



Universidad Nacional Autónoma de México

Facultad de Ciencias

CRIPTOGRAFÍA Y SEGURIDAD

Tarea 6: DES - Segunda Parte

FECHA DE ENTREGA: 06/11/2023

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Marco Antonio Rivera Silva - 318183583



1. Código

El código se encuentra en la siguiente liga a *colab*, en el mismo se pueden ver comentarios que indican cómo fue ejecutado el código. Además de que *colab* guarda un historial.

<https://colab.research.google.com/drive/1MltnByhjLbq1Mmd-oC4QgKUkgadpimJC?usp=sharing>

Veámos cómo se comporta el cifrado con las distintas llaves:

- **Llaves débiles.**

Tomamos las 3 primeras llaves débiles y vemos que resultado nos arroja.

```

█ texto plano: 02468ACEECA86420
texto plano binario: 0000010010001101000101011001110110110010101000011001000010000
llave: 0101010101010101
llave en binario: 000000100000001000000010000000100000001000000010000000100000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 59567161 000000000000
Round 2 59567161 AA0F2981 000000000000
Round 3 AA0F2981 94114E02 000000000000
Round 4 94114E02 C2D713A9 000000000000
Round 5 C2D713A9 041054FB 000000000000
Round 6 041054FB 9307B579 000000000000
Round 7 9307B579 FACD91DB 000000000000
Round 8 FACD91DB FAE4D809 000000000000
Round 9 FAE4D809 993D69E7 000000000000
Round 10 993D69E7 F82CFAAA 000000000000
Round 11 F82CFAAA 1BAB0957 000000000000
Round 12 1BAB0957 4BA74F36 000000000000
Round 13 4BA74F36 6151AB32 000000000000
Round 14 6151AB32 CD761C59 000000000000
Round 15 CD761C59 CA919993 000000000000
Round 16 7A8143B0 CA919993 000000000000
Cipher Text :
    Hexadecimal: 3ec600c86b41c4b Binario: 001111011000110000000011001000011010110100001110001001011011
Presentation

```

Figura 1: Cifrado con llave 1



```

Cipher Text :
    Hexadecimal: 3ec600c86b41c4bb Binario: 001111101100011000000000110010000110101101000001110001001011101

Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 59567161 000000000000
Round 2 59567161 AA0F2981 000000000000
Round 3 AA0F2981 94114E02 000000000000
Round 4 94114E02 C2D713A9 000000000000
Round 5 C2D713A9 041054F8 000000000000
Round 6 041054F8 9307B579 000000000000
Round 7 9307B579 FACD91D8 000000000000
Round 8 FACD91D8 FAE4D809 000000000000
Round 9 FAE4D809 993D69E7 000000000000
Round 10 993D69E7 F82CFAAA 000000000000
Round 11 F82CFAAA 1BAB0957 000000000000
Round 12 1BAB0957 4BA74F36 000000000000
Round 13 4BA74F36 6151AB32 000000000000
Round 14 6151AB32 CD761C59 000000000000
Round 15 CD761C59 CA919993 000000000000
Round 16 7A814380 CA919993 000000000000
Plain Text : 3EC600C86B41C4BB

```

Figura 2: Descifrado con llave 1

Figura 3: Cifrado con llave 2



```

Cipher Text :
    Hexadecimal: 089ae4220dd84d7e Binario: 000010001001101011100100001000100000110111011000010011010111110
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 9E2DED2 FFFFFFFFFFFF
Round 2 9E2DED2 1EA84F1A FFFFFFFFFFFF
Round 3 1EA84F1A BA39139C FFFFFFFFFF
Round 4 BA39139C 4B09CF31 FFFFFFFFFF
Round 5 4B09CF31 52F9CE94 FFFFFFFFFF
Round 6 52F9CE94 F72AC07A FFFFFFFFFF
Round 7 F72AC07A EA36606F FFFFFFFFFF
Round 8 EA36606F 00743DC7 FFFFFFFFFF
Round 9 00743DC7 F0893C8F FFFFFFFFFF
Round 10 F0893C8F F14A01AE FFFFFFFFFF
Round 11 F14A01AE 0C22D609 FFFFFFFFFF
Round 12 0C22D609 FC0FE7A FFFFFFFFFF
Round 13 FC0FE7A 69433ED5 FFFFFFFFFF
Round 14 69433ED5 DF9804D9 FFFFFFFFFF
Round 15 DF9804D9 268CF38A FFFFFFFFFF
Round 16 EA42D450 268CF38A FFFFFFFFFF
Plain Text : 089AE4220DD84D7E

```

Figura 4: Descifrado con llave 2

```

☒ texto plano: 02468ACEECA86420
texto plano binario: 00000100100011010001010110011101100100101010000110010000100000
llave: 1F1F1F1F0E0E0E0E
llave en binario: 00011110001111000111110001111100001110000011100000111000001110

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 5A665DC0 00000FFFFF
Round 2 5A665DC0 A3CF335B 000000FFFFF
Round 3 A3CF335B BCA40C37 000000FFFFF
Round 4 BCA40C37 BA58B4D2 000000FFFFF
Round 5 BA58B4D2 1E3D0E6C 000000FFFFF
Round 6 1E3D0E6C DDA1BF1 000000FFFFF
Round 7 DDA1BF1 042C6F19 000000FFFFF
Round 8 042C6F19 3CF89789 000000FFFFF
Round 9 3CF89789 BA3C6D08 000000FFFFF
Round 10 8A3C6D08 C058A881 000000FFFFF
Round 11 C058A881 608802A8 000000FFFFF
Round 12 608802A8 73D1442B 000000FFFFF
Round 13 73D1442B 6E787106 000000FFFFF
Round 14 6E787106 FB25B1D0 000000FFFFF
Round 15 FB25B1D0 A6BDC55C 000000FFFFF
Round 16 786802F8 A6BDC55C 000000FFFFF
Cipher Text :
    Hexadecimal: 2884aa7363f15ba9 Binario: 00101000100001001010101001110011000111110001010110110101001

```

Figura 5: Cifrado con llave 3



```

Cipher Text :
    Hexadecimal: 2884aa7363f15ba9 Binario: 00101000100001001010100111001101100011111100010101101110101001
Decryption
After initial permutation 5A005A003CF03C0F
Round  Parte Izquierda Parte derecha Llave k
Round 1  3CF03C0F  5A665DC0  000000FFFF
Round 2  5A665DC0  A3CF335B  000000FFFF
Round 3  A3CF335B  BCA40C37  000000FFFF
Round 4  BCA40C37  BA5884D2  000000FFFF
Round 5  BA5884D2  1E3D0E6C  000000FFFF
Round 6  1E3D0E6C  D0AA1BF1  000000FFFF
Round 7  D0AA1BF1  042C6F19  000000FFFF
Round 8  042C6F19  3CF89789  000000FFFF
Round 9  3CF89789  8A3C6D08  000000FFFF
Round 10 8A3C6D08  C95BA881  000000FFFF
Round 11 C95BA881  608802AB  000000FFFF
Round 12 608802AB  73D1442B  000000FFFF
Round 13 73D1442B  6E787106  000000FFFF
Round 14 6E787106  FB25B1DD  000000FFFF
Round 15 FB25B1DD  A6BDC55C  000000FFFF
Round 16 786802F8  A6BDC55C  000000FFFF
Plain Text : 2884AA7363F15BA9

```

Figura 6: Descifrado con llave 3

Podemos ver que tanto para cifrar como descifrar con la misma llave los resultados son idénticos, esto se debe a que las llaves son involutivas, es decir, son su propia inversa. La razón principal por la que se considera débil es que, debido a la estructura del algoritmo DES, generan un patrón de cifrado y descifrado lo cual facilita ciertos tipos de ataques como fuerza bruta.

En términos matemáticos se expresa como

$$E_k(E_k(P)) = P$$

donde E_k es el cifrado con la llave k y P es el texto plano. O bien

$$E_k = D_k$$

donde D_k es el texto descifrado con la llave k . Es decir, cifrar y descifrar con la misma llave es exactamente lo mismo.

■ Llaves Semidébiles.

Con la llaves semidébiles pasa algo “*curioso*”, dados dos pares de llaves el cifrado de una llave es el descifrado de la otra llave y viceversa.



```

█ texto plano: 02468ACECA86420
texto plano binario: 0000001001000110100010101001110110100101010000110010000100000
llave: 01FE01FE01FE01FE
llave en binario: 00000001111111100000000111111110000000111111110000000111111110

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F DBE8B0DF 9153E54319BD
Round 2 D8E8B0DF EF9BE8EA 6EAC1ABCE642
Round 3 EF9BE8EA 27FECB9 6EAC1ABCE642
Round 4 27FECB9 15646CA5 6EAC1ABCE642
Round 5 15646CA5 7505AE35 6EAC1ABCE642
Round 6 7505AE35 497C12BF 6EAC1ABCE642
Round 7 497C12BF 73D0569C 6EAC1ABCE642
Round 8 73D0569C 4997BA7F 6EAC1ABCE642
Round 9 4997BA7F 1913CE22 9153E54319BD
Round 10 1913CE22 F9A5C137 9153E54319BD
Round 11 F9A5C137 C42A16E8 9153E54319BD
Round 12 C42A16E8 15AB2559 9153E54319BD
Round 13 15AB2559 872647D0 9153E54319BD
Round 14 872647D0 38476C32 9153E54319BD
Round 15 38476C32 71AAE6DE 9153E54319BD
Round 16 C3AB88AB 71AAE6DE 6EAC1ABCE642
Cipher Text :
Hexadecimal: d17b0a3782b9ca7f Binario: 1101000101111011000010100011011110000010101110011100101001111111

```

Figura 7: Cifrado con llave 5

```

Cipher Text :
Hexadecimal: d17b0a3782b9ca7f Binario: 1101000101111011000010100011011110000010101110011100101001111111
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 4170DAA2 6EAC1ABCE642
Round 2 4170DAA2 4A8E22CE 9153E54319BD
Round 3 4A8E22CE 216A8879 9153E54319BD
Round 4 216A8879 9B53B022 9153E54319BD
Round 5 9B53B022 8CD10991 9153E54319BD
Round 6 8CD10991 7EC06C02 9153E54319BD
Round 7 7EC06C02 DF4A3996 9153E54319BD
Round 8 DF4A3996 B14A8D01 9153E54319BD
Round 9 B14A8D01 8C001C0D 6EAC1ABCE642
Round 10 0C001C0D 02B39771 6EAC1ABCE642
Round 11 02B39771 5B5F312C 6EAC1ABCE642
Round 12 5B5F312C 94B7D42E 6EAC1ABCE642
Round 13 94B7D42E FEC1C6B4 6EAC1ABCE642
Round 14 FEC1C6B4 4D1D71A5 6EAC1ABCE642
Round 15 4D1D71A5 EF27234D 6EAC1ABCE642
Round 16 88B95CAE EF27234D 9153E54319BD
Plain Text : BAA9A7D7148986D1

```

Figura 8: Descifrado con llave 5



```

☒ texto plano: 02468ACECA86420
texto plano binario: 000000100100011010001010110011101100101010000110010000100000
llave: FE01FE01FE01FE01
llave en binario: 111111100000001111111100000001111111100000001111111100000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 4170DA02 6EAC1ABCE642
Round 2 4170DA02 4A8E22CE 9153E54319BD
Round 3 4A8E22CE 216A8B79 9153E54319BD
Round 4 216A8B79 9B53B022 9153E54319BD
Round 5 9B53B022 8CD11091 9153E54319BD
Round 6 8CD11091 7EC06C02 9153E54319BD
Round 7 7EC06C02 DF4A3996 9153E54319BD
Round 8 DF4A3996 B14A8D01 9153E54319BD
Round 9 B14A8D01 0C0D1C0D 6EAC1ABCE642
Round 10 0C0D1C0D 02B39771 6EAC1ABCE642
Round 11 02B39771 5B5F312C 6EAC1ABCE642
Round 12 5B5F312C 94B7D42E 6EAC1ABCE642
Round 13 94B7D42E FEC1C6B4 6EAC1ABCE642
Round 14 FEC1C6B4 4D1D71A5 6EAC1ABCE642
Round 15 4D1D71A5 EF27234D 6EAC1ABCE642
Round 16 88B95CAE EF27234D 9153E54319BD
Cipher Text :
Hexadecimal: baa9a7d714b986d1 Binario: 1011101010101001101001111101011100010100101110011000011011010001

```

Figura 9: Cifrado con llave 11

```

Cipher Text :
Hexadecimal: baa9a7d714b986d1 Binario: 1011101010101001101001111101011100010100101110011000011011010001
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F DBE8B00F 9153E54319BD
Round 2 DBE8B00F EF9B8E8A 6EAC1ABCE642
Round 3 EF9B8E8A 27EFE89 6EAC1ABCE642
Round 4 27EFE89 15646CA5 6EAC1ABCE642
Round 5 15646CA5 7505AE35 6EAC1ABCE642
Round 6 7505AE35 497C12BF 6EAC1ABCE642
Round 7 497C12BF 73DD569C 6EAC1ABCE642
Round 8 73DD569C 4997BA7F 6EAC1ABCE642
Round 9 4997BA7F 1913CE22 9153E54319BD
Round 10 1913CE22 F9A5C137 9153E54319BD
Round 11 F9A5C137 C42A16E8 9153E54319BD
Round 12 C42A16E8 15AB2559 9153E54319BD
Round 13 15AB2559 872647DE 9153E54319BD
Round 14 872647DE 38476C32 9153E54319BD
Round 15 38476C32 71AAE6DE 9153E54319BD
Round 16 C3AB88AB 71AAE6DE 6EAC1ABCE642
Plain Text : D17B0A3782B9CA7F

```

Figura 10: Descifrado con llave 11

Notemos que el resultado del cifrado con la llave 5 es el mismo que el descifrado de la llave 11.

Y el descifrado con la llave 5 es el mismo que el cifrado con la llave 11.

Para poner a prueba las demás llaves tuvimos algunos problemas ya que esta propiedad solo funcionaba con el primer par de llaves semidébiles del archivo *llavesdebiles.txt* proporcionado.

Investigando más a fondo pudimos encontrar pares de llaves que sí cumplían con la propiedad anteriormente mencionada. Estas llaves las pusimos en el colab enumeradas del 90 al 98. La



propiedad en términos matemáticos se describe como

$$E_{K_1}(E_{K_2}(P)) = P$$

o bien

$$E_{K_2} = D_{K_1}$$

```

█ texto plano: 02468ACECA86420
texto plano binario: 000000100100011010001010110011101101100101010000110010000100000
llave: 1FE01F00EF10EF1
llave en binario: 00011111110000000111111110000000011101110001000011101110001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F C1F898F6 9153E5BCE642
Round 2 C1F898F6 C572FF81 6EAC1AA319BD
Round 3 C572FF81 FB280D86 6EAC1AA319BD
Round 4 FB280D86 FB852B93 6EAC1AA319BD
Round 5 FB852B93 39E1FEFB 6EAC1AA319BD
Round 6 39E1FEFB 1E82A68C 6EAC1AA319BD
Round 7 1E82A68C E7DE5B98 6EAC1AA319BD
Round 8 E7DE5B98 65B90E84 6EAC1AA319BD
Round 9 65B90E84 AB41E37A 9153E5BCE642
Round 10 AB41E37A 75B1E97 9153E5BCE642
Round 11 75B1E97 458F004D 9153E5BCE642
Round 12 458F004D 8378F0B1 9153E5BCE642
Round 13 8378F0B1 51A8878C 9153E5BCE642
Round 14 51A8878C 7388F326 9153E5BCE642
Round 15 7388F326 D7C50908 9153E5BCE642
Round 16 F98FD792 D7C50908 6EAC1AA319BD
Cipher Text :
    Hexadecimal: fc95b45ad550e4f5 Binario: 11111100100101011011010001011010101010100001110010011110101

```

Figura 11: Cifrado con llave 90

```

Cipher Text :
    Hexadecimal: fc95b45ad550e4f5 Binario: 1111110010010101101101000101101010101010100001110010011110101
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 5B60F28B 6EAC1AA319BD
Round 2 5B60F28B BEE11C0 9153E5BCE642
Round 3 BEE11C0 07DBCD61 9153E5BCE642
Round 4 07DBCD61 970AB966 9153E5BCE642
Round 5 970AB966 97BF3F93 9153E5BCE642
Round 6 97BF3F93 EBF05986 9153E5BCE642
Round 7 EBF05986 013B7CF7 9153E5BCE642
Round 8 013B7CF7 2107EC2C 9153E5BCE642
Round 9 2107EC2C 5FF15856 6EAC1AA319BD
Round 10 5FF15856 BF32BA0E 6EAC1AA319BD
Round 11 BF32BA0E 1A364239 6EAC1AA319BD
Round 12 1A364239 DE6F806C 6EAC1AA319BD
Round 13 DE6F806C B9FFEA0C4 6EAC1AA319BD
Round 14 B9FFEA0C4 9689BA72 6EAC1AA319BD
Round 15 9689BA72 DD2A7A7D 6EAC1AA319BD
Round 16 401E973E DD2A7A7D 9153E5BCE642
Plain Text : 863D97BB9F2BCA84

```

Figura 12: Descifrado con llave 90



```

→ texto plano: 02468ACEECA86420
texto plano binario: 0000001001000110100010101100111011001001010000110010000100000
llave: E01FE01FF10EF10E
llave en binario: 111000000001111111000000011111111000100011101111000100001110

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 5B60F2B8 6EAC1AA319BD
Round 2 5B60F2B8 BEEF11C0 9153E5BCE642
Round 3 BEEF11C0 07DBCD61 9153E5BCE642
Round 4 07DBCD61 970AB966 9153E5BCE642
Round 5 970AB966 97BF3F93 9153E5BCE642
Round 6 97BF3F93 EBF05986 9153E5BCE642
Round 7 EBF05986 013B7CF7 9153E5BCE642
Round 8 013B7CF7 2107EC2C 9153E5BCE642
Round 9 2107EC2C 5FF15856 6EAC1AA319BD
Round 10 5FF15856 BF32BA0E 6EAC1A4319BD
Round 11 BF32BA0E A364239 6EAC1A4319BD
Round 12 A364239 DE6F806C 6EAC1A4319BD
Round 13 DE6F806C B9FEAO4 6EAC1A4319BD
Round 14 B9FEAO4 9689BA72 6EAC1A4319BD
Round 15 9689BA72 DD2A7A7D 6EAC1A4319BD
Round 16 401E973E DD2A7A7D 9153E5BCE642
Cipher Text :
Hexadecimal: 863d97bb9f2bca84 Binario: 100001100011110110010111101110011111001010111100101010000100

```

Figura 13: Cifrado con llave 91

```

Cipher Text :
Hexadecimal: 863d97bb9f2bca84 Binario: 100001100011110110010111101110011111001010111100101010000100
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F C1F898F6 9153E5BCE642
Round 2 C1F898F6 C572FF81 6EAC1AA319BD
Round 3 C572FF81 F82800B6 6EAC1AA319BD
Round 4 FB2800B6 FBB52B93 6EAC1AA319BD
Round 5 FBB52B93 39E1FFEB 6EAC1AA319BD
Round 6 39E1FFEB 1E82A68C 6EAC1AA319BD
Round 7 1E82A68C E7DE5B98 6EAC1AA319BD
Round 8 E7DE5B98 65B90E84 6EAC1AA319BD
Round 9 65B90E84 A841E37A 9153E5BCE642
Round 10 A841E37A 75B1EE97 9153E5BCE642
Round 11 75B1EE97 458F004D 9153E5BCE642
Round 12 458F004D 837BF0B1 9153E5BCE642
Round 13 837BF0B1 51A8878C 9153E5BCE642
Round 14 51A8878C 7388F326 9153E5BCE642
Round 15 7388F326 D7C50908 9153E5BCE642
Round 16 F9BF0792 D7C50908 6EAC1A4319BD
Plain Text : FC95B45AD550E4F5

```

Figura 14: Descifrado con llave 91

El cifrado con la llave 90 es el mismo que el descifrado de la llave 91. Y el descifrado con la llave 90 es el mismo que el cifrado con la llave 91.



```

 texto plano: 02468ACECA86420
texto plano binario: 000001001000011010001010110011101101100101010000110010000100000
llave: 01E001E001F101F1
llave en binario: 00000011110000000000001111000000000000111110001000000111110001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F D9DEB077 9153E500000
Round 2 D9DEB077 47A5B4BE 6EAC1A000000
Round 3 47A5B4BE BCE20BDE 6EAC1A000000
Round 4 BCE20BDE D2439250 6EAC1A000000
Round 5 D2439250 89813B86 6EAC1A000000
Round 6 89813B86 72A53DBF 6EAC1A000000
Round 7 72A53DBF 639C3D15 6EAC1A000000
Round 8 639C3D15 6F708FB3 6EAC1A000000
Round 9 6F708FB3 1758AB74 9153E5000000
Round 10 1758AB74 46E5C35A 9153E5000000
Round 11 46E5C35A 8F669BA1 9153E5000000
Round 12 8F669BA1 1AD5F01C 9153E5000000
Round 13 1AD5F01C D2A1B04C 9153E5000000
Round 14 D2A1B04C 20C19108 9153E5000000
Round 15 20C19108 AB923540 9153E5000000
Round 16 50598919 AB923540 6EAC1A000000
Cipher Text :
Hexadecimal: 9da00895798852a4 Binario: 100111011010000000010001001010101111001100010000101001010100100

```

Figura 15: Cifrado con llave 92

```

Cipher Text :
Hexadecimal: 9da00895798852a4 Binario: 100111011010000000010001001010101111001100010000101001010100100
Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 5956F223 6EAC1A000000
Round 2 5956F223 09D15925 9153E5000000
Round 3 09D15925 92596D94 9153E5000000
Round 4 92596D94 5FE9AE6 9153E5000000
Round 5 5FE9AE6 9C2B07C6 9153E5000000
Round 6 9C2B07C6 EB4B2472 9153E5000000
Round 7 EB4B2472 A2B1A4F7 9153E5000000
Round 8 A2B1A4F7 60264F58 9153E5000000
Round 9 60264F58 320596E1 6EAC1A000000
Round 10 320596E1 5514F844 6EAC1A000000
Round 11 5514F844 74BAE158 6EAC1A000000
Round 12 74BAE158 54881894 6EAC1A000000
Round 13 54881894 49429BC9 6EAC1A000000
Round 14 49429BC9 D830F5D9 6EAC1A000000
Round 15 D830F5D9 E0032EE1 6EAC1A000000
Round 16 514608BF E0032EE1 9153E5000000
Plain Text : 6339190D418BD283

```

Figura 16: Descifrado con llave 92



Figura 17: Cifrado con llave 93

```

Cipher Text :
    Hexadecimal: 6339190d418bd283 Binario: 01100011001110010001100100001100101000011000101110100101000001

Decryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F D9DEB077 9153E5000000
Round 2 D9DEB077 47A584BE 6EAC1A000000
Round 3 47A584BE BCE20BDE 6EAC1A000000
Round 4 BCE20BDE D2439250 6EAC1A000000
Round 5 D2439250 89813B86 6EAC1A000000
Round 6 89813B86 72A53DBF 6EAC1A000000
Round 7 72A53DBF 639C3D15 6EAC1A000000
Round 8 639C3D15 6F78FB83 6EAC1A000000
Round 9 6F78FB83 1758AB74 9153E5000000
Round 10 1758AB74 46E5C35A 9153E5000000
Round 11 46E5C35A 8F6698AC 9153E5000000
Round 12 8F6698AC 14D5F01C 9153E5000000
Round 13 14D5F01C D2A1B04C 9153E5000000
Round 14 D2A1B04C 20C19108 9153E5000000
Round 15 20C19108 A8923540 9153E5000000
Round 16 50598919 A8923540 6EAC1A000000
Plain Text : 90A000895798852A4

```

Figura 18: Descifrado con llave 93

El cifrado con la llave 91 es el mismo que el descifrado de la llave 92. Y el descifrado con la llave 91 es el mismo que el cifrado con la llave 92.

■ Llaves Posiblemente Débiles.

El concepto de llaves posiblemente débiles no tiene una definición formal ni es muy reconocido en el ámbito de la criptografía. Son llaves que poseen ciertos patrones o propiedades pero que a pesar de ello no se ha demostrado que sean débiles o inseguras, es meramente especulación



que puede ser objeto de discusiones y evaluaciones en investigación criptográfica, sin embargo carece de evidencia sólida que las clasifique como seguras o inseguras.

```

texto plano: 02468ACECA86420
texto plano binario: 00000100100110100010101100111011001100101010000110010000100000
llave: 1F1F01010E0E0101
llave en binario: 000111110001111100000010000001000011100001110000000100000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 794051C1 0000002E82B8
Round 2 794051C1 B5AAA725 0000009264FA
Round 3 B5AAA725 0B399EDE 0000006D9B05
Round 4 0B399EDE A692D394 0000009264FA
Round 5 A692D394 04161D76 0000006D9B05
Round 6 04161D76 4C54652C 0000009264FA
Round 7 4C54652C 098EA7A2 0000006D9B05
Round 8 098EA7A2 751155ED 0000009264FA
Round 9 751155ED 327F99B5 000000017D47
Round 10 327F99B5 2FF52C38 0000002E82B8
Round 11 2FF52C38 942A7FEA 000000017D47
Round 12 942A7FEA 75492A71 0000002E82B8
Round 13 75492A71 ACCD59D4 000000017D47
Round 14 ACCD59D4 2DEC9F00 0000002E82B8
Round 15 2DEC9F00 16D1BB52 000000017D47
Round 16 9D9B0BD1 16D1BB52 0000006D9B05
Cipher Text :
    Hexadecimal: 7d9ec05cfb082379 Binario: 011111011001111011000000101110011111011000010000010001101111001
Decryption

```

Figura 19: Cifrado con llave 17

```

Cipher Text :
    Hexadecimal: 7d9ec05cfb082379 Binario: 011111011001111011000000101110011111011000010000010001101111001
Decryption
After initial permutation 9D9B0BD116D1B852
Round Parte Izquierda Parte derecha Llave k
Round 1 16D1BB52 2DEC9F00 0000006D9B05
Round 2 2DEC9F00 ACCD59D4 000000017D47
Round 3 ACCD59D4 75492A71 0000002E82B8
Round 4 75492A71 942A7FEA 000000017D47
Round 5 942A7FEA 2FF52C38 0000002E82B8
Round 6 2FF52C38 327F99B5 000000017D47
Round 7 327F99B5 751155ED 0000002E82B8
Round 8 751155ED 098EA7A2 000000017D47
Round 9 098EA7A2 4C54652C 0000009264FA
Round 10 4C54652C 04161D76 0000006D9B05
Round 11 04161D76 A692D394 0000009264FA
Round 12 A692D394 0B399EDE 0000006D9B05
Round 13 0B399EDE B5AAA725 0000009264FA
Round 14 B5AAA725 794051C1 0000006D9B05
Round 15 794051C1 3CF03C0F 0000009264FA
Round 16 5A005A00 3CF03C0F 0000002E82B8
Plain Text : 02468ACECA86420

```

Figura 20: Descifrado con llave 17



```

 texto plano: 02468ACECA86420
texto plano binario: 000000100100011010001010110011101101100101010000110010000100000
llave: E0E00101F1F10101
llave en binario: 1110000011100000000000100000011111000111110001000000100000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 1D166267 A2DC99000000
Round 2 1D166267 49D937DC CC7083000000
Round 3 49D937DC 6470AD91 338F7C000000
Round 4 6470AD91 93620BC9 CC7083000000
Round 5 93620BC9 B541B13C 338F7C000000
Round 6 B541B13C 27851204 CC7083000000
Round 7 27851204 BD28AFE9 338F7C000000
Round 8 BD28AFE9 54499E66 CC7083000000
Round 9 54499E66 400ED46A 5D2366000000
Round 10 400ED46A 522A0732 A2DC99000000
Round 11 522A0732 921FD60D 5D2366000000
Round 12 921FD60D 20936B89 A2DC99000000
Round 13 20936B89 0CFCC56 5D2366000000
Round 14 0CFCC56 39B9EA31 A2DC99000000
Round 15 39B9EA31 24012341 5D2366000000
Round 16 090B1A2E 24012341 338F7C000000
Cipher Text :
Hexadecimal: 7a1d815504890200 Binario: 011110100001110110000001010101010000010010001001000000100000000
Decryption

```

Figura 21: Cifrado con llave 21

```

Round 10 0CFCC56 5D2366000000
Cipher Text :
Hexadecimal: 7a1d815504890200 Binario: 011110100001110110000001010101010000010010001001000000100000000
Decryption
After initial permutation 090B1A2E24012341
Round Parte Izquierda Parte derecha Llave k
Round 1 24012341 39B9EA31 338F7C000000
Round 2 39B9EA31 0CFCC56 5D2366000000
Round 3 0CFCC56 20936B89 A2DC99000000
Round 4 20936B89 921FD60D 5D2366000000
Round 5 921FD60D 522A0732 A2DC99000000
Round 6 522A0732 400ED46A 5D2366000000
Round 7 400ED46A 54499E66 A2DC99000000
Round 8 54499E66 BD28AFE9 5D2366000000
Round 9 BD28AFE9 27851204 CC7083000000
Round 10 27851204 B541B13C 338F7C000000
Round 11 B541B13C 93620BC9 CC7083000000
Round 12 93620BC9 6470AD91 338F7C000000
Round 13 6470AD91 49D937DC CC7083000000
Round 14 49D937DC 1D166267 338F7C000000
Round 15 1D166267 3CF03C0F CC7083000000
Round 16 5A005A00 3CF03C0F A2DC99000000
Plain Text : 02468ACECA86420

```

Figura 22: Descifrado con llave 21



```

[+] texto plano: 02468ACECA86420
texto plano binario: 000001001000110100010101100111011101100101010000110010000100000
llave: 1FE001F0EF101FE
llave en binario: 000111111100000000001111111000001110111000100000011111110

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F D3CE9CF 9153E5609B05
Round 2 D3CE9CF 934CAE01 6EAC1A2E82B8
Round 3 934CAE01 AACF5D37 6EAC1AD17D47
Round 4 AACF5D37 8993D04F 6EAC1A2E82B8
Round 5 8993D04F A8ABF79E 6EAC1AD17D47
Round 6 A8ABF79E 85229D7E 6EAC1A2E82B8
Round 7 85229D7E 188CD857 6EAC1AD17D47
Round 8 188CD857 9818DF14 6EAC1A2E82B8
Round 9 9818DF14 6E2553BA 9153E59264FA
Round 10 6E2553BA D22713ED 9153E5609B05
Round 11 D22713ED 9E1E95B9 9153E59264FA
Round 12 9E1E95B9 1CF25C8A 9153E5609B05
Round 13 1CF25C8A 2D10C3EC 9153E59264FA
Round 14 2D10C3EC 650AE359 9153E5609B05
Round 15 650AE359 BD56B11C 9153E59264FA
Round 16 EFD3859B BD56B11C 6EAC1AD17D47
Cipher Text :
Hexadecimal: dd71e6c3bbc870dd Binario: 11011101011100011110011011000011101110010000111000011011101
Decryption

```

Figura 23: Cifrado con llave 51

```

Cipher Text :
Hexadecimal: dd71e6c3bbc870dd Binario: 11011101011100011110011011000011101110010000111000011011101
Decryption
After initial permutation EFD3859BB056B11C
Round Parte Izquierda Parte derecha Llave k
Round 1 BD56B11C 650AE359 6EAC1AD17D47
Round 2 650AE359 2D10C3EC 9153E59264FA
Round 3 2D10C3EC 1CF25C8A 9153E5609B05
Round 4 1CF25C8A 9E1E95B9 9153E59264FA
Round 5 9E1E95B9 D22713ED 9153E5609B05
Round 6 D22713ED 6E2553BA 9153E59264FA
Round 7 6E2553BA 9818DF14 9153E5609B05
Round 8 9818DF14 188CD857 9153E59264FA
Round 9 188CD857 85229D7E 6EAC1A2E82B8
Round 10 85229D7E A8ABF79E 6EAC1AD17D47
Round 11 A8ABF79E 8993D04F 6EAC1A2E82B8
Round 12 8993D04F AACF5D37 6EAC1AD17D47
Round 13 AACF5D37 934CAE01 6EAC1A2E82B8
Round 14 934CAE01 D3CE9CF 6EAC1AD17D47
Round 15 D3CE9CF 3CF03C0F 6EAC1A2E82B8
Round 16 5A005A00 3CF03C0F 9153E5609B05
Plain Text : 02468ACECA86420

```

Figura 24: Descifrado con llave 51

El cifrado no corresponde a algún otro cifrado o descifrado de otra llave posiblemente débil por lo cual no podemos afirmar o negar alguna relación entre llaves, sin embargo hemos de notar que generan 4 subllaves diferentes k_i . En realidad es la única observación que tenemos, no nos dice mucho a comparación de las llaves débiles o semidébiles que generaban solo una subllave k o 2 subllaves k_a, k_b respectivamente, pero ciertamente es un patrón particular.



2. Preguntas

- ¿Por qué es mala idea usarlas?

Existen varios motivos por los cuales es malo usar las llaves débiles que se nos proporcionó el archivo de texto. Las dos principales razones son:

- Tamaño de la llave:

En el archivo proporcionado de claves DES la longitud de la clave es de suma importancia ya que entre menor es la longitud de bits que tiene la clave, es más fácil realizar un ataque por diccionario o por fuerza bruta para obtenerla, tal como explica el artículo *Can you explain “weak keys” for DES?*.

Por lo general actualmente se recomienda siempre usar llaves con longitudes grandes (como 1024, 2048, etc.) pues la cantidad de operaciones que se deberían de hacer para obtenerlas crece de forma exponencial y por lo tanto haría inviable la opción de hacer un ataque de fuerza bruta.

- Combinación de caracteres en la llave

La combinación de caracteres (nuestro alfabeto) para la llave está íntimamente ligada a la longitud, pues no sirve tener una llave con una longitud considerable si la cantidad de caracteres empleados es baja, tal como podemos ver con la llave **0101010101010101** pues al tener una longitud de 16 bits las combinaciones que se pueden hacer son a lo máximo 2^{16} (ya que solo se usaron 2 caracteres) lo que es demasiado fácil para nuestras computadoras actuales.

Para crear una llave segura debemos de ocupar caracteres lo suficientemente variados (números, letras, caracteres especiales como arrobas, puntos, hashtags, etc.) y a su vez combinarla con una longitud considerable de caracteres para hacer inviables tanto el ataque



por diccionario como por fuerza bruta.

- ¿Por qué el diseño de DES hace que estas llaves no sean adecuadas?

Algo importante en el algoritmo de DES es que por cada permutación va generando llaves k_i para usarse en cada iteración. En el caso de las llaves débiles estas k_i son siempre las mismas.

```

E texto plano: 02468ACEECA86420
texto plano binario: 0000001001000110100010101100111011101100101010000110010000100000
llave: FEFEFEFEEFEEFEEFEE
llave en binario: 111111101111111011111110111111101111111011111110111111101111111011111110

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha llave k
Round 1 3CF03C0F 9E2EDED2 FFFFFFFFFFFF
Round 2 9E2EDED2 1EA84F1A FFFFFFFFFFFF
Round 3 1EA84F1A BA39139C FFFFFFFFFFFF
Round 4 BA39139C 4B09CF31 FFFFFFFFFFFF
Round 5 4B09CF31 52F9CE94 FFFFFFFFFFFF
Round 6 52F9CE94 F72AC07A FFFFFFFFFFFF
Round 7 F72AC07A EA36606F FFFFFFFFFFFF
Round 8 EA36606F 00743DC7 FFFFFFFFFFFF
Round 9 00743DC7 F0893C8F FFFFFFFFFFFF
Round 10 F0893C8F F14A01AE FFFFFFFFFFFF
Round 11 F14A01AE 0C22D609 FFFFFFFFFFFF
Round 12 0C22D609 FC0FE7AC FFFFFFFFFFFF
Round 13 FC0FE7AC 69433ED5 FFFFFFFFFFFF
Round 14 69433ED5 DF98D4D9 FFFFFFFFFFFF
Round 15 DF98D4D9 268CF38A FFFFFFFFFFFF
Round 16 E4A2D450 268CF38A FFFFFFFFFFFF
Cipher Text :
    Hexadecimal: 089ae4220dd84d7e Binario: 00001000100110101110010000100010000100000

```

Figura 25: llave 2, la cual es débil

Como podemos notar, al ejecutar la llave 2 del archivo solo se nos genera una k . En el caso de las llaves semidébiles generan 2 subllaves k_i distintas.



```
☒ texto plano: 02468ACEECA86420
texto plano binario: 0000001001000110100010101100111011101100101010000110010000100000
llave: FE01FE01FE01FE01
llave en binario: 1111111000000001111111000000001111111000000001111111000000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 4170DAA2 6EAC1ABCE642
Round 2 4170DAA2 4A8E22CE 9153E54319BD
Round 3 4A8E22CE 216A8B79 9153E54319BD
Round 4 216A8B79 9B53B022 9153E54319BD
Round 5 9B53B022 8CD11091 9153E54319BD
Round 6 8CD11091 7EC06C02 9153E54319BD
Round 7 7EC06C02 DF4A3996 9153E54319BD
Round 8 DF4A3996 B14A8DD1 9153E54319BD
Round 9 B14A8DD1 0C0D1C0D 6EAC1ABCE642
Round 10 0C0D1C0D 02B39771 6EAC1ABCE642
Round 11 02B39771 5B5F312C 6EAC1ABCE642
Round 12 5B5F312C 94B7D42E 6EAC1ABCE642
Round 13 94B7D42E FEC1C6B4 6EAC1ABCE642
Round 14 FEC1C6B4 4D1D71A5 6EAC1ABCE642
Round 15 4D1D71A5 EF27234D 6EAC1ABCE642
Round 16 88B95CAE EF27234D 9153E54319BD
Cipher Text :
    Hexadecimal: baa9a7d714b986d1 Binario: 101110101010100110100111110101110001010
```

Figura 26: llave 11, la cual es semidébil

Y de la misma manera al cifrar con las *llaves posiblemente débiles* vemos que nos genera solo 4 subllaves k distintas.



```
[→] texto plano: 02468ACEECA86420
texto plano binario: 000000100100011010001010110011101100101010000110010000100000
llave: E0E00101F1F10101
llave en binario: 11100000111000000000001000000011111000111110001000000100000001

Encryption
After initial permutation 5A005A003CF03C0F
Round Parte Izquierda Parte derecha Llave k
Round 1 3CF03C0F 1D166267 A2DC99000000
Round 2 1D166267 49D937DC CC7083000000
Round 3 49D937DC 647DAD91 338F7C000000
Round 4 647DAD91 93620BC9 CC7083000000
Round 5 93620BC9 B541B13C 338F7C000000
Round 6 B541B13C 278512D4 CC7083000000
Round 7 278512D4 BD28AFE9 338F7C000000
Round 8 BD28AFE9 54499E66 CC7083000000
Round 9 54499E66 400ED46A 5D2366000000
Round 10 400ED46A 522A0732 A2DC99000000
Round 11 522A0732 921FD6DD 5D2366000000
Round 12 921FD6DD 20936B89 A2DC99000000
Round 13 20936B89 0CFFCC56 5D2366000000
Round 14 0CFFCC56 39B9EA31 A2DC99000000
Round 15 39B9EA31 24012341 5D2366000000
Round 16 090B1A2E 24012341 338F7C000000

Cipher Text :
    Hexadecimal: 7a1d815504890200 Binario: 0111101000011101100000010101010101000001
```

Figura 27: llave 21, la cual es una llave probablemente débil

Por lo que este hecho que con una llave débil se generen menos subllaves k, si hace que los que conocen como funciona el algoritmo tengan mas pistas sobre como romper el algoritmo y de una forma mas rápida.

El diseño del algoritmo DES puede permitir que ciertas claves generen patrones predecibles o conduzcan a ciclos cortos durante el cifrado y descifrado, lo que debilita la seguridad general del algoritmo. Podríamos decir que si ciframos algo con estas llaves e intentamos descifrar por fuerza bruta en algún momento “caeremos” en el ciclo de estas llaves y por lo tanto lograremos descifrar el mensaje, cosa que no ocurre con otras llaves.



DES fue robusto en su época, pero con el avance tecnológico se descubrieron debilidades en su diseño original, estas debilidades, combinadas con la longitud de la clave y otras consideraciones, han llevado a que ciertas llaves sean inadecuadas y puedan comprometer la seguridad de los datos cifrados con DES.

3. Referencias

- *Colaboradores de Wikipedia. (2023, 7 abril). Clave débil. Wikipedia, la enciclopedia libre.*
https://es.wikipedia.org/wiki/Clave_d%C3%A9bil
- *Can you explain “weak keys” for DES? (s.f.). Cryptography Stack Exchange.*
<https://crypto.stackexchange.com/questions/12214/can-you-explain-weak-keys-for-des>
- *Colaboradores de Wikipedia. (2023, septiembre 29). Data Encryption Standard. Wikipedia, la enciclopedia libre.*https://es.wikipedia.org/wiki/Data_Encryption_Standard
- *Colaboradores de Wikipedia. (2019, 4 septiembre). Involución (matemática). Wikipedia, la enciclopedia libre.*[https://es.wikipedia.org/wiki/Involuci%C3%B3n_\(matem%C3%A1tica\)](https://es.wikipedia.org/wiki/Involuci%C3%B3n_(matem%C3%A1tica))