø Z . Â U N ▯ §   û .   7
000000b0  f9 3e a3 fc 69 79 4e 59 e4 20 21 7c 2b 4e 4c 37  ù > £ ü i y N Y ä   ! | + N L 7
000000c0  e4 6a 1b 73 c2 51 7a 7f d7 7f 00 9d 82 68 91 e4  ä j . s Â Q z   ×   . ▯ . h ▯ ä
000000d0  f4 6c f4 e0 da bd f6 af a4 c5 c2 cc ab 02 fe 9f  ô l ô à Ú ½ ö ¯ ¤ Å Â Ì « . þ .
000000e0  81 31 38 5a 40 0e c7 c5 98 49 64 4a b1 78 a1 0e  . 1 8 Z @ . Ç Å ▯ I d J ± x ¡ .
000000f0  ea d7 9e 1f bd fa 82 64 53 fa 77 99 98 40 90 f4  ê × . . ½ ú . d S ú w . ▯ @ ▯ ô
00000100  8b 09 51 97 3b 26 7e b4 0d 49 89 3c b2 a8 3b 3a  ▯ . Q . ; & ~ ´ . I . < ² ¨ ; :
00000110  ad 9b d5 0f 98 d6 08 fe cb 7a 24 e0 6a 17 d4 5b  . . Õ . ▯ Ö . þ Ë z $ à j . Ô [
00000120  72 7f 91 50 c2 74 1a 3f 40 9c 02 19 12 13 65 ce  r   ▯ P Â t . ? @ ▯ . . . . e Î
00000130  af a6 d4 78 b7 0f 4d 57 e5 35 da 26 aa 11 b5 8d  ¯ ¦ Ô x · . M W å 5 Ú & ª . µ ▯
00000140  6a 29 2b e0 29 a8 25 cf 1c af 21 0e c8 a0 12 c5  j ) + à ) ¨ % Ï . ¯ ! . È   . Å
00000150  38 c8                                            8 È
```

Decryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
ad 9b d5 0f 98 d6 08 fe cb 7a 24 e0 6a 17 d4 5b
72 7f 91 50 c2 74 1a 3f 40 9c 02 19 12 13 65 ce
af a6 d4 78 b7 0f 4d 57 e5 35 da 26 aa 11 b5 8d
6a 29 2b e0 29 a8 25 cf 1c af 21 0e c8 a0 12 c5
38 c8
```

○ Plaintext ● Hex

Autodetect: ON | OFF

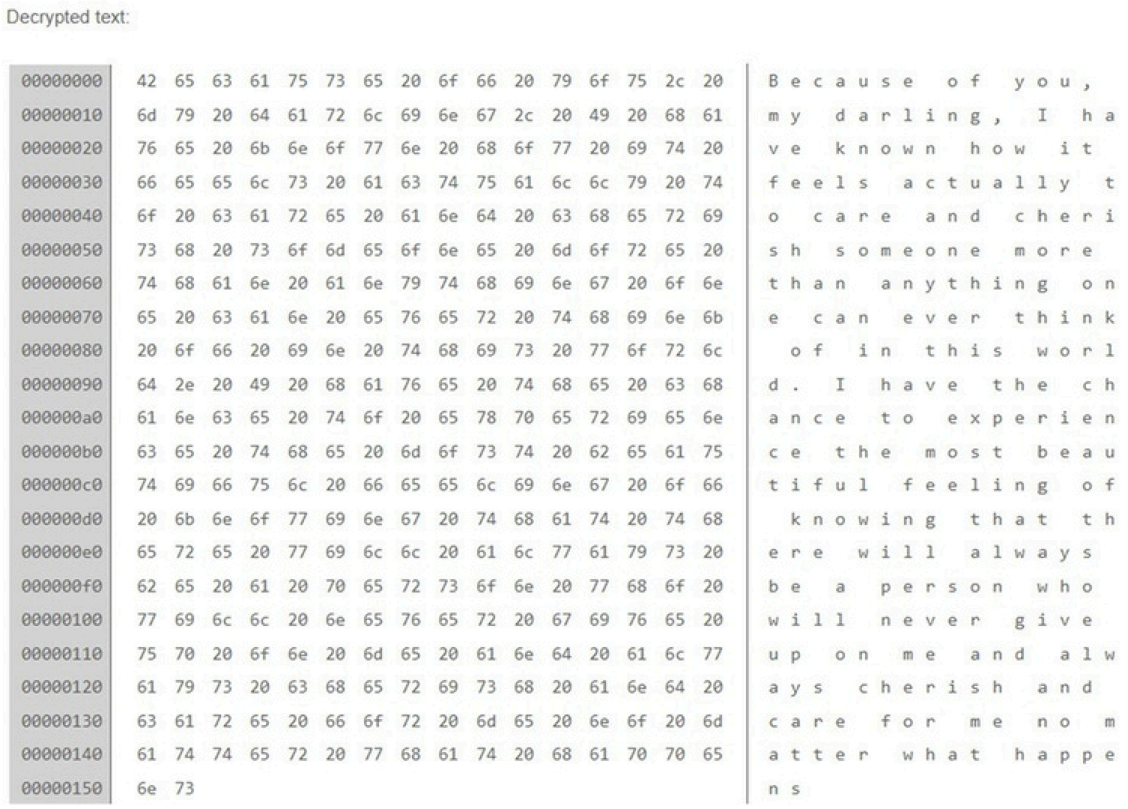
Function: DES

Mode: CFB (cipher feedback)

Key: (plain) dhruuv

● Plaintext ○ Hex

Init. vector: 21 e2 b0 8a 35 5a db 8d

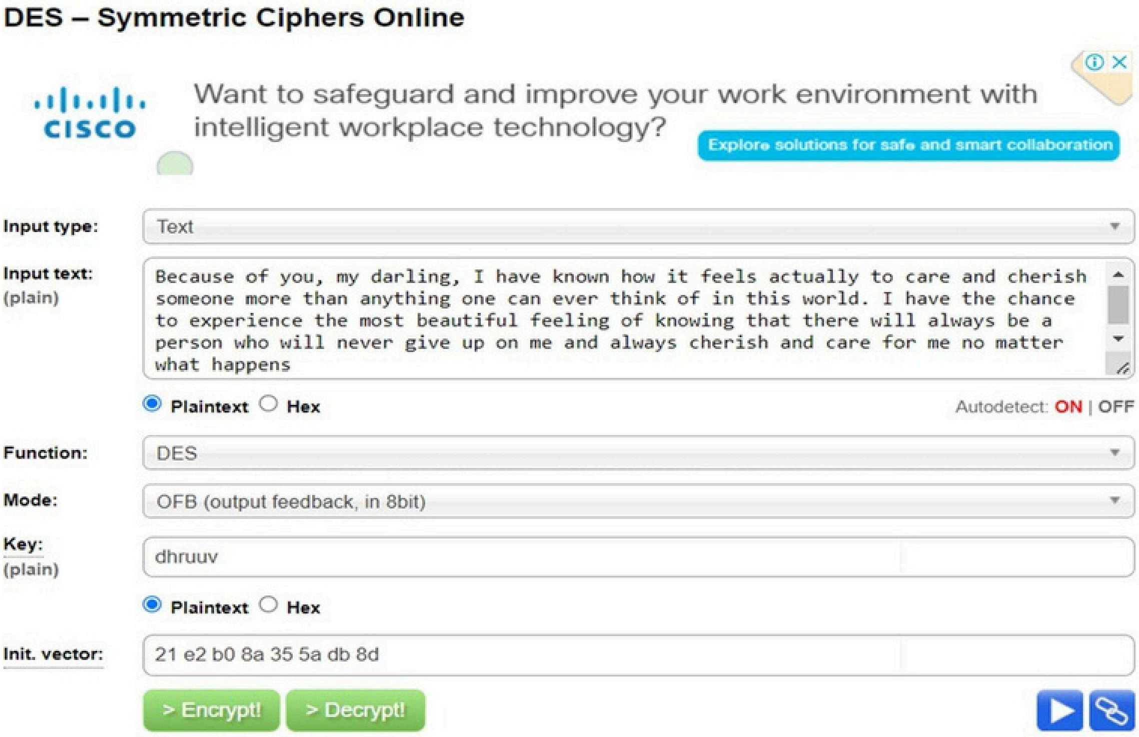


Decrypted text:

```
00000000  42 65 63 61 75 73 65 20 6f 66 20 79 6f 75 2c 20  Because of you, 
00000010  6d 79 20 64 61 72 6c 69 6e 67 2c 20 49 20 68 61  my darling, I ha
00000020  76 65 20 6b 6e 6f 77 6e 20 68 6f 77 20 69 74 20  ve known how it 
00000030  66 65 65 6c 73 20 61 63 74 75 61 6c 6c 79 20 74  feels actually t
00000040  6f 20 63 61 72 65 20 61 6e 64 20 63 68 65 72 69  o care and cheri
00000050  73 68 20 73 6f 6d 65 6f 6e 65 20 6d 6f 72 65 20  sh someone more 
00000060  74 68 61 6e 20 61 6e 79 74 68 69 6e 67 20 6f 6e  than anything on
00000070  65 20 63 61 6e 20 65 76 65 72 20 74 68 69 6e 6b  e can ever think
00000080  20 6f 66 20 69 6e 20 74 68 69 73 20 77 6f 72 6c   of in this worl
00000090  64 2e 20 49 20 68 61 76 65 20 74 68 65 20 63 68  d. I have the ch
000000a0  61 6e 63 65 20 74 6f 20 65 78 70 65 72 69 65 6e  ance to experien
000000b0  63 65 20 74 68 65 20 6d 6f 73 74 20 62 65 61 75  ce the most beau
000000c0  74 69 66 75 6c 20 66 65 65 6c 69 6e 67 20 6f 66  tiful feeling of
000000d0  20 6b 6e 6f 77 69 6e 67 20 74 68 61 74 20 74 68   knowing that th
000000e0  65 72 65 20 77 69 6c 6c 20 61 6c 77 61 79 73 20  ere will always 
000000f0  62 65 20 61 20 70 65 72 73 6f 6e 20 77 68 6f 20  be a person who 
00000100  77 69 6c 6c 20 6e 65 76 65 72 20 67 69 76 65 20  will never give 
00000110  75 70 20 6f 6e 20 6d 65 20 61 6e 64 20 61 6c 77  up on me and alw
00000120  61 79 73 20 63 68 65 72 69 73 68 20 61 6e 64 20  ays cherish and 
00000130  63 61 72 65 20 66 6f 72 20 6d 65 20 6e 6f 20 6d  care for me no m
00000140  61 74 74 65 72 20 77 68 61 74 20 68 61 70 70 65  atter what happe
00000150  6e 73                                            ns
```

1.4 OFB

Encryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (plain)

```
Because of you, my darling, I have known how it feels actually to care and cherish
someone more than anything one can ever think of in this world. I have the chance
to experience the most beautiful feeling of knowing that there will always be a
person who will never give up on me and always cherish and care for me no matter
what happens
```

● Plaintext ○ Hex Autodetect: ON | OFF

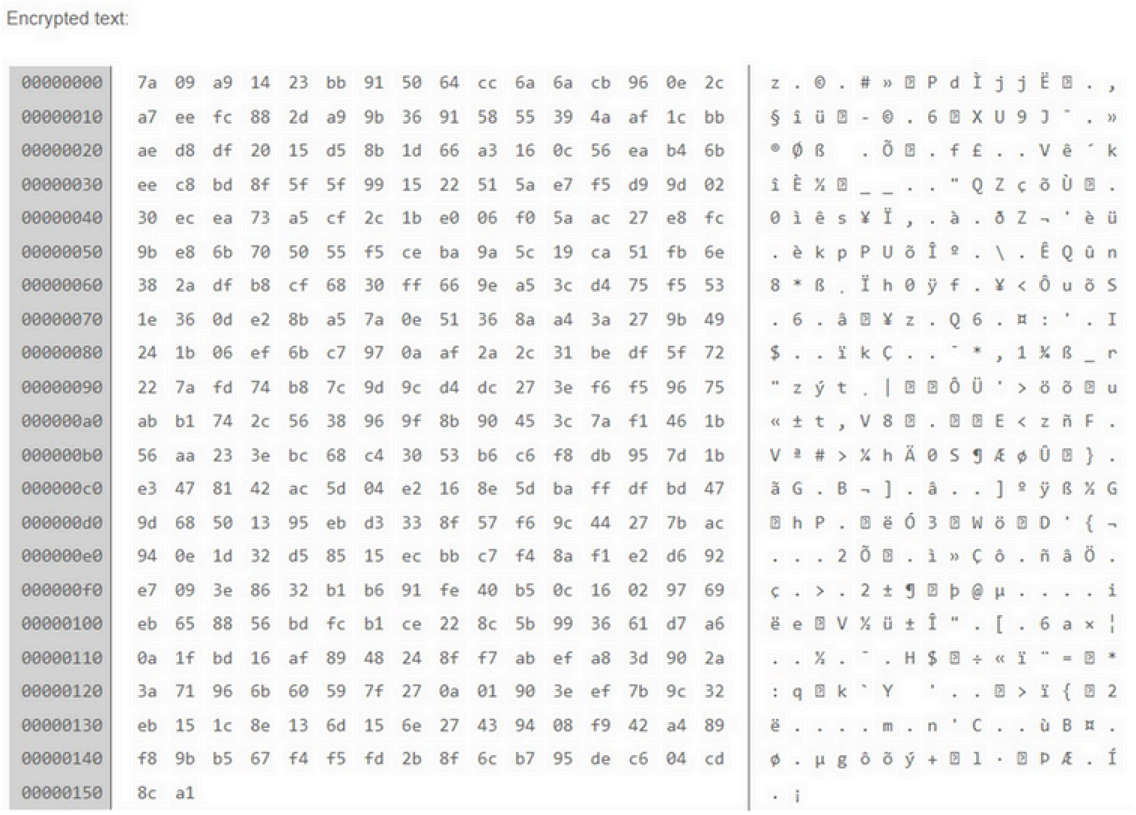
Function: DES

Mode: OFB (output feedback, in 8bit)

Key: (plain) dhruuv

● Plaintext ○ Hex

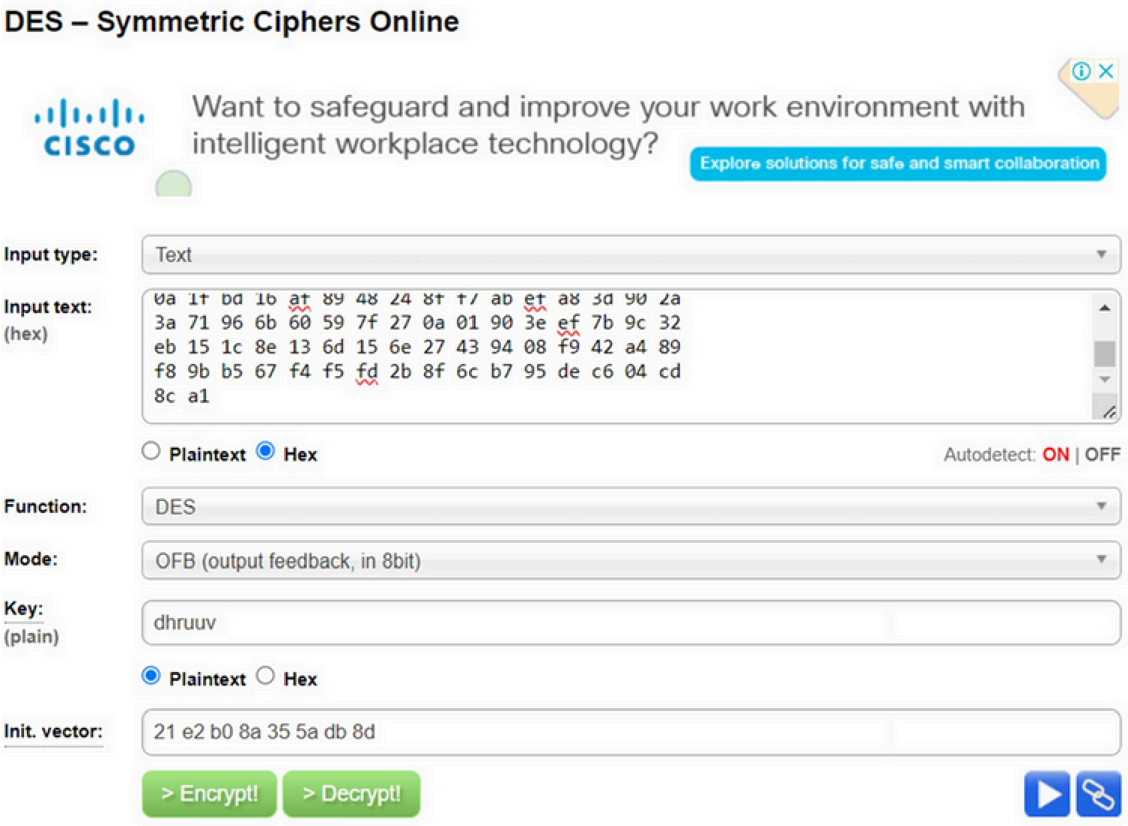
Init. vector: 21 e2 b0 8a 35 5a db 8d



Encrypted text:

```
00000000  7a 09 a9 14 23 bb 91 50 64 cc 6a 6a cb 96 0e 2c  z . © . # » ▯ P d Ì j j Ë ▯ . ,
00000010  a7 ee fc 88 2d a9 9b 36 91 58 55 39 4a af 1c bb  § î ü ▯ - © . 6 ▯ X U 9 J ¯ . »
00000020  ae d8 df 20 15 d5 8b 1d 66 a3 16 0c 56 ea b4 6b  ® ø ß   . Õ ▯ . f £ . . V ê ´ k
00000030  ee c8 bd 8f 5f 5f 99 15 22 51 5a e7 f5 d9 9d 02  î È ½ ▯ _ _ . . " Q Z ç õ Ù ▯ .
00000040  30 ec ea 73 a5 cf 2c 1b e0 06 f0 5a ac 27 e8 fc  0 ì ê s ¥ Ï , . à . ð Z ¬ ' è ü
00000050  9b e8 6b 70 50 55 f5 ce ba 9a 5c 19 ca 51 fb 6e  . è k p P U õ Î º . \ . Ê Q û n
00000060  38 2a df b8 cf 68 30 ff 66 9e a5 3c d4 75 f5 53  8 * ß ¸ Ï h 0 ÿ f . ¥ < Ô u õ S
00000070  1e 36 0d e2 8b a5 7a 0e 51 36 8a a4 3a 27 9b 49  . 6 . â ▯ ¥ z . Q 6 . ¤ : ' . I
00000080  24 1b 06 ef 6b c7 97 0a af 2a 2c 31 be df 5f 72  $ . . ï k Ç . . ¯ * , 1 ¾ ß _ r
00000090  22 7a fd 74 b8 7c 9d 9c d4 dc 27 3e f6 f5 96 75  " z ý t ¸ | ▯ ▯ Ô Ü ' > ö õ ▯ u
000000a0  ab b1 74 2c 56 38 96 9f 8b 90 45 3c 7a f1 46 1b  « ± t , V 8 ▯ . ▯ ▯ E < z ñ F .
000000b0  56 aa 23 3e bc 68 c4 30 53 b6 c6 f8 db 95 7d 1b  V ª # > ¼ h Ä 0 S ¶ Æ ø Û ▯ } .
000000c0  e3 47 81 42 ac 5d 04 e2 16 8e 5d ba ff df bd 47  ã G . B ¬ ] . â . . ] º ÿ ß ½ G
000000d0  9d 68 50 13 95 eb d3 33 8f 57 f6 9c 44 27 7b ac  ▯ h P . ▯ ë Ó 3 ▯ W ö ▯ D ' { ¬
000000e0  94 0e 1d 32 d5 85 15 ec bb c7 f4 8a f1 e2 d6 92  . . . 2 Õ ▯ . ì » Ç ô . ñ â Ö .
000000f0  e7 09 3e 86 32 b1 b6 91 fe 40 b5 0c 16 02 97 69  ç . > . 2 ± ¶ ▯ þ @ µ . . . . i
00000100  eb 65 88 56 bd fc b1 ce 22 8c 5b 99 36 61 d7 a6  ë e ▯ V ½ ü ± Î " . [ . 6 a × ¦
00000110  0a 1f bd 16 af 89 48 24 8f f7 ab ef a8 3d 90 2a  . . ½ . ¯ . H $ ▯ ÷ « ï ¨ = ▯ *
00000120  3a 71 96 6b 60 59 7f 27 0a 01 90 3e ef 7b 9c 32  : q ▯ k ` Y   ' . . ▯ > ï { ▯ 2
00000130  eb 15 1c 8e 13 6d 15 6e 27 43 94 08 f9 42 a4 89  ë . . . . m . n ' C . . ù B ¤ .
00000140  f8 9b b5 67 f4 f5 fd 2b 8f 6c b7 95 de c6 04 cd  ø . µ g ô õ ý + ▯ l · ▯ Þ Æ . Í
00000150  8c a1                                            . ¡
```

Decryption



DES – Symmetric Ciphers Online

Input type: Text

Input text: (hex)

```
0a 1f bd 16 af 89 48 24 8f f7 ab ef a8 3d 90 2a
3a 71 96 6b 60 59 7f 27 0a 01 90 3e ef 7b 9c 32
eb 15 1c 8e 13 6d 15 6e 27 43 94 08 f9 42 a4 89
f8 9b b5 67 f4 f5 fd 2b 8f 6c b7 95 de c6 04 cd
8c a1
```

○ Plaintext ● Hex

Autodetect: ON | OFF

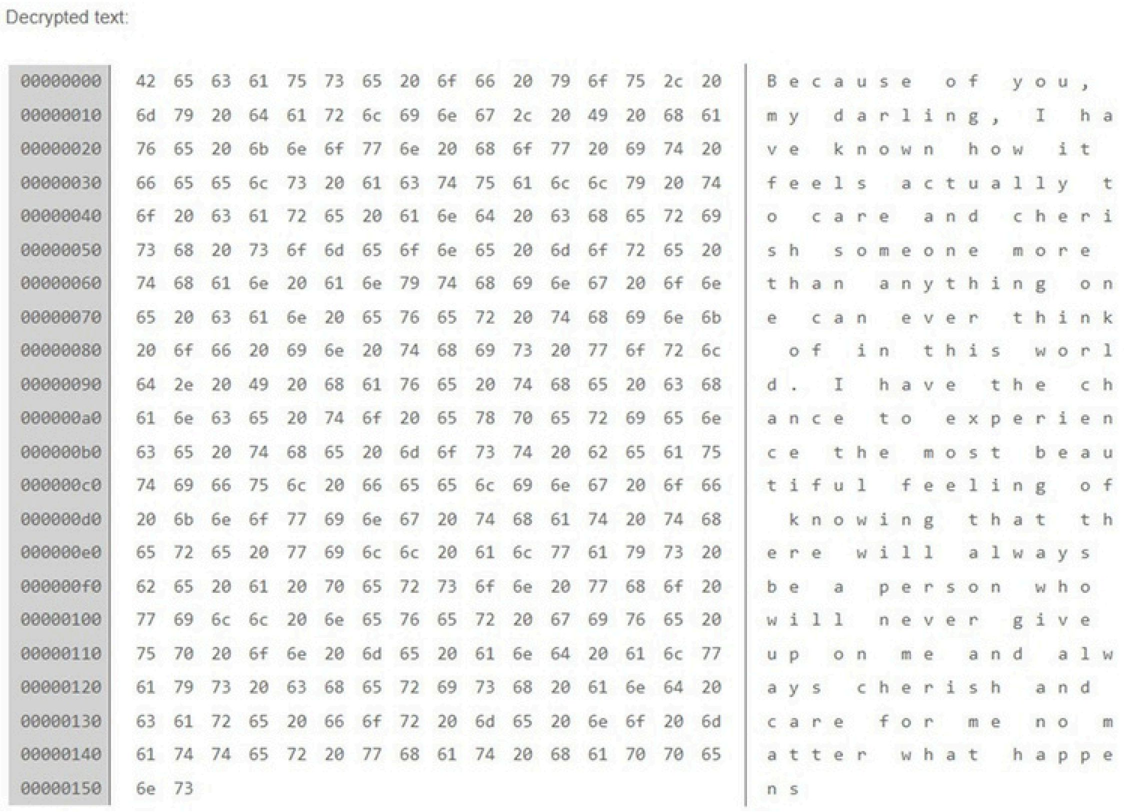
Function: DES

Mode: OFB (output feedback, in 8bit)

Key: (plain) dhruuv

● Plaintext ○ Hex

Init. vector: 21 e2 b0 8a 35 5a db 8d



Decrypted text:

```
00000000  42 65 63 61 75 73 65 20 6f 66 20 79 6f 75 2c 20  | Because of you, 
00000010  6d 79 20 64 61 72 6c 69 6e 67 2c 20 49 20 68 61  | my darling, I ha
00000020  76 65 20 6b 6e 6f 77 6e 20 68 6f 77 20 69 74 20  | ve known how it 
00000030  66 65 65 6c 73 20 61 63 74 75 61 6c 6c 79 20 74  | feels actually t
00000040  6f 20 63 61 72 65 20 61 6e 64 20 63 68 65 72 69  | o care and cheri
00000050  73 68 20 73 6f 6d 65 6f 6e 65 20 6d 6f 72 65 20  | sh someone more 
00000060  74 68 61 6e 20 61 6e 79 74 68 69 6e 67 20 6f 6e  | than anything on
00000070  65 20 63 61 6e 20 65 76 65 72 20 74 68 69 6e 6b  | e can ever think
00000080  20 6f 66 20 69 6e 20 74 68 69 73 20 77 6f 72 6c  |  of in this worl
00000090  64 2e 20 49 20 68 61 76 65 20 74 68 65 20 63 68  | d. I have the ch
000000a0  61 6e 63 65 20 74 6f 20 65 78 70 65 72 69 65 6e  | ance to experien
000000b0  63 65 20 74 68 65 20 6d 6f 73 74 20 62 65 61 75  | ce the most beau
000000c0  74 69 66 75 6c 20 66 65 65 6c 69 6e 67 20 6f 66  | tiful feeling of
000000d0  20 6b 6e 6f 77 69 6e 67 20 74 68 61 74 20 74 68  |  knowing that th
000000e0  65 72 65 20 77 69 6c 6c 20 61 6c 77 61 79 73 20  | ere will always 
000000f0  62 65 20 61 20 70 65 72 73 6f 6e 20 77 68 6f 20  | be a person who 
00000100  77 69 6c 6c 20 6e 65 76 65 72 20 67 69 76 65 20  | will never give 
00000110  75 70 20 6f 6e 20 6d 65 20 61 6e 64 20 61 6c 77  | up on me and alw
00000120  61 79 73 20 63 68 65 72 69 73 68 20 61 6e 64 20  | ays cherish and 
00000130  63 61 72 65 20 66 6f 72 20 6d 65 20 6e 6f 20 6d  | care for me no m
00000140  61 74 74 65 72 20 77 68 61 74 20 68 61 70 70 65  | atter what happe
00000150  6e 73                                            | ns
```

Comparison of block cipher modes: ECB: Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption. Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

CBC: CBC works well for input greater than b bits. CBC is a good authentication mechanism. Better resistive nature towards cryptanalysis than ECB.

Parallel encryption is not possible since every encryption requires a previous cipher.

CFB:

Since, there is some data loss due to the use of shift register, thus it is difficult for applying cryptanalysis.

The drawbacks of CFB are the same as those of CBC mode. Both block losses and concurrent encryption of several blocks are not supported by the encryption. Decryption, however, is parallelizable and loss-tolerant.

OFB: In the case of CFB, a single bit error in a block is propagated to all subsequent blocks. This problem is solved by OFB as it is free from bit errors in the plaintext block.
The drawback of OFB is that, because to its operational modes, it is more susceptible to a message stream modification attack than CFB.

CTR: Since there is a different counter value for each block, the direct plaintext and ciphertext relationship is avoided. This means that the same plain text can map to different ciphertext. Parallel execution of encryption is possible as outputs from previous stages are not chained as in the case of CBC.
The fact that CTR mode requires a synchronous counter at both the transmitter and the receiver is a severe drawback. The recovery of plaintext is erroneous when synchronisation is lost.

Cipher Block Chaining (CBC):

CBC mode XORs each plaintext block with the previous ciphertext block before encryption.

Requires an Initialization Vector (IV) to start the process. Provides confidentiality and data integrity but not authentication. Parallelization is challenging due to the dependency on previous ciphertext blocks.

Cipher Feedback (CFB): CFB mode turns a block cipher into a stream cipher. It operates on a bit or byte level, providing inherent support for streaming data. It doesn't require padding and allows any size of plaintext to be encrypted. It's sensitive to bit errors in the ciphertext and requires synchronization. Output Feedback (OFB): OFB mode also turns a block cipher into a stream cipher. Like CFB, it operates on a bit or byte level and allows any size of plaintext. Bit errors in the ciphertext don't affect decryption, but it doesn't provide data integrity or authentication.

Counter (CTR): CTR mode turns a block cipher into a stream cipher similar to OFB and CFB. It uses a counter as input to the block cipher, generating a stream of key-based pseudo-random values. Well- suited for parallelization and random access, making it suitable for disk encryption and secure communication.

References:

1. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf 2.

https://www.geeksforgeeks.org/block-cipher-modes-of-operation/ 3.

https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf 4.

https://www.youtube.com/watch?v=fgyfvRuhMvM

Questions (Short, Long, MCQs) (optional): L1: Explain different Block cipher modes of operation Electronic Codebook (ECB): ECB mode encrypts each block of plaintext independently with the same key. It is deterministic, meaning the same plaintext block will always produce the same ciphertext block. Vulnerable to patterns in the plaintext, making it unsuitable for encrypting large amounts of structured data.