Experiment Number: 5

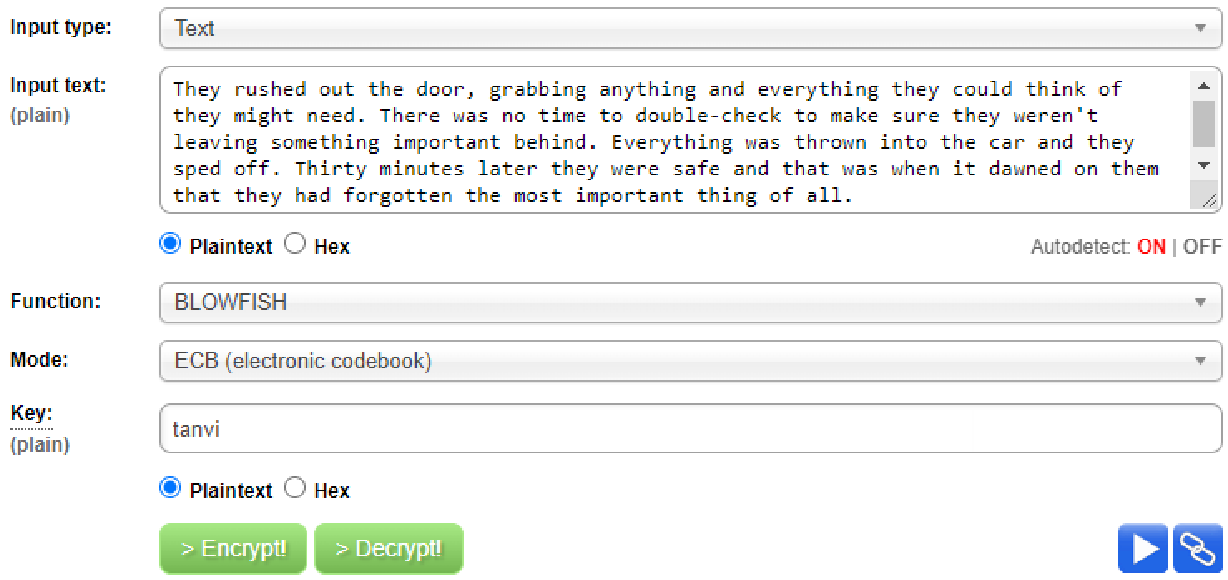
UID : 2019140050 **Name: Tanvi Sunil Pen**

Batch: C **Branch: TE IT**

AIM : The aim of this lab is to experiment with an online encryption tool. We will encode a message and send it to someone else in the class, who will decode it when we supply the secret key. Note that this particular tool is of limited use in a security context, since the plaintext of the message is sent to and from the encryption website! However, it could be used to prevent people from reading your email. A similar tool downloaded and running on your computer would provide a greater level of security. Some email clients even provide support for automatic encryption and decryption of all messages.

PROBLEM STATEMENT:

1) **Go to the encryption tool website and try it out. Enter a short key phrase and a longer piece of text to be encoded. Then submit and see what your text looks like when encrypted. Try the following experiments and note how they change the output:**



Input type: Text

Input text: (plain)

```
They rushed out the door, grabbing anything and everything they could think of
they might need. There was no time to double-check to make sure they weren't
leaving something important behind. Everything was thrown into the car and they
sped off. Thirty minutes later they were safe and that was when it dawned on them
that they had forgotten the most important thing of all.
```

● Plaintext ○ Hex

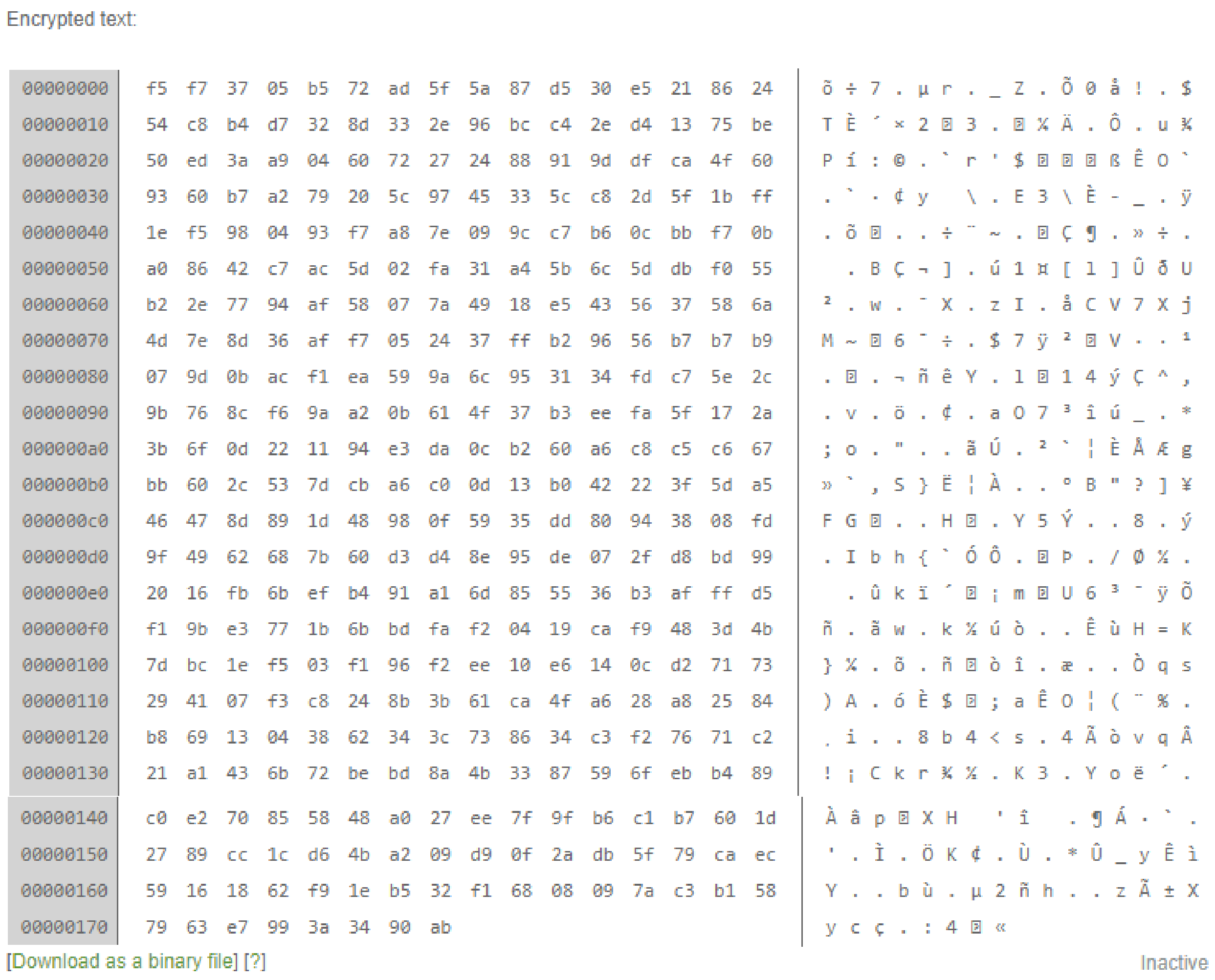
Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvi

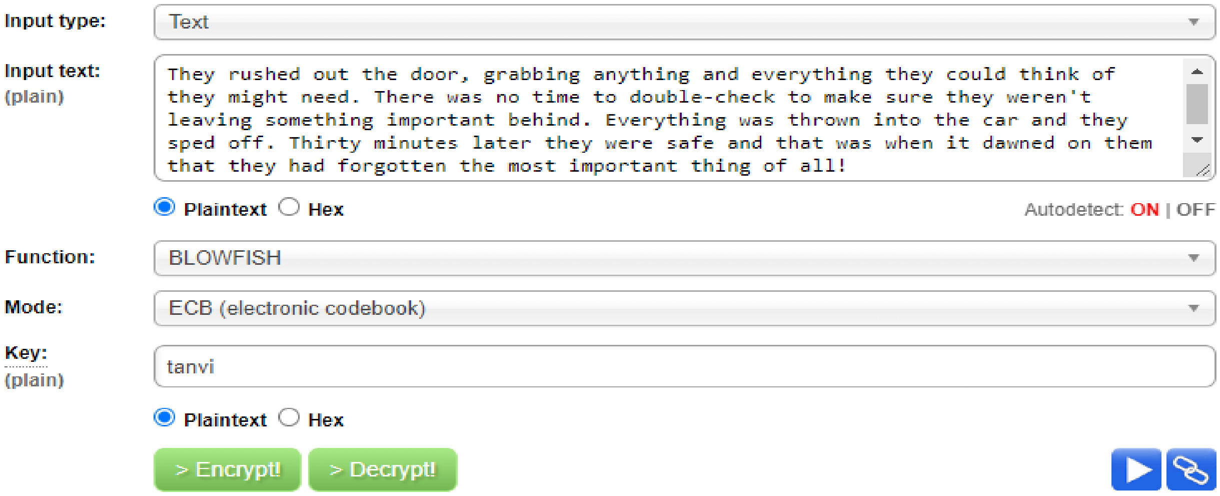
● Plaintext ○ Hex



Encrypted text:

```
00000000  f5 f7 37 05 b5 72 ad 5f 5a 87 d5 30 e5 21 86 24  õ ÷ 7 . µ r . _ Z . Õ 0 å ! . $
00000010  54 c8 b4 d7 32 8d 33 2e 96 bc c4 2e d4 13 75 be  T È ´ × 2 ⍰ 3 . ⍰ ¼ Ä . Ô . u ¾
00000020  50 ed 3a a9 04 60 72 27 24 88 91 9d df ca 4f 60  P í : © . ` r ' $ ⍰ ⍰ ⍰ ß Ê O `
00000030  93 60 b7 a2 79 20 5c 97 45 33 5c c8 2d 5f 1b ff  . ` · ¢ y   \ . E 3 \ È - _ . ÿ
00000040  1e f5 98 04 93 f7 a8 7e 09 9c c7 b6 0c bb f7 0b  . õ ⍰ . . ÷ ¨ ~ . ⍰ Ç ¶ . » ÷ .
00000050  a0 86 42 c7 ac 5d 02 fa 31 a4 5b 6c 5d db f0 55    . B Ç ¬ ] . ú 1 ¤ [ l ] Û ð U
00000060  b2 2e 77 94 af 58 07 7a 49 18 e5 43 56 37 58 6a  ² . w . ¯ X . z I . å C V 7 X j
00000070  4d 7e 8d 36 af f7 05 24 37 ff b2 96 56 b7 b7 b9  M ~ ⍰ 6 ¯ ÷ . $ 7 ÿ ² ⍰ V · · ¹
00000080  07 9d 0b ac f1 ea 59 9a 6c 95 31 34 fd c7 5e 2c  . ⍰ . ¬ ñ ê Y . l ⍰ 1 4 ý Ç ^ ,
00000090  9b 76 8c f6 9a a2 0b 61 4f 37 b3 ee fa 5f 17 2a  . v . ö . ¢ . a O 7 ³ î ú _ . *
000000a0  3b 6f 0d 22 11 94 e3 da 0c b2 60 a6 c8 c5 c6 67  ; o . " . . ã Ú . ² ` ¦ È Å Æ g
000000b0  bb 60 2c 53 7d cb a6 c0 0d 13 b0 42 22 3f 5d a5  » ` , S } Ë ¦ À . . ° B " ? ] ¥
000000c0  46 47 8d 89 1d 48 98 0f 59 35 dd 80 94 38 08 fd  F G ⍰ . . H ⍰ . Y 5 Ý . . 8 . ý
000000d0  9f 49 62 68 7b 60 d3 d4 8e 95 de 07 2f d8 bd 99  . I b h { ` Ó Ô . ⍰ Þ . / Ø ½ .
000000e0  20 16 fb 6b ef b4 91 a1 6d 85 55 36 b3 af ff d5    . û k ï ´ ⍰ ¡ m ⍰ U 6 ³ ¯ ÿ Õ
000000f0  f1 9b e3 77 1b 6b bd fa f2 04 19 ca f9 48 3d 4b  ñ . ã w . k ½ ú ò . . Ê ù H = K
00000100  7d bc 1e f5 03 f1 96 f2 ee 10 e6 14 0c d2 71 73  } ¼ . õ . ñ ⍰ ò î . æ . . Ò q s
00000110  29 41 07 f3 c8 24 8b 3b 61 ca 4f a6 28 a8 25 84  ) A . ó È $ ⍰ ; a Ê O ¦ ( ¨ % .
00000120  b8 69 13 04 38 62 34 3c 73 86 34 c3 f2 76 71 c2  ¸ i . . 8 b 4 < s . 4 Ã ò v q Â
00000130  21 a1 43 6b 72 be bd 8a 4b 33 87 59 6f eb b4 89  ! ¡ C k r ¾ ½ . K 3 . Y o ë ´ .
00000140  c0 e2 70 85 58 48 a0 27 ee 7f 9f b6 c1 b7 60 1d  À â p ⍰ X H   ' î   . ¶ Á · ` .
00000150  27 89 cc 1c d6 4b a2 09 d9 0f 2a db 5f 79 ca ec  ' . Ì . Ö K ¢ . Ù . * Û _ y Ê ì
00000160  59 16 18 62 f9 1e b5 32 f1 68 08 09 7a c3 b1 58  Y . . b ù . µ 2 ñ h . . z Ã ± X
00000170  79 63 e7 99 3a 34 90 ab                          y c ç . : 4 ⍰ «
```

- **Change one character at the end of the message. How much of the encoded message changes?**



Input type: Text

Input text: (plain)

```
They rushed out the door, grabbing anything and everything they could think of
they might need. There was no time to double-check to make sure they weren't
leaving something important behind. Everything was thrown into the car and they
sped off. Thirty minutes later they were safe and that was when it dawned on them
that they had forgotten the most important thing of all!
```

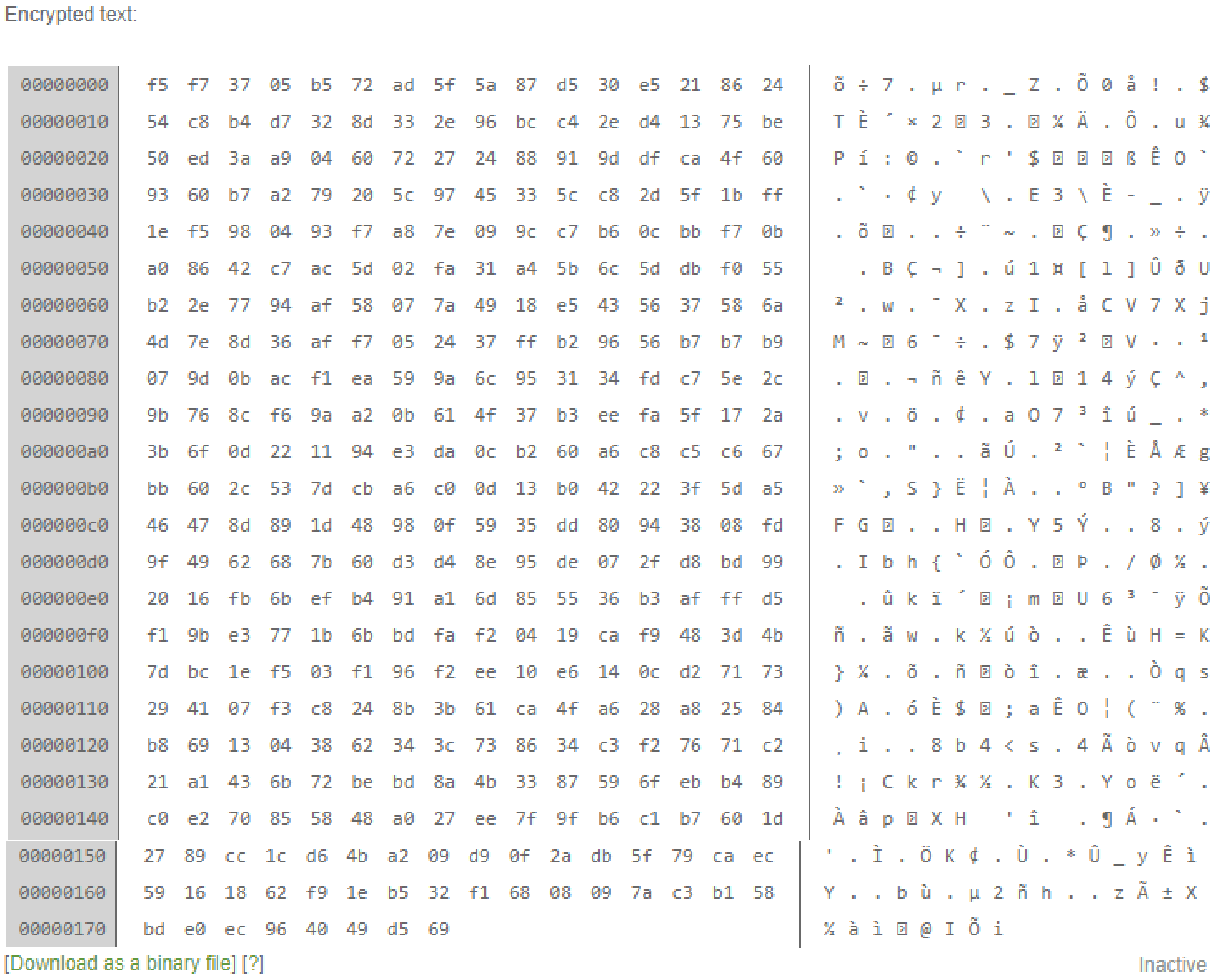
● Plaintext ○ Hex

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvi

● Plaintext ○ Hex



Encrypted text:

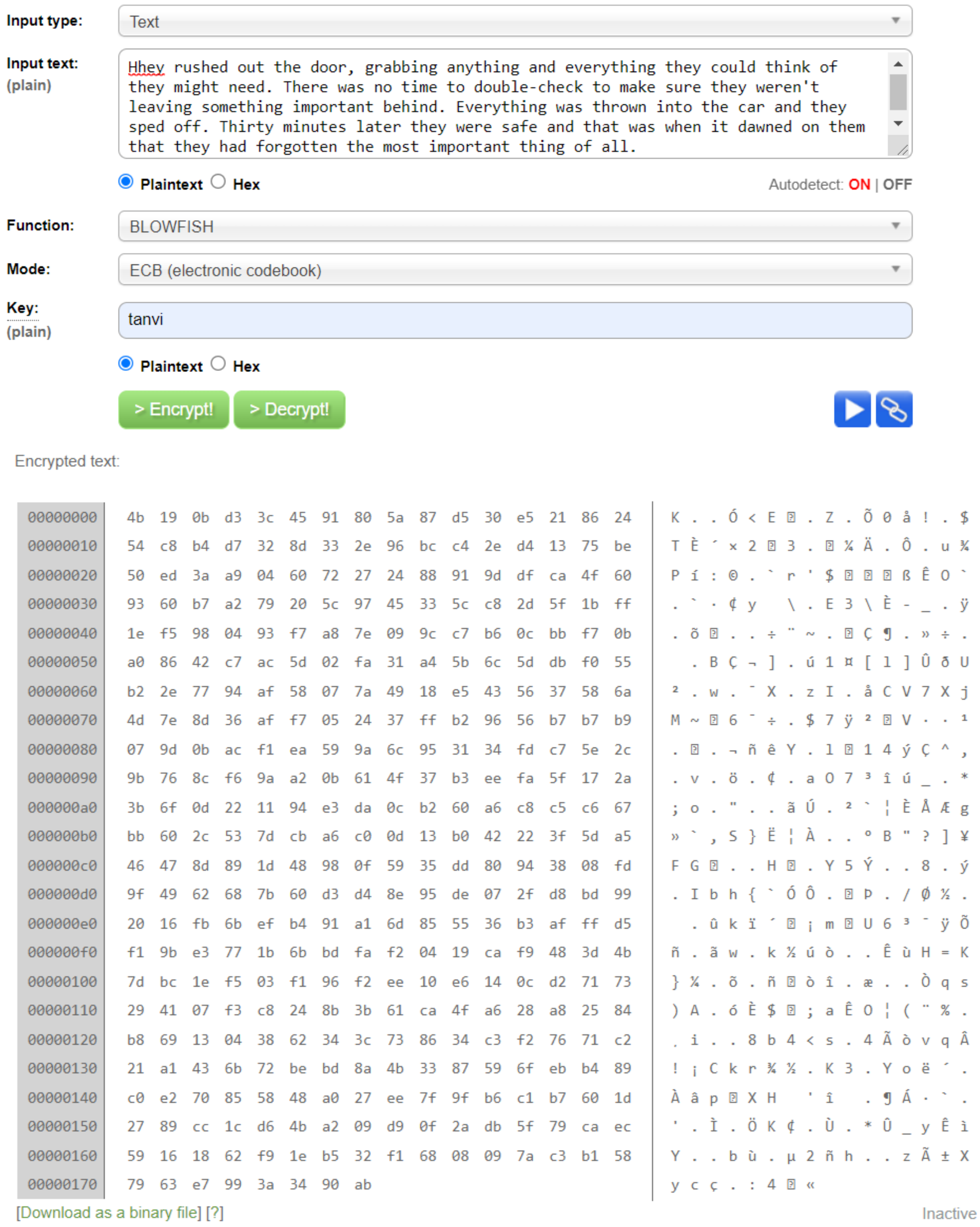
```
00000000  f5 f7 37 05 b5 72 ad 5f 5a 87 d5 30 e5 21 86 24  õ ÷ 7 . µ r . _ Z . Õ 0 å ! . $
00000010  54 c8 b4 d7 32 8d 33 2e 96 bc c4 2e d4 13 75 be  T È ´ × 2 ⍰ 3 . ⍰ ¼ Ä . Ô . u ¾
00000020  50 ed 3a a9 04 60 72 27 24 88 91 9d df ca 4f 60  P í : © . ` r ' $ ⍰ ⍰ ⍰ ß Ê O `
00000030  93 60 b7 a2 79 20 5c 97 45 33 5c c8 2d 5f 1b ff  . ` · ¢ y   \ . E 3 \ È - _ . ÿ
00000040  1e f5 98 04 93 f7 a8 7e 09 9c c7 b6 0c bb f7 0b  . õ ⍰ . . ÷ ¨ ~ . ⍰ Ç ¶ . » ÷ .
00000050  a0 86 42 c7 ac 5d 02 fa 31 a4 5b 6c 5d db f0 55    . B Ç ¬ ] . ú 1 ¤ [ l ] Û ð U
00000060  b2 2e 77 94 af 58 07 7a 49 18 e5 43 56 37 58 6a  ² . w . ¯ X . z I . å C V 7 X j
00000070  4d 7e 8d 36 af f7 05 24 37 ff b2 96 56 b7 b7 b9  M ~ ⍰ 6 ¯ ÷ . $ 7 ÿ ² ⍰ V · · ¹
00000080  07 9d 0b ac f1 ea 59 9a 6c 95 31 34 fd c7 5e 2c  . ⍰ . ¬ ñ ê Y . l ⍰ 1 4 ý Ç ^ ,
00000090  9b 76 8c f6 9a a2 0b 61 4f 37 b3 ee fa 5f 17 2a  . v . ö . ¢ . a O 7 ³ î ú _ . *
000000a0  3b 6f 0d 22 11 94 e3 da 0c b2 60 a6 c8 c5 c6 67  ; o . " . . ã Ú . ² ` ¦ È Å Æ g
000000b0  bb 60 2c 53 7d cb a6 c0 0d 13 b0 42 22 3f 5d a5  » ` , S } Ë ¦ À . . ° B " ? ] ¥
000000c0  46 47 8d 89 1d 48 98 0f 59 35 dd 80 94 38 08 fd  F G ⍰ . . H ⍰ . Y 5 Ý . . 8 . ý
000000d0  9f 49 62 68 7b 60 d3 d4 8e 95 de 07 2f d8 bd 99  . I b h { ` Ó Ô . ⍰ Þ . / Ø ½ .
000000e0  20 16 fb 6b ef b4 91 a1 6d 85 55 36 b3 af ff d5    . û k ï ´ ⍰ ¡ m ⍰ U 6 ³ ¯ ÿ Õ
000000f0  f1 9b e3 77 1b 6b bd fa f2 04 19 ca f9 48 3d 4b  ñ . ã w . k ½ ú ò . . Ê ù H = K
00000100  7d bc 1e f5 03 f1 96 f2 ee 10 e6 14 0c d2 71 73  } ¼ . õ . ñ ⍰ ò î . æ . . Ò q s
00000110  29 41 07 f3 c8 24 8b 3b 61 ca 4f a6 28 a8 25 84  ) A . ó È $ ⍰ ; a Ê O ¦ ( ¨ % .
00000120  b8 69 13 04 38 62 34 3c 73 86 34 c3 f2 76 71 c2  ¸ i . . 8 b 4 < s . 4 Ã ò v q Â
00000130  21 a1 43 6b 72 be bd 8a 4b 33 87 59 6f eb b4 89  ! ¡ C k r ¾ ½ . K 3 . Y o ë ´ .
00000140  c0 e2 70 85 58 48 a0 27 ee 7f 9f b6 c1 b7 60 1d  À â p ⍰ X H   ' î   . ¶ Á · ` .
00000150  27 89 cc 1c d6 4b a2 09 d9 0f 2a db 5f 79 ca ec  ' . Ì . Ö K ¢ . Ù . * Û _ y Ê ì
00000160  59 16 18 62 f9 1e b5 32 f1 68 08 09 7a c3 b1 58  Y . . b ù . µ 2 ñ h . . z Ã ± X
00000170  bd e0 ec 96 40 49 d5 69                          ½ à ì ⍰ @ I Õ i
```

[Download as a binary file] [?]

Inactive

The change that I observed was that the entire last block ended up changing in the encrypted text.

- **Change one character at the beginning of the message. How much of the encoded message changes?**



Input type: Text

Input text: (plain)

```
Hhey rushed out the door, grabbing anything and everything they could think of
they might need. There was no time to double-check to make sure they weren't
leaving something important behind. Everything was thrown into the car and they
sped off. Thirty minutes later they were safe and that was when it dawned on them
that they had forgotten the most important thing of all.
```

● Plaintext ○ Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvi

● Plaintext ○ Hex

Encrypted text:

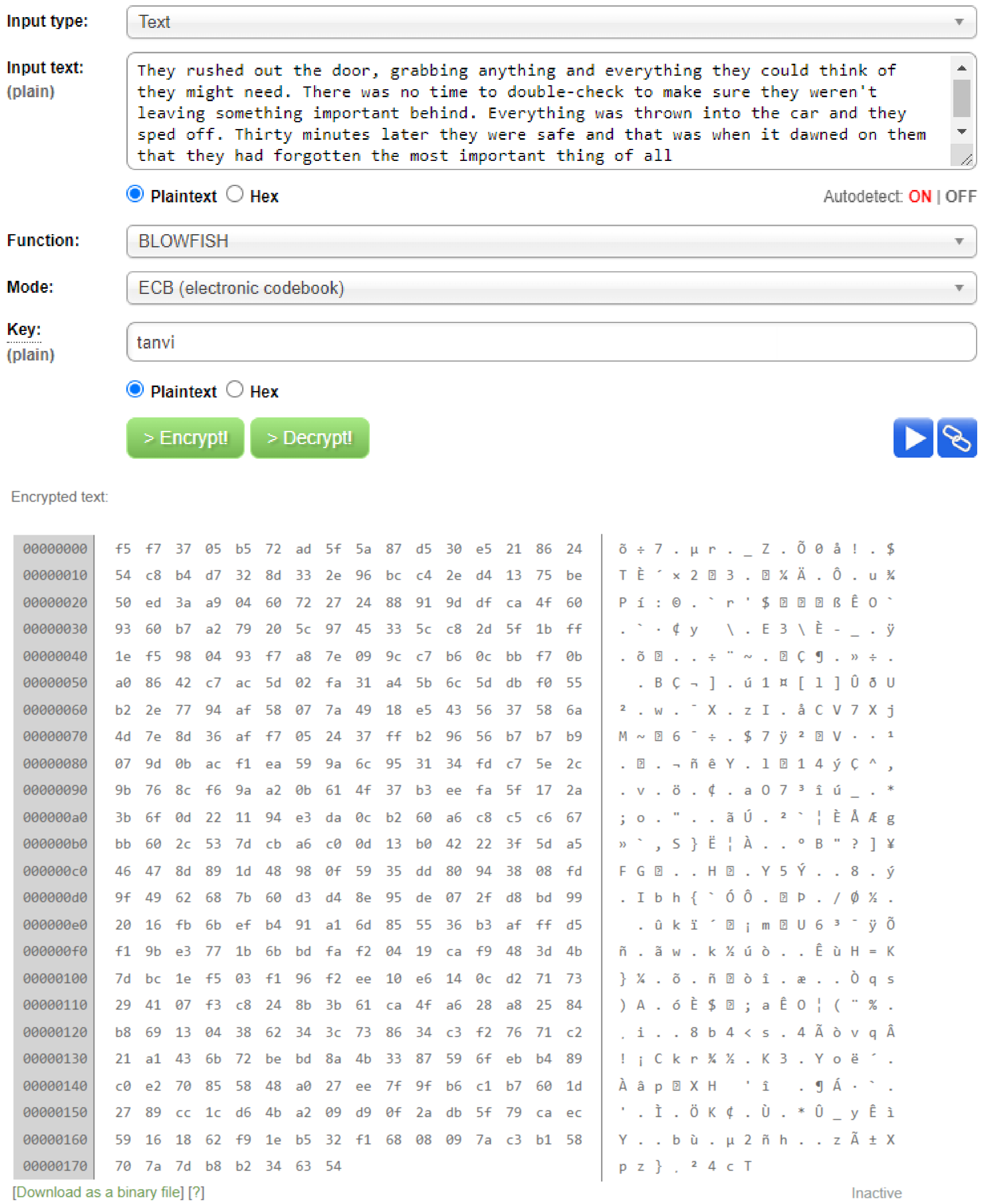
```
00000000  4b 19 0b d3 3c 45 91 80 5a 87 d5 30 e5 21 86 24   K . . Ó < E ▯ . Z . Õ 0 å ! . $
00000010  54 c8 b4 d7 32 8d 33 2e 96 bc c4 2e d4 13 75 be   T È ´ × 2 ▯ 3 . ▯ ¼ Ä . Ô . u ¾
00000020  50 ed 3a a9 04 60 72 27 24 88 91 9d df ca 4f 60   P í : © . ` r ' $ ▯ ▯ ▯ ß Ê O `
00000030  93 60 b7 a2 79 20 5c 97 45 33 5c c8 2d 5f 1b ff   . ` · ¢ y   \ . E 3 \ È - _ . ÿ
00000040  1e f5 98 04 93 f7 a8 7e 09 9c c7 b6 0c bb f7 0b   . õ ▯ . . ÷ ¨ ~ . ▯ Ç ¶ . » ÷ .
00000050  a0 86 42 c7 ac 5d 02 fa 31 a4 5b 6c 5d db f0 55     . B Ç ¬ ] . ú 1 ¤ [ l ] Û ð U
00000060  b2 2e 77 94 af 58 07 7a 49 18 e5 43 56 37 58 6a   ² . w . ¯ X . z I . å C V 7 X j
00000070  4d 7e 8d 36 af f7 05 24 37 ff b2 96 56 b7 b7 b9   M ~ ▯ 6 ¯ ÷ . $ 7 ÿ ² ▯ V · · ¹
00000080  07 9d 0b ac f1 ea 59 9a 6c 95 31 34 fd c7 5e 2c   . ▯ . ¬ ñ ê Y . l ▯ 1 4 ý Ç ^ ,
00000090  9b 76 8c f6 9a a2 0b 61 4f 37 b3 ee fa 5f 17 2a   . v . ö . ¢ . a O 7 ³ î ú _ . *
000000a0  3b 6f 0d 22 11 94 e3 da 0c b2 60 a6 c8 c5 c6 67   ; o . " . . ã Ú . ² ` ¦ È Å Æ g
000000b0  bb 60 2c 53 7d cb a6 c0 0d 13 b0 42 22 3f 5d a5   » ` , S } Ë ¦ À . . ° B " ? ] ¥
000000c0  46 47 8d 89 1d 48 98 0f 59 35 dd 80 94 38 08 fd   F G ▯ . . H ▯ . Y 5 Ý . . 8 . ý
000000d0  9f 49 62 68 7b 60 d3 d4 8e 95 de 07 2f d8 bd 99   . I b h { ` Ó Ô . ▯ Þ . / Ø ½ .
000000e0  20 16 fb 6b ef b4 91 a1 6d 85 55 36 b3 af ff d5     . û k ï ´ ▯ ¡ m ▯ U 6 ³ ¯ ÿ Õ
000000f0  f1 9b e3 77 1b 6b bd fa f2 04 19 ca f9 48 3d 4b   ñ . ã w . k ½ ú ò . . Ê ù H = K
00000100  7d bc 1e f5 03 f1 96 f2 ee 10 e6 14 0c d2 71 73   } ¼ . õ . ñ ▯ ò î . æ . . Ò q s
00000110  29 41 07 f3 c8 24 8b 3b 61 ca 4f a6 28 a8 25 84   ) A . ó È $ ▯ ; a Ê O ¦ ( ¨ % .
00000120  b8 69 13 04 38 62 34 3c 73 86 34 c3 f2 76 71 c2   ¸ i . . 8 b 4 < s . 4 Ã ò v q Â
00000130  21 a1 43 6b 72 be bd 8a 4b 33 87 59 6f eb b4 89   ! ¡ C k r ¾ ½ . K 3 . Y o ë ´ .
00000140  c0 e2 70 85 58 48 a0 27 ee 7f 9f b6 c1 b7 60 1d   À â p ▯ X H   ' î   . ¶ Á · ` .
00000150  27 89 cc 1c d6 4b a2 09 d9 0f 2a db 5f 79 ca ec   ' . Ì . Ö K ¢ . Ù . * Û _ y Ê ì
00000160  59 16 18 62 f9 1e b5 32 f1 68 08 09 7a c3 b1 58   Y . . b ù . µ 2 ñ h . . z Ã ± X
00000170  79 63 e7 99 3a 34 90 ab                           y c ç . : 4 ▯ «
```

[Download as a binary file] [?]

Inactive

Similar to the above case the entire first block ended up changing on account of replacing T by H.

- **Delete one character at the end of the message. How much of the encoded message changes?**



Input type: Text

Input text: (plain)

```
They rushed out the door, grabbing anything and everything they could think of
they might need. There was no time to double-check to make sure they weren't
leaving something important behind. Everything was thrown into the car and they
sped off. Thirty minutes later they were safe and that was when it dawned on them
that they had forgotten the most important thing of all
```

● Plaintext ○ Hex

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvi

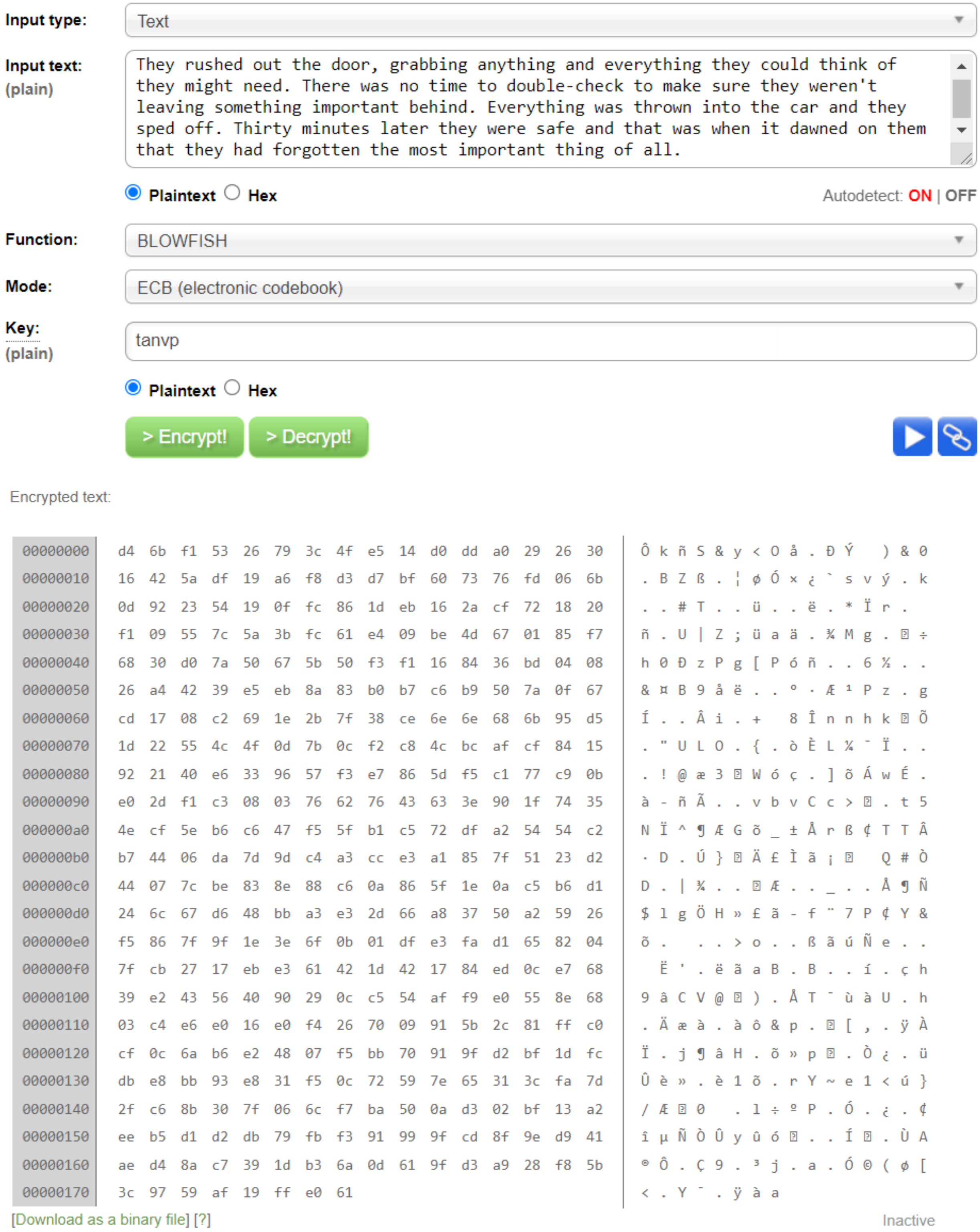
● Plaintext ○ Hex

Encrypted text:

```
00000000  f5 f7 37 05 b5 72 ad 5f 5a 87 d5 30 e5 21 86 24  õ ÷ 7 . µ r . _ Z . Õ 0 å ! . $
00000010  54 c8 b4 d7 32 8d 33 2e 96 bc c4 2e d4 13 75 be  T È ´ × 2 ⍰ 3 . ⍰ ¼ Ä . Ô . u ¾
00000020  50 ed 3a a9 04 60 72 27 24 88 91 9d df ca 4f 60  P í : © . ` r ' $ ⍰ ⍰ ⍰ ß Ê O `
00000030  93 60 b7 a2 79 20 5c 97 45 33 5c c8 2d 5f 1b ff  . ` · ¢ y   \ . E 3 \ È - _ . ÿ
00000040  1e f5 98 04 93 f7 a8 7e 09 9c c7 b6 0c bb f7 0b  . õ ⍰ . . ÷ ¨ ~ . ⍰ Ç ¶ . » ÷ .
00000050  a0 86 42 c7 ac 5d 02 fa 31 a4 5b 6c 5d db f0 55    . B Ç ¬ ] . ú 1 ¤ [ l ] Û ð U
00000060  b2 2e 77 94 af 58 07 7a 49 18 e5 43 56 37 58 6a  ² . w . ¯ X . z I . å C V 7 X j
00000070  4d 7e 8d 36 af f7 05 24 37 ff b2 96 56 b7 b7 b9  M ~ ⍰ 6 ¯ ÷ . $ 7 ÿ ² ⍰ V · · ¹
00000080  07 9d 0b ac f1 ea 59 9a 6c 95 31 34 fd c7 5e 2c  . ⍰ . ¬ ñ ê Y . l ⍰ 1 4 ý Ç ^ ,
00000090  9b 76 8c f6 9a a2 0b 61 4f 37 b3 ee fa 5f 17 2a  . v . ö . ¢ . a O 7 ³ î ú _ . *
000000a0  3b 6f 0d 22 11 94 e3 da 0c b2 60 a6 c8 c5 c6 67  ; o . " . . ã Ú . ² ` ¦ È Å Æ g
000000b0  bb 60 2c 53 7d cb a6 c0 0d 13 b0 42 22 3f 5d a5  » ` , S } Ë ¦ À . . ° B " ? ] ¥
000000c0  46 47 8d 89 1d 48 98 0f 59 35 dd 80 94 38 08 fd  F G ⍰ . . H ⍰ . Y 5 Ý . . 8 . ý
000000d0  9f 49 62 68 7b 60 d3 d4 8e 95 de 07 2f d8 bd 99  . I b h { ` Ó Ô . ⍰ Þ . / Ø ½ .
000000e0  20 16 fb 6b ef b4 91 a1 6d 85 55 36 b3 af ff d5    . û k ï ´ ⍰ ¡ m ⍰ U 6 ³ ¯ ÿ Õ
000000f0  f1 9b e3 77 1b 6b bd fa f2 04 19 ca f9 48 3d 4b  ñ . ã w . k ½ ú ò . . Ê ù H = K
00000100  7d bc 1e f5 03 f1 96 f2 ee 10 e6 14 0c d2 71 73  } ¼ . õ . ñ ⍰ ò î . æ . . Ò q s
00000110  29 41 07 f3 c8 24 8b 3b 61 ca 4f a6 28 a8 25 84  ) A . ó È $ ⍰ ; a Ê O ¦ ( ¨ % .
00000120  b8 69 13 04 38 62 34 3c 73 86 34 c3 f2 76 71 c2  ¸ i . . 8 b 4 < s . 4 Ã ò v q Â
00000130  21 a1 43 6b 72 be bd 8a 4b 33 87 59 6f eb b4 89  ! ¡ C k r ¾ ½ . K 3 . Y o ë ´ .
00000140  c0 e2 70 85 58 48 a0 27 ee 7f 9f b6 c1 b7 60 1d  À â p ⍰ X H   ' î   . ¶ Á · ` .
00000150  27 89 cc 1c d6 4b a2 09 d9 0f 2a db 5f 79 ca ec  ' . Ì . Ö K ¢ . Ù . * Û _ y Ê ì
00000160  59 16 18 62 f9 1e b5 32 f1 68 08 09 7a c3 b1 58  Y . . b ù . µ 2 ñ h . . z Ã ± X
00000170  70 7a 7d b8 b2 34 63 54                          p z } ¸ ² 4 c T
```

Again after removing the last character, the entire last block ended up changing.

- **Change one character in the key. How much of the encoded message changes?**



Input type: Text

Input text: (plain)

```
They rushed out the door, grabbing anything and everything they could think of
they might need. There was no time to double-check to make sure they weren't
leaving something important behind. Everything was thrown into the car and they
sped off. Thirty minutes later they were safe and that was when it dawned on them
that they had forgotten the most important thing of all.
```

● Plaintext ○ Hex Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvp

● Plaintext ○ Hex

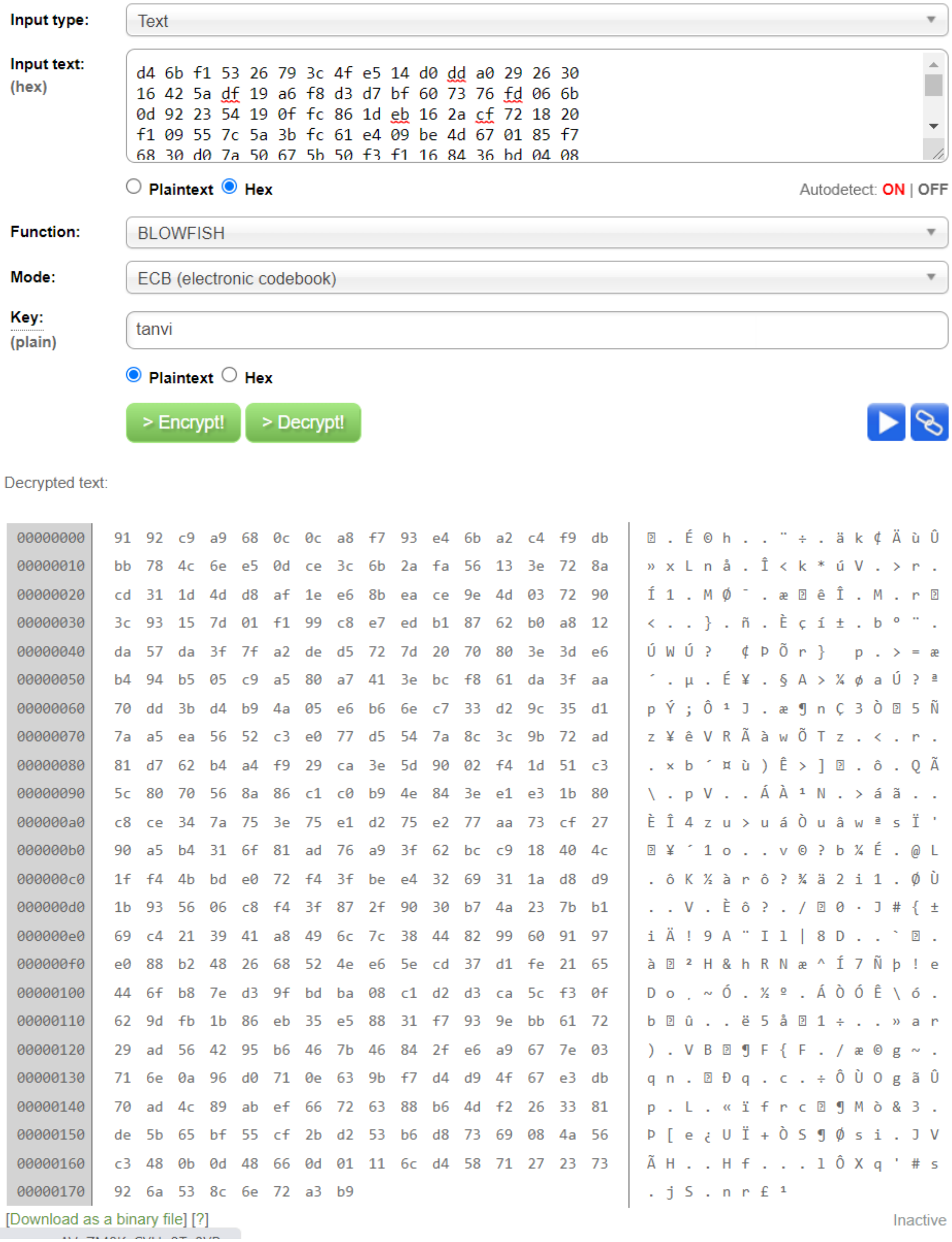
Encrypted text:

```
00000000  d4 6b f1 53 26 79 3c 4f e5 14 d0 dd a0 29 26 30  Ô k ñ S & y < O å . Ð Ý   ) & 0
00000010  16 42 5a df 19 a6 f8 d3 d7 bf 60 73 76 fd 06 6b  . B Z ß . ¦ ø Ó × ¿ ` s v ý . k
00000020  0d 92 23 54 19 0f fc 86 1d eb 16 2a cf 72 18 20  . . # T . . ü . . ë . * Ï r .
00000030  f1 09 55 7c 5a 3b fc 61 e4 09 be 4d 67 01 85 f7  ñ . U | Z ; ü a ä . ¾ M g . ⍰ ÷
00000040  68 30 d0 7a 50 67 5b 50 f3 f1 16 84 36 bd 04 08  h 0 Ð z P g [ P ó ñ . . 6 ½ . .
00000050  26 a4 42 39 e5 eb 8a 83 b0 b7 c6 b9 50 7a 0f 67  & ¤ B 9 å ë . . ° · Æ ¹ P z . g
00000060  cd 17 08 c2 69 1e 2b 7f 38 ce 6e 6e 68 6b 95 d5  Í . . Â i . +   8 Î n n h k ⍰ Õ
00000070  1d 22 55 4c 4f 0d 7b 0c f2 c8 4c bc af cf 84 15  . " U L O . { . ò È L ¼ ¯ Ï . .
00000080  92 21 40 e6 33 96 57 f3 e7 86 5d f5 c1 77 c9 0b  . ! @ æ 3 ⍰ W ó ç . ] õ Á w É .
00000090  e0 2d f1 c3 08 03 76 62 76 43 63 3e 90 1f 74 35  à - ñ Ã . . v b v C c > ⍰ . t 5
000000a0  4e cf 5e b6 c6 47 f5 5f b1 c5 72 df a2 54 54 c2  N Ï ^ ¶ Æ G õ _ ± Å r ß ¢ T T Â
000000b0  b7 44 06 da 7d 9d c4 a3 cc e3 a1 85 7f 51 23 d2  · D . Ú } ⍰ Ä £ Ì ã ¡ ⍰   Q # Ò
000000c0  44 07 7c be 83 8e 88 c6 0a 86 5f 1e 0a c5 b6 d1  D . | ¾ . . ⍰ Æ . . _ . . Å ¶ Ñ
000000d0  24 6c 67 d6 48 bb a3 e3 2d 66 a8 37 50 a2 59 26  $ l g Ö H » £ ã - f ¨ 7 P ¢ Y &
000000e0  f5 86 7f 9f 1e 3e 6f 0b 01 df e3 fa d1 65 82 04  õ .     . . > o . . ß ã ú Ñ e . .
000000f0  7f cb 27 17 eb e3 61 42 1d 42 17 84 ed 0c e7 68    Ë ' . ë ã a B . B . . í . ç h
00000100  39 e2 43 56 40 90 29 0c c5 54 af f9 e0 55 8e 68  9 â C V @ ⍰ ) . Å T ¯ ù à U . h
00000110  03 c4 e6 e0 16 e0 f4 26 70 09 91 5b 2c 81 ff c0  . Ä æ à . à ô & p . ⍰ [ , . ÿ À
00000120  cf 0c 6a b6 e2 48 07 f5 bb 70 91 9f d2 bf 1d fc  Ï . j ¶ â H . õ » p ⍰ . Ò ¿ . ü
00000130  db e8 bb 93 e8 31 f5 0c 72 59 7e 65 31 3c fa 7d  Û è » . è 1 õ . r Y ~ e 1 < ú }
00000140  2f c6 8b 30 7f 06 6c f7 ba 50 0a d3 02 bf 13 a2  / Æ ⍰ 0   . l ÷ º P . Ó . ¿ . ¢
00000150  ee b5 d1 d2 db 79 fb f3 91 99 9f cd 8f 9e d9 41  î µ Ñ Ò Û y û ó ⍰ . . Í ⍰ . Ù A
00000160  ae d4 8a c7 39 1d b3 6a 0d 61 9f d3 a9 28 f8 5b  ® Ô . Ç 9 . ³ j . a . Ó © ( ø [
00000170  3c 97 59 af 19 ff e0 61                          < . Y ¯ . ÿ à a
```

[Download as a binary file] [?] Inactive

A minor change in the key HAS led to an entirely different encrypted text

- **Decrypt a message using a key with one character changed. Does it look anything like the original?**



Input type: Text

Input text: (hex)

```
d4 6b f1 53 26 79 3c 4f e5 14 d0 dd a0 29 26 30
16 42 5a df 19 a6 f8 d3 d7 bf 60 73 76 fd 06 6b
0d 92 23 54 19 0f fc 86 1d eb 16 2a cf 72 18 20
f1 09 55 7c 5a 3b fc 61 e4 09 be 4d 67 01 85 f7
68 30 d0 7a 50 67 5b 50 f3 f1 16 84 36 bd 04 08
```

○ Plaintext ● Hex

Autodetect: ON | OFF

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvi

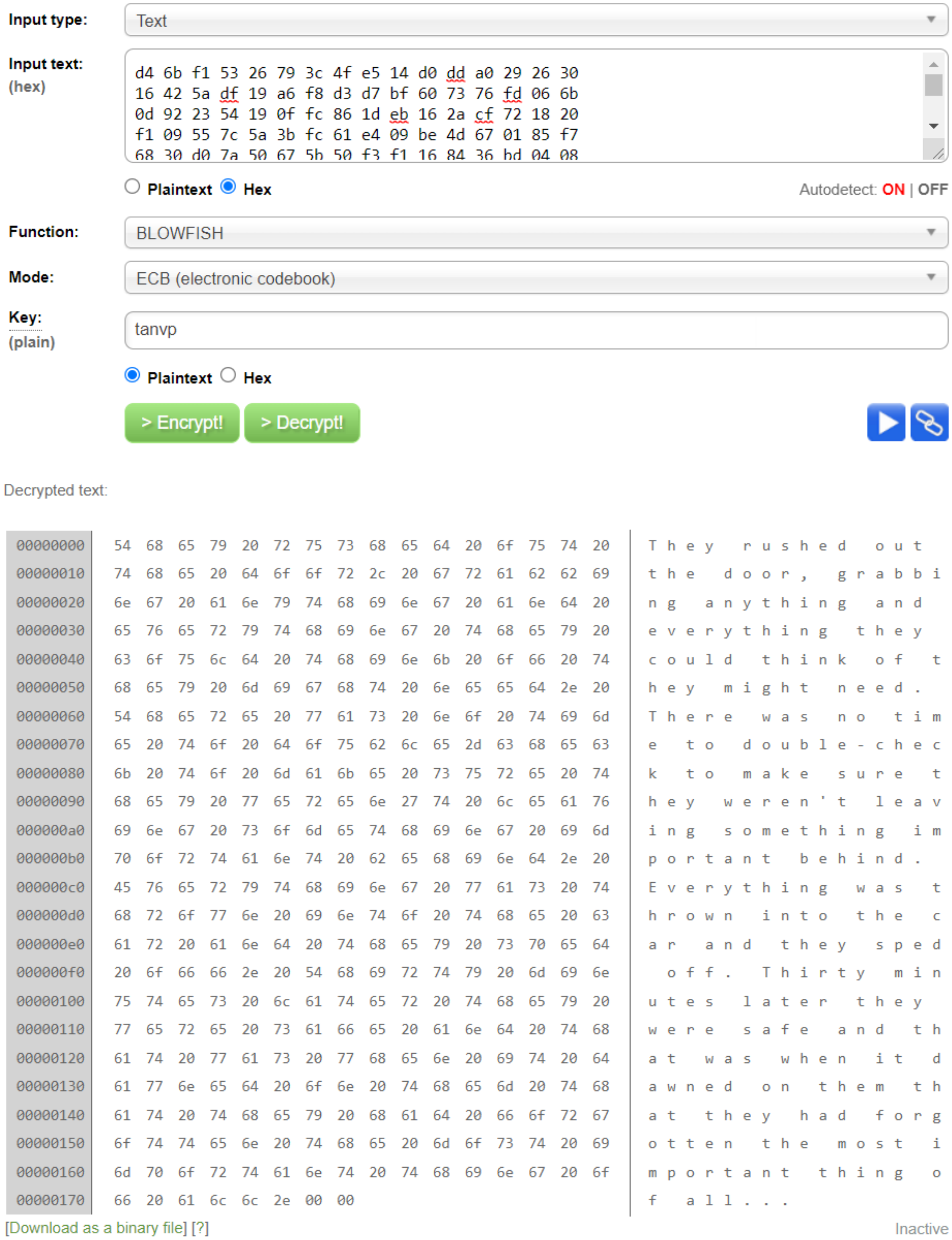
● Plaintext ○ Hex

Decrypted text:

```
00000000  91 92 c9 a9 68 0c 0c a8 f7 93 e4 6b a2 c4 f9 db  ⍰ . É © h . . ¨ ÷ . ä k ¢ Ä ù Û
00000010  bb 78 4c 6e e5 0d ce 3c 6b 2a fa 56 13 3e 72 8a  » x L n å . Î < k * ú V . > r .
00000020  cd 31 1d 4d d8 af 1e e6 8b ea ce 9e 4d 03 72 90  Í 1 . M Ø ¯ . æ ⍰ ê Î . M . r ⍰
00000030  3c 93 15 7d 01 f1 99 c8 e7 ed b1 87 62 b0 a8 12  < . . } . ñ . È ç í ± . b ° ¨ .
00000040  da 57 da 3f 7f a2 de d5 72 7d 20 70 80 3e 3d e6  Ú W Ú ?   ¢ Þ Õ r }   p . > = æ
00000050  b4 94 b5 05 c9 a5 80 a7 41 3e bc f8 61 da 3f aa  ´ . µ . É ¥ . § A > ¼ ø a Ú ? ª
00000060  70 dd 3b d4 b9 4a 05 e6 b6 6e c7 33 d2 9c 35 d1  p Ý ; Ô ¹ J . æ ¶ n Ç 3 Ò ⍰ 5 Ñ
00000070  7a a5 ea 56 52 c3 e0 77 d5 54 7a 8c 3c 9b 72 ad  z ¥ ê V R Ã à w Õ T z . < . r .
00000080  81 d7 62 b4 a4 f9 29 ca 3e 5d 90 02 f4 1d 51 c3  . × b ´ ¤ ù ) Ê > ] ⍰ . ô . Q Ã
00000090  5c 80 70 56 8a 86 c1 c0 b9 4e 84 3e e1 e3 1b 80  \ . p V . . Á À ¹ N . > á ã . .
000000a0  c8 ce 34 7a 75 3e 75 e1 d2 75 e2 77 aa 73 cf 27  È Î 4 z u > u á Ò u â w ª s Ï '
000000b0  90 a5 b4 31 6f 81 ad 76 a9 3f 62 bc c9 18 40 4c  ⍰ ¥ ´ 1 o . . v © ? b ¼ É . @ L
000000c0  1f f4 4b bd e0 72 f4 3f be e4 32 69 31 1a d8 d9  . ô K ½ à r ô ? ¾ ä 2 i 1 . Ø Ù
000000d0  1b 93 56 06 c8 f4 3f 87 2f 90 30 b7 4a 23 7b b1  . . V . È ô ? . / ⍰ 0 · J # { ±
000000e0  69 c4 21 39 41 a8 49 6c 7c 38 44 82 99 60 91 97  i Ä ! 9 A ¨ I l | 8 D . . ` ⍰ .
000000f0  e0 88 b2 48 26 68 52 4e e6 5e cd 37 d1 fe 21 65  à ⍰ ² H & h R N æ ^ Í 7 Ñ þ ! e
00000100  44 6f b8 7e d3 9f bd ba 08 c1 d2 d3 ca 5c f3 0f  D o ¸ ~ Ó . ½ º . Á Ò Ó Ê \ ó .
00000110  62 9d fb 1b 86 eb 35 e5 88 31 f7 93 9e bb 61 72  b ⍰ û . . ë 5 å ⍰ 1 ÷ . . » a r
00000120  29 ad 56 42 95 b6 46 7b 46 84 2f e6 a9 67 7e 03  ) . V B ⍰ ¶ F { F . / æ © g ~ .
00000130  71 6e 0a 96 d0 71 0e 63 9b f7 d4 d9 4f 67 e3 db  q n . ⍰ Ð q . c . ÷ Ô Ù O g ã Û
00000140  70 ad 4c 89 ab ef 66 72 63 88 b6 4d f2 26 33 81  p . L . « ï f r c ⍰ ¶ M ò & 3 .
00000150  de 5b 65 bf 55 cf 2b d2 53 b6 d8 73 69 08 4a 56  Þ [ e ¿ U Ï + Ò S ¶ Ø s i . J V
00000160  c3 48 0b 0d 48 66 0d 01 11 6c d4 58 71 27 23 73  Ã H . . H f . . . l Ô X q ' # s
00000170  92 6a 53 8c 6e 72 a3 b9                          . j S . n r £ ¹
```

[Download as a binary file] [?]

Inactive



Input type: Text

Input text: (hex)

```
d4 6b f1 53 26 79 3c 4f e5 14 d0 dd a0 29 26 30
16 42 5a df 19 a6 f8 d3 d7 bf 60 73 76 fd 06 6b
0d 92 23 54 19 0f fc 86 1d eb 16 2a cf 72 18 20
f1 09 55 7c 5a 3b fc 61 e4 09 be 4d 67 01 85 f7
68 30 d0 7a 50 67 5b 50 f3 f1 16 84 36 bd 04 08
```

○ Plaintext ● Hex

Function: BLOWFISH

Mode: ECB (electronic codebook)

Key: (plain) tanvp

● Plaintext ○ Hex

Decrypted text:

```
00000000  54 68 65 79 20 72 75 73 68 65 64 20 6f 75 74 20  They rushed out 
00000010  74 68 65 20 64 6f 6f 72 2c 20 67 72 61 62 62 69  the door, grabbi
00000020  6e 67 20 61 6e 79 74 68 69 6e 67 20 61 6e 64 20  ng anything and 
00000030  65 76 65 72 79 74 68 69 6e 67 20 74 68 65 79 20  everything they 
00000040  63 6f 75 6c 64 20 74 68 69 6e 6b 20 6f 66 20 74  could think of t
00000050  68 65 79 20 6d 69 67 68 74 20 6e 65 65 64 2e 20  hey might need. 
00000060  54 68 65 72 65 20 77 61 73 20 6e 6f 20 74 69 6d  There was no tim
00000070  65 20 74 6f 20 64 6f 75 62 6c 65 2d 63 68 65 63  e to double-chec
00000080  6b 20 74 6f 20 6d 61 6b 65 20 73 75 72 65 20 74  k to make sure t
00000090  68 65 79 20 77 65 72 65 6e 27 74 20 6c 65 61 76  hey weren't leav
000000a0  69 6e 67 20 73 6f 6d 65 74 68 69 6e 67 20 69 6d  ing something im
000000b0  70 6f 72 74 61 6e 74 20 62 65 68 69 6e 64 2e 20  portant behind. 
000000c0  45 76 65 72 79 74 68 69 6e 67 20 77 61 73 20 74  Everything was t
000000d0  68 72 6f 77 6e 20 69 6e 74 6f 20 74 68 65 20 63  hrown into the c
000000e0  61 72 20 61 6e 64 20 74 68 65 79 20 73 70 65 64  ar and they sped
000000f0  20 6f 66 66 2e 20 54 68 69 72 74 79 20 6d 69 6e   off. Thirty min
00000100  75 74 65 73 20 6c 61 74 65 72 20 74 68 65 79 20  utes later they 
00000110  77 65 72 65 20 73 61 66 65 20 61 6e 64 20 74 68  were safe and th
00000120  61 74 20 77 61 73 20 77 68 65 6e 20 69 74 20 64  at was when it d
00000130  61 77 6e 65 64 20 6f 6e 20 74 68 65 6d 20 74 68  awned on them th
00000140  61 74 20 74 68 65 79 20 68 61 64 20 66 6f 72 67  at they had forg
00000150  6f 74 74 65 6e 20 74 68 65 20 6d 6f 73 74 20 69  otten the most i
00000160  6d 70 6f 72 74 61 6e 74 20 74 68 69 6e 67 20 6f  mportant thing o
00000170  66 20 61 6c 6c 2e 00 00                          f all...
```

Decrypting a message with a changed key leads to a different message altogether. There is absolutely no similarity between the actual plain text and the message obtained in the latter case.

CONCLUSION:

We can conclude that Blowfish is a block cipher as any changes made to the text affected the whole block and even after deleting a character the length of cipher text did not change.

We can also say the blowfish is symmetric cipher as encryption and decryption can be done using the same key.

Also if there is minor change in the key the encrypted or decrypted message is changed completely.

Github: **https://github.com/tanvipen/CSS-Lab/tree/main/Exp5**