

# Microsurf Analysis Results

## Metadata

Run at: 03/29/2022, 11:40:03

Elapsed time (analysis): None

Elapsed time (single run emulation): 0:00:00.361392

Binary: /home/nicolas/msc-thesis-work/doc/examples/rootfs/jail-openssl-x8664/openssl

ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 4.4.0, with debug\_info, not stripped

Args: ['des-ecb', '-e', '-in', 'input.bin', '-out', 'output.bin', '-nosalt', '-K', '@']

Deterministic: False

Emulation root: /home/nicolas/msc-thesis-work/doc/examples/rootfs/jail-openssl-x8664/

## Results

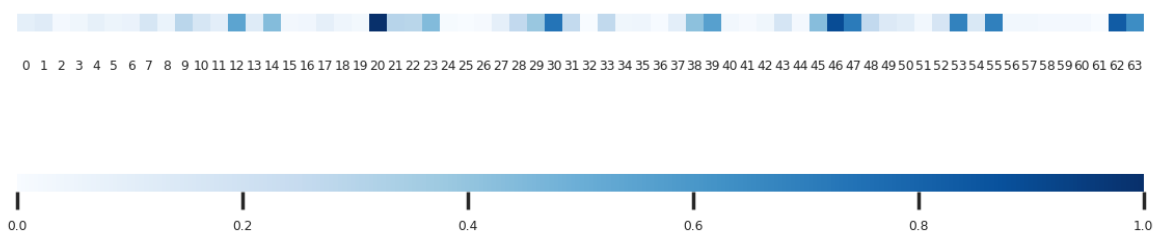
### Leaks (detailed), sorted by MI

offset	MI score	Leakage model	Function
0x111155	1.48753	neural-learnt	DES_set_key_unchecked

Source code snippet:

```
* to investigate
*/
s = des_skb[0][(c) & 0x3f] |
    des_skb[1][((c >> 6L) & 0x03) | ((c >> 7L) & 0x3c)] |
    des_skb[2][((c >> 13L) & 0x0f) | ((c >> 14L) & 0x30)] |
    des_skb[3][((c >> 20L) & 0x01) | ((c >> 21L) & 0x06)] |
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x111266	1.47854	neural-learnt	DES_set_key_unchecked

Source code snippet:

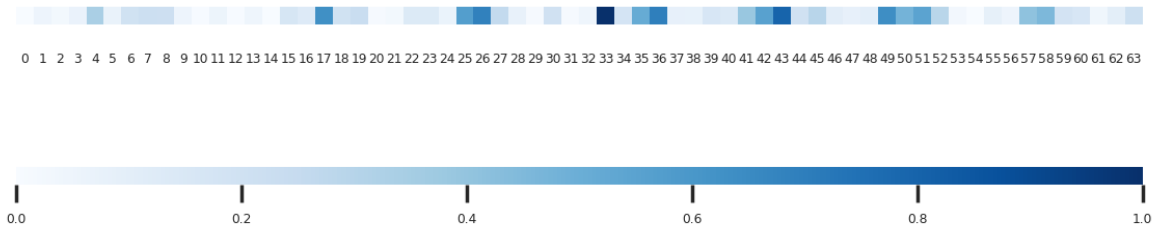
```

t = des_skb[4][(d) & 0x3f] |
    des_skb[5][((d >> 7L) & 0x03) | ((d >> 8L) & 0x3c)] |
    des_skb[6][(d >> 15L) & 0x3f] |
    des_skb[7][((d >> 21L) & 0x0f) | ((d >> 22L) & 0x30)];

/* table contained 0213 4657 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x111181	1.44628	neural-learnt	DES_set_key_unchecked

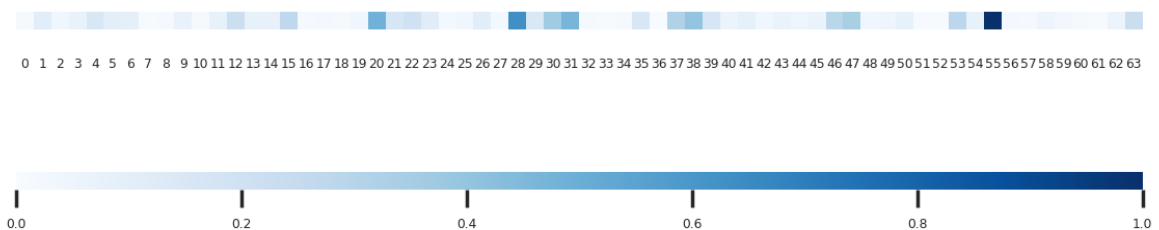
Source code snippet:

```

*/
s = des_skb[0][(c) & 0x3f] |
    des_skb[1][((c >> 6L) & 0x03) | ((c >> 7L) & 0x3c)] |
    des_skb[2][((c >> 13L) & 0x0f) | ((c >> 14L) & 0x30)] |
    des_skb[3][((c >> 20L) & 0x01) | ((c >> 21L) & 0x06) |
        ((c >> 22L) & 0x38)];

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1111eb	1.44279	neural-learnt	DES_set_key_unchecked

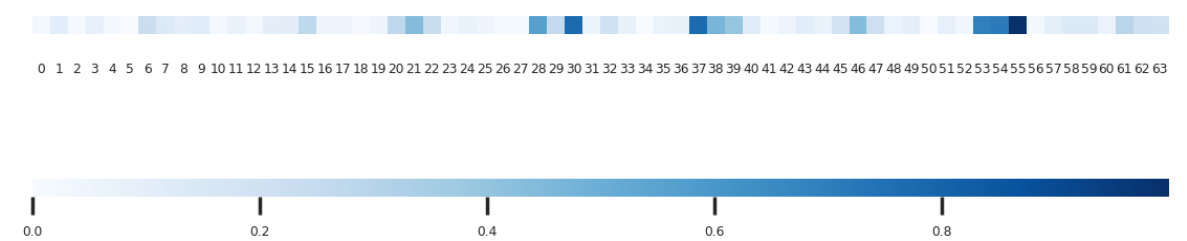
Source code snippet:

```

    des_skb[1][((c >> 6L) & 0x03) | ((c >> 7L) & 0x3c)] |
    des_skb[2][((c >> 13L) & 0x0f) | ((c >> 14L) & 0x30)] |
    des_skb[3][((c >> 20L) & 0x01) | ((c >> 21L) & 0x06) |
        ((c >> 22L) & 0x38)];
t = des_skb[4][(d) & 0x3f] |
    des_skb[5][((d >> 7L) & 0x03) | ((d >> 8L) & 0x3c)] |

```

Key bit dependencies (estimated):

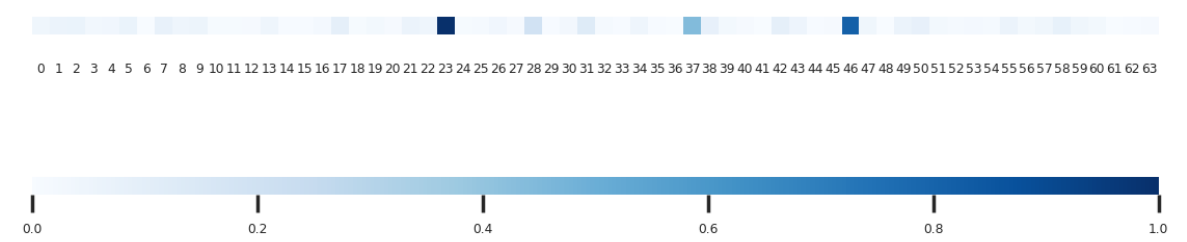


offset	MI score	Leakage model	Function
0x108387	1.41744	neural-learnt	DES_encrypt1

Source code snippet:

```
    */
    if (enc) {
        D_ENCRYPT(l, r, 0);    /* 1 */
        D_ENCRYPT(r, l, 2);    /* 2 */
        D_ENCRYPT(l, r, 4);    /* 3 */
        D_ENCRYPT(r, l, 6);    /* 4 */
    }
```

Key bit dependencies (estimated):



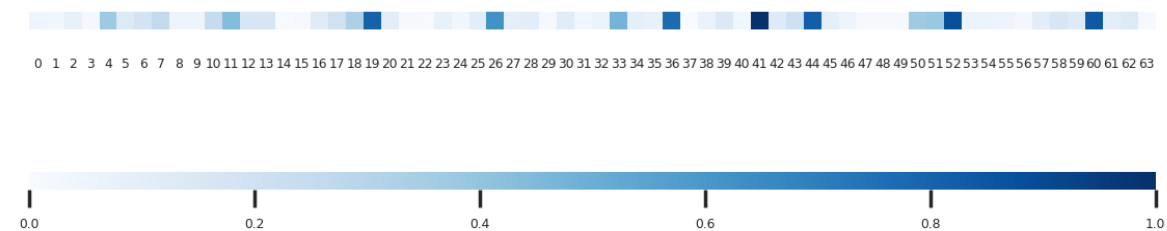
offset	MI score	Leakage model	Function
0x111298	1.33979	neural-learnt	DES_set_key_unchecked

Source code snippet:

```
    des_skb[5][((d >> 7L) & 0x03) | ((d >> 8L) & 0x3c)] |
    des_skb[6][(d >> 15L) & 0x3f] |
    des_skb[7][((d >> 21L) & 0x0f) | ((d >> 22L) & 0x30)];

    /* table contained 0213 4657 */
    t2 = ((t << 16L) | (s & 0x0000ffffL)) & 0xfffffffffL;
```

Key bit dependencies (estimated):

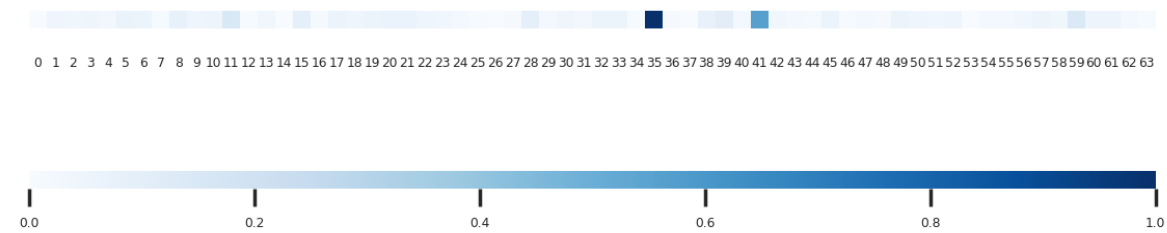


offset	MI score	Leakage model	Function
0x1083a6	1.3205	neural-learnt	DES_encrypt1

Source code snippet:

```
*/
if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
}
```

Key bit dependencies (estimated):

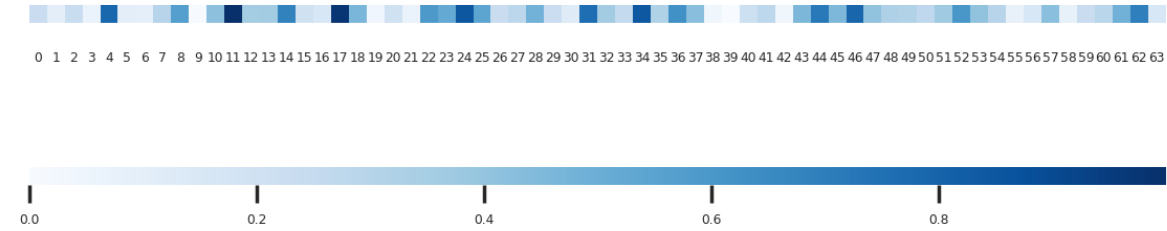


offset	MI score	Leakage model	Function
0x108e0a	1.28946	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
```

Key bit dependencies (estimated):

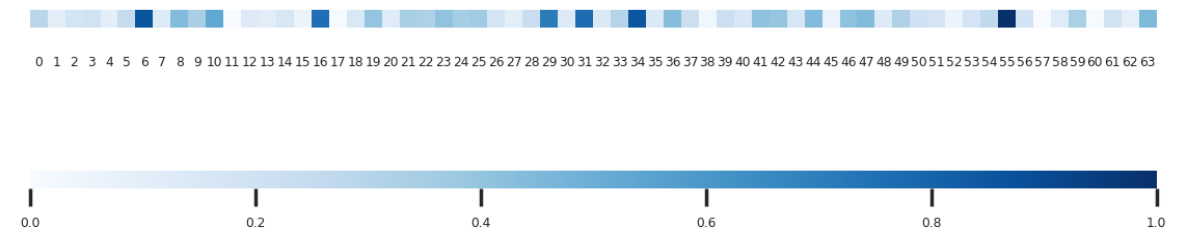


offset	MI score	Leakage model	Function
0x108fa9	1.28552	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
```

Key bit dependencies (estimated):



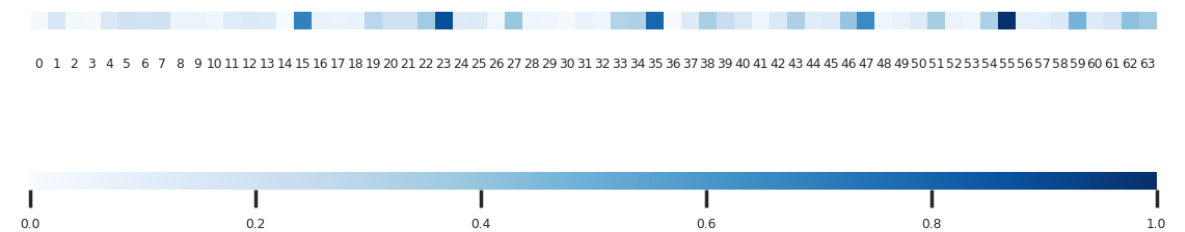
offset	MI score	Leakage model	Function
0x1a9af0	1.26796	neural-learnt	OPENSSL_hexchar2int

Source code snippet:

```
#endif

switch (c) {
case '0':
    return 0;
case '1':
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x11123f	1.23345	neural-learnt	DES_set_key_unchecked

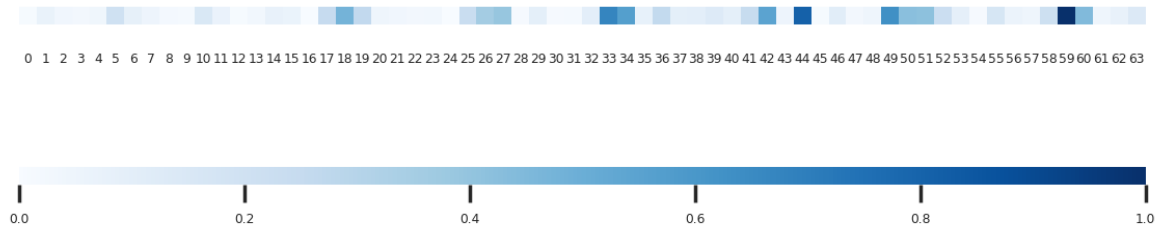
Source code snippet:

```

        ((c >> 22L) & 0x38));
t = des_skb[4][(d) & 0x3f] |
    des_skb[5][((d >> 7L) & 0x03) | ((d >> 8L) & 0x3c)] |
    des_skb[6][(d >> 15L) & 0x3f] |
    des_skb[7][((d >> 21L) & 0x0f) | ((d >> 22L) & 0x30)];

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1092a5	1.22984	neural-learnt	DES_encrypt1

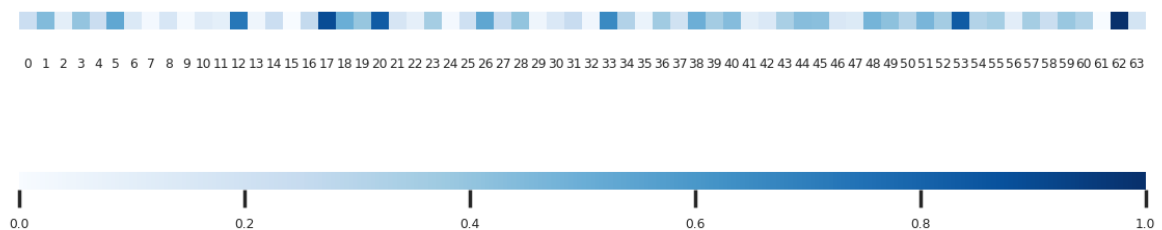
Source code snippet:

```

D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
D_ENCRYPT(l, r, 30); /* 16 */
D_ENCRYPT(r, l, 28); /* 15 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1083fe	1.22978	neural-learnt	DES_encrypt1

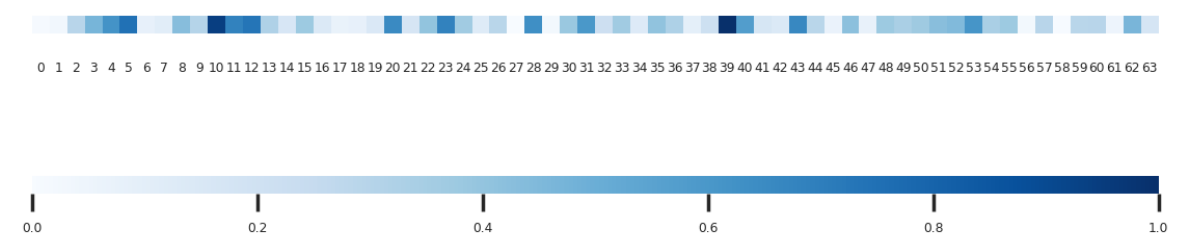
Source code snippet:

```

if (enc) {
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */

```

Key bit dependencies (estimated):

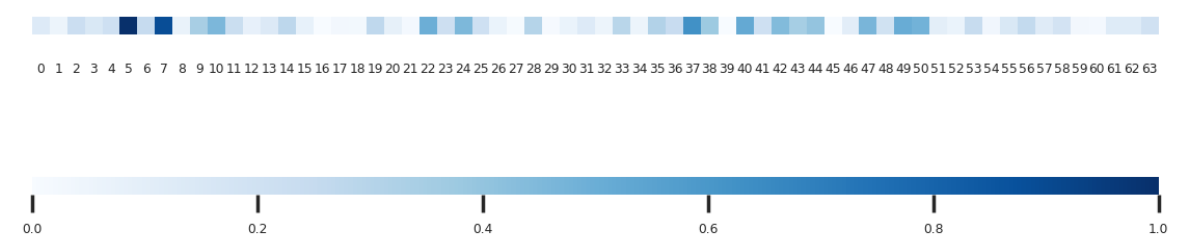


offset	MI score	Leakage model	Function
0x1090ce	1.22908	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
```

Key bit dependencies (estimated):

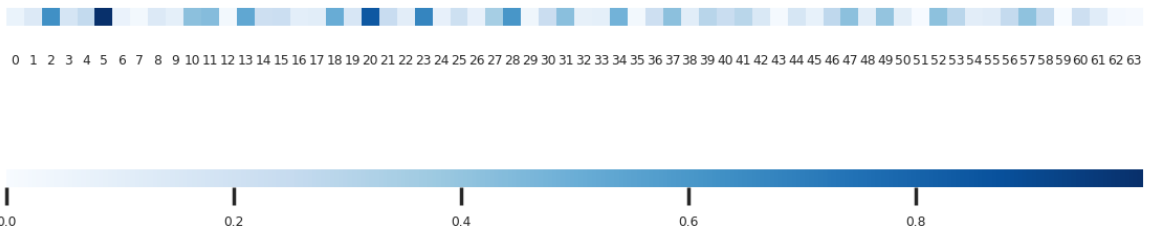


offset	MI score	Leakage model	Function
0x108930	1.21887	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
```

Key bit dependencies (estimated):

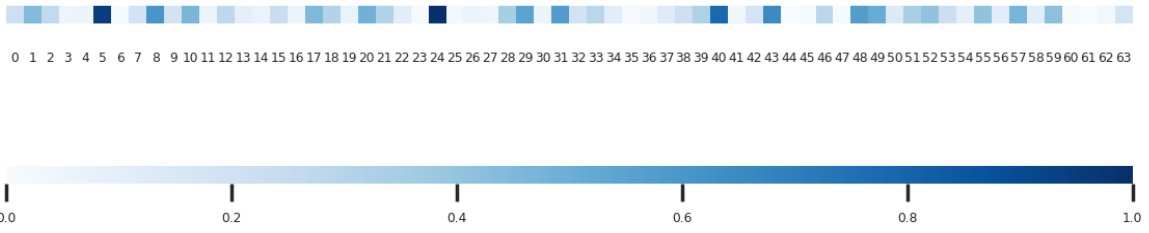


offset	MI score	Leakage model	Function
0x1084b0	1.21441	neural-learnt	DES_encrypt1

Source code snippet:

```
if (enc) {
    D_ENCRYPT(1, r, 0); /* 1 */
    D_ENCRYPT(r, 1, 2); /* 2 */
    D_ENCRYPT(1, r, 4); /* 3 */
    D_ENCRYPT(r, 1, 6); /* 4 */
    D_ENCRYPT(1, r, 8); /* 5 */
}
```

Key bit dependencies (estimated):

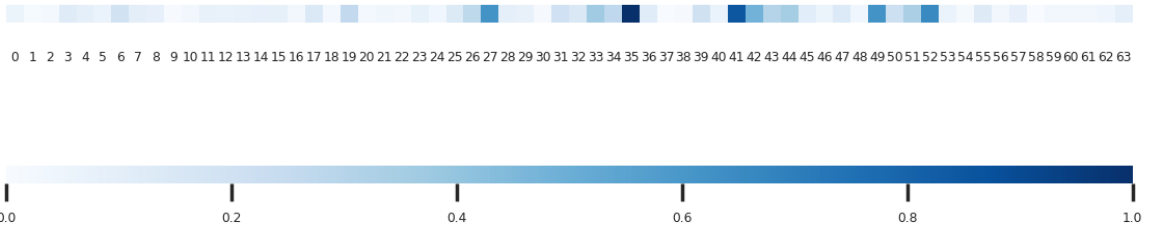


offset	MI score	Leakage model	Function
0x11120f	1.2141	neural-learnt	DES_set_key_unchecked

Source code snippet:

```
des_skb[3][((c >> 20L) & 0x01) | ((c >> 21L) & 0x06) |
            ((c >> 22L) & 0x38)];
t = des_skb[4][(d) & 0x3f] |
    des_skb[5][((d >> 7L) & 0x03) | ((d >> 8L) & 0x3c)] |
    des_skb[6][(d >> 15L) & 0x3f] |
    des_skb[7][((d >> 21L) & 0x0f) | ((d >> 22L) & 0x30)];
```

Key bit dependencies (estimated):



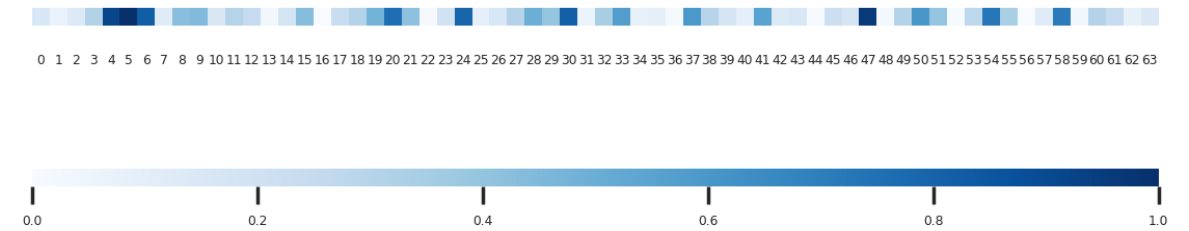


offset	MI score	Leakage model	Function
0x108aae	1.21079	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):

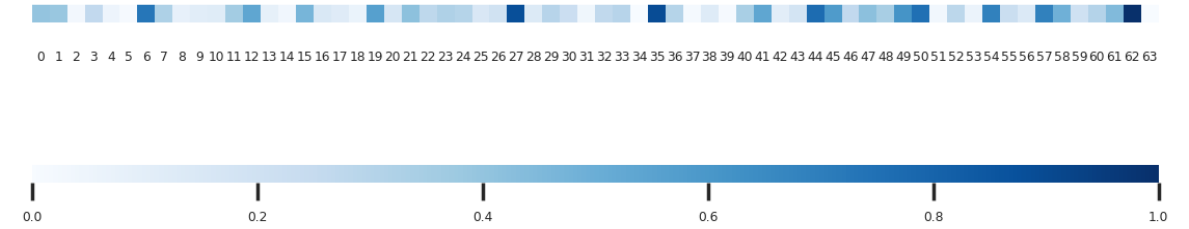


offset	MI score	Leakage model	Function
0x108d73	1.20173	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108d58	1.19477	neural-learnt	DES_encrypt1

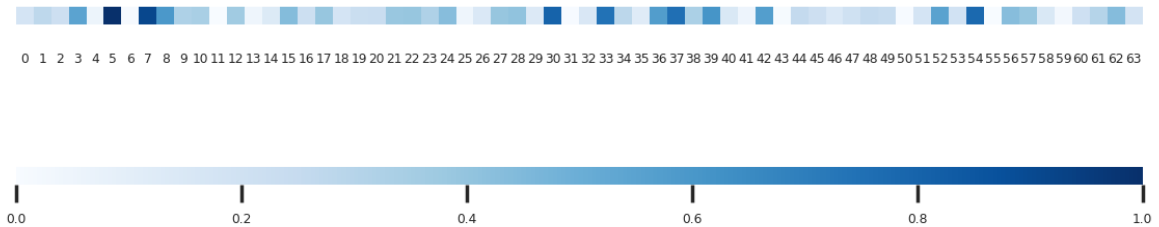
Source code snippet:

```

D_ENCRYPT(1, r, 16);    /* 9 */
D_ENCRYPT(r, 1, 18);    /* 10 */
D_ENCRYPT(1, r, 20);    /* 11 */
D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */
D_ENCRYPT(r, 1, 26);    /* 14 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x109076	1.18844	neural-learnt	DES_encrypt1

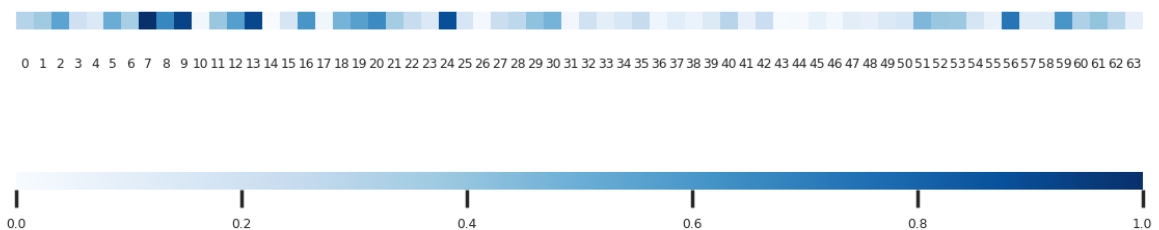
Source code snippet:

```

D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */
D_ENCRYPT(r, 1, 26);    /* 14 */
D_ENCRYPT(1, r, 28);    /* 15 */
D_ENCRYPT(r, 1, 30);    /* 16 */
} else {

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108ca6	1.18824	neural-learnt	DES_encrypt1

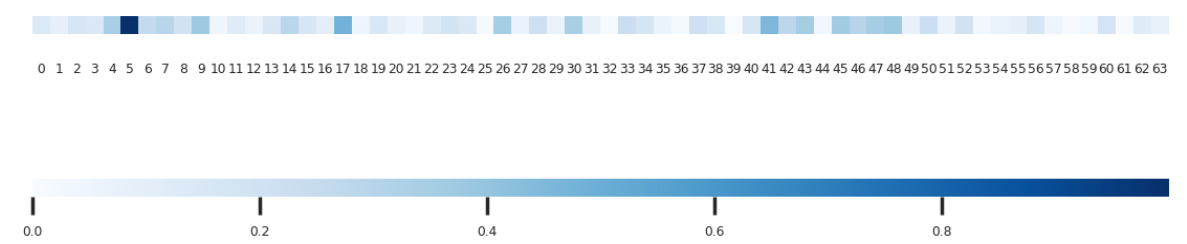
Source code snippet:

```

D_ENCRYPT(r, 1, 14);    /* 8 */
D_ENCRYPT(1, r, 16);    /* 9 */
D_ENCRYPT(r, 1, 18);    /* 10 */
D_ENCRYPT(1, r, 20);    /* 11 */
D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */

```

Key bit dependencies (estimated):

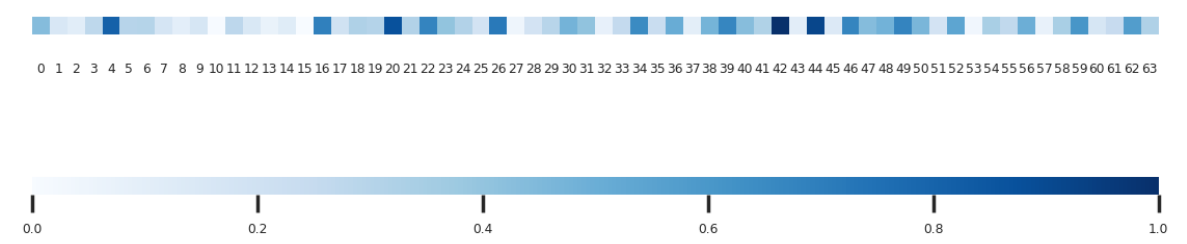


offset	MI score	Leakage model	Function
0x108ef5	1.18057	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
```

Key bit dependencies (estimated):

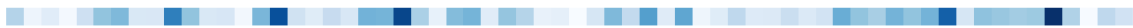


offset	MI score	Leakage model	Function
0x108b44	1.17905	neural-learnt	DES_encrypt1

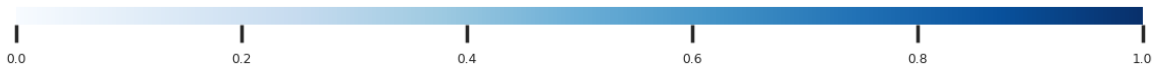
Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x108b9c	1.17222	neural-learnt	DES_encrypt1

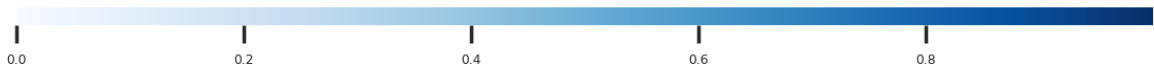
Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x10928a	1.17207	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
D_ENCRYPT(l, r, 30); /* 16 */
D_ENCRYPT(r, l, 28); /* 15 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63

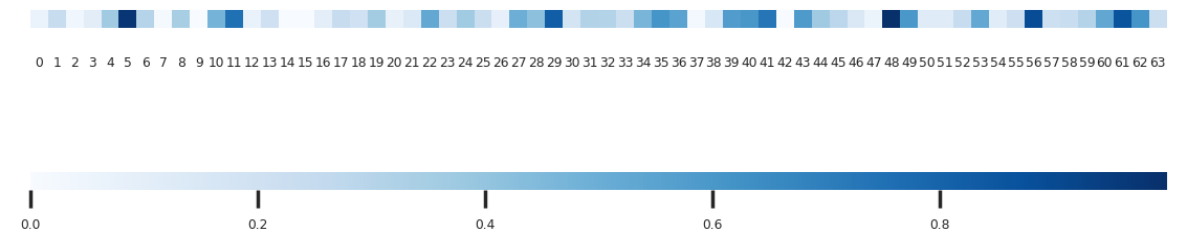


offset	MI score	Leakage model	Function
0x10919b	1.17093	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):

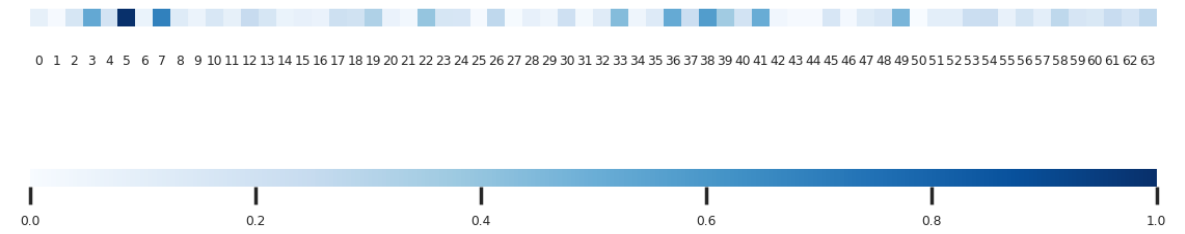


offset	MI score	Leakage model	Function
0x108841	1.16688	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x10862d	1.16432	neural-learnt	DES_encrypt1

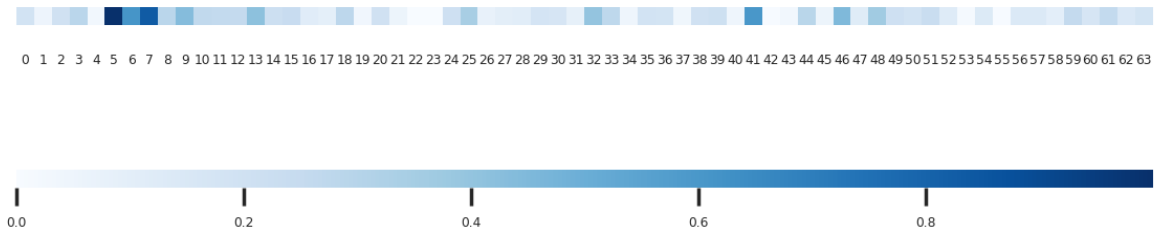
Source code snippet:

```

D_ENCRYPT(r, 1, 2);      /* 2 */
D_ENCRYPT(1, r, 4);      /* 3 */
D_ENCRYPT(r, 1, 6);      /* 4 */
D_ENCRYPT(1, r, 8);      /* 5 */
D_ENCRYPT(r, 1, 10);     /* 6 */
D_ENCRYPT(1, r, 12);     /* 7 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x035720	1.16133	neural-learnt	set_hex

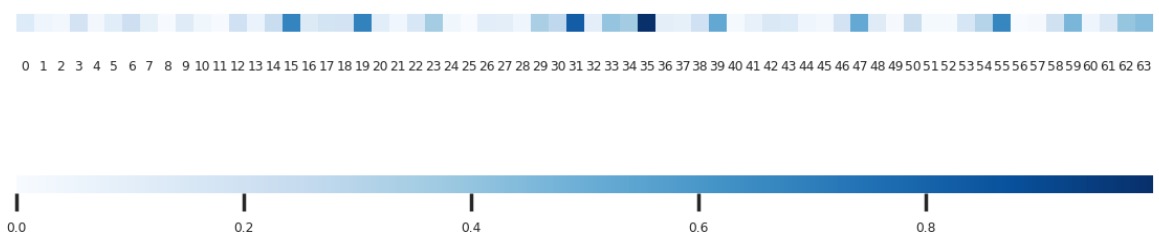
Source code snippet:

```

if (j == 0)
    break;
if (!isdigit(j)) {
    BIO_printf(bio_err, "non-hex digit\n");
    return 0;
}

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1111b1	1.15831	neural-learnt	DES_set_key_unchecked

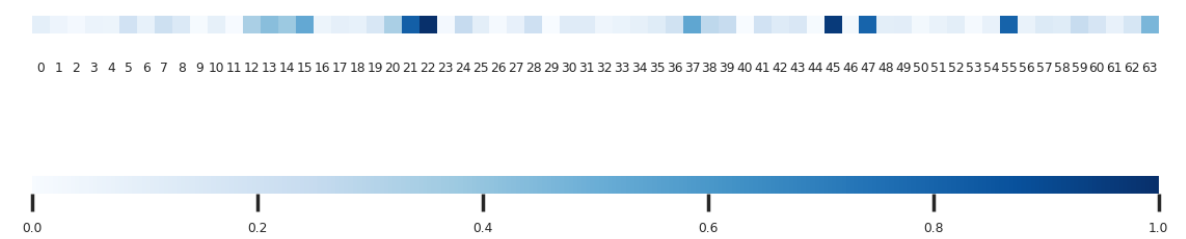
Source code snippet:

```

s = des_skb[0][(c) & 0x3f] |
    des_skb[1][((c >> 6L) & 0x03) | ((c >> 7L) & 0x3c)] |
    des_skb[2][((c >> 13L) & 0x0f) | ((c >> 14L) & 0x30)] |
    des_skb[3][((c >> 20L) & 0x01) | ((c >> 21L) & 0x06) |
                ((c >> 22L) & 0x38)];
t = des_skb[4][(d) & 0x3f] |

```

Key bit dependencies (estimated):

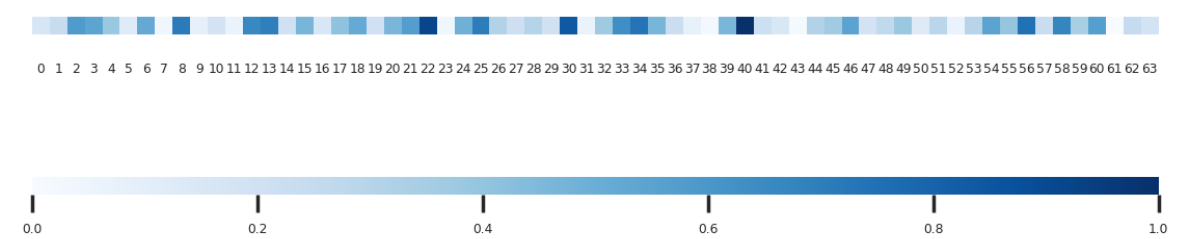


offset	MI score	Leakage model	Function
0x1088f2	1.15831	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):

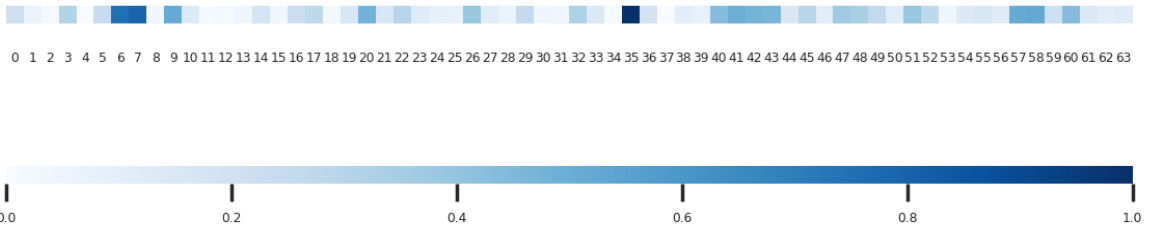


offset	MI score	Leakage model	Function
0x1087ce	1.14497	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):

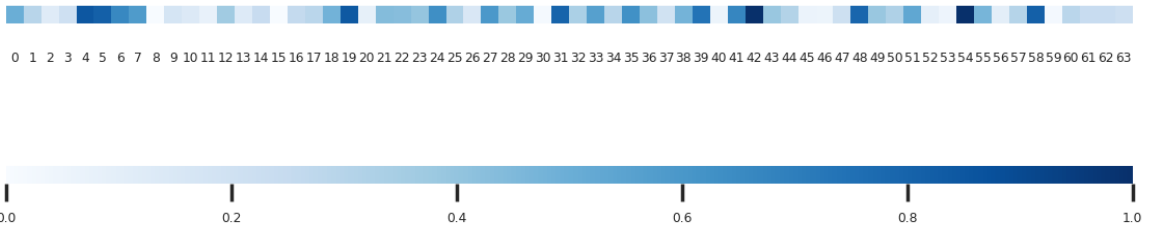


offset	MI score	Leakage model	Function
0x1092fe	1.13991	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
    D_ENCRYPT(r, l, 28); /* 15 */
}
```

Key bit dependencies (estimated):

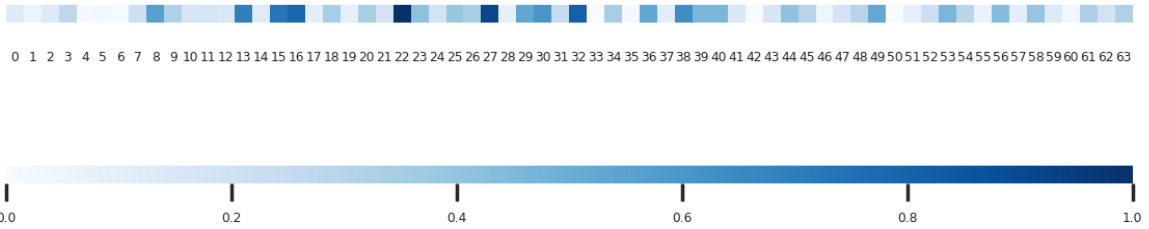


offset	MI score	Leakage model	Function
0x108f2e	1.13856	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
```

Key bit dependencies (estimated):



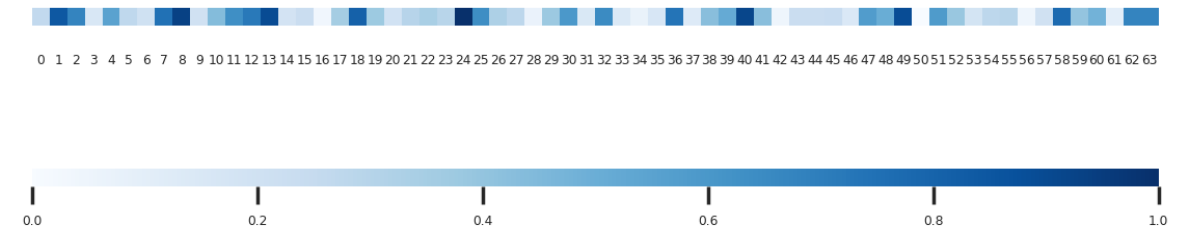


offset	MI score	Leakage model	Function
0x109109	1.13848	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
```

Key bit dependencies (estimated):

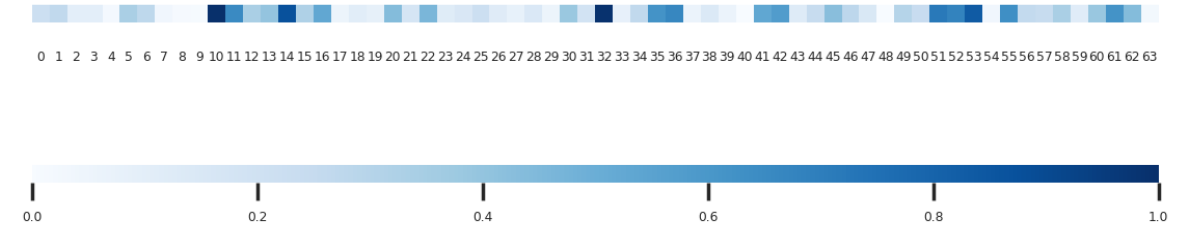


offset	MI score	Leakage model	Function
0x1086de	1.13462	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1088b9	1.13447	neural-learnt	DES_encrypt1

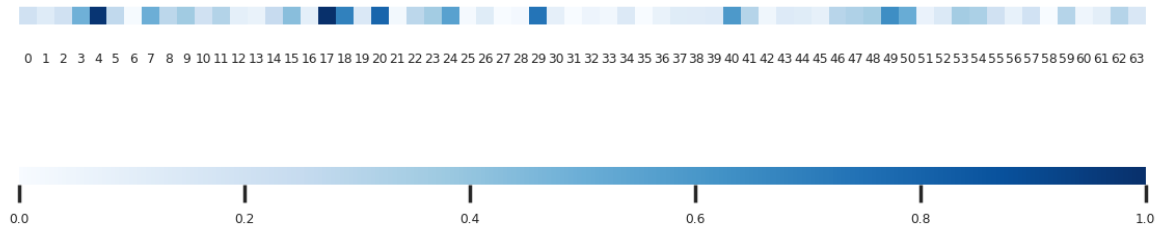
Source code snippet:

```

D_ENCRYPT(r, l, 6);      /* 4 */
D_ENCRYPT(l, r, 8);      /* 5 */
D_ENCRYPT(r, l, 10);     /* 6 */
D_ENCRYPT(l, r, 12);     /* 7 */
D_ENCRYPT(r, l, 14);     /* 8 */
D_ENCRYPT(l, r, 16);     /* 9 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1089a4	1.13308	neural-learnt	DES_encrypt1

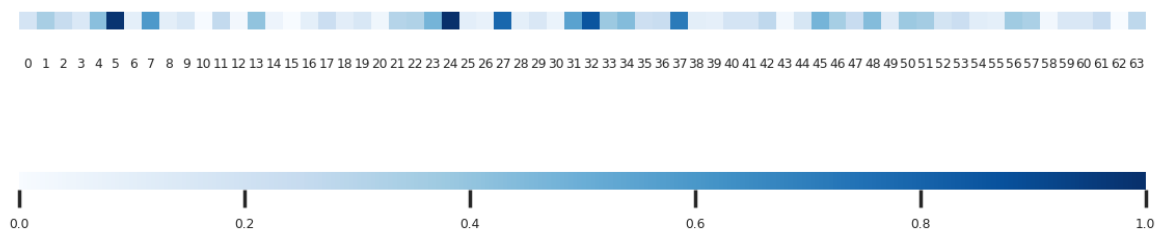
Source code snippet:

```

D_ENCRYPT(l, r, 8);      /* 5 */
D_ENCRYPT(r, l, 10);     /* 6 */
D_ENCRYPT(l, r, 12);     /* 7 */
D_ENCRYPT(r, l, 14);     /* 8 */
D_ENCRYPT(l, r, 16);     /* 9 */
D_ENCRYPT(r, l, 18);     /* 10 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108d95	1.13199	neural-learnt	DES_encrypt1

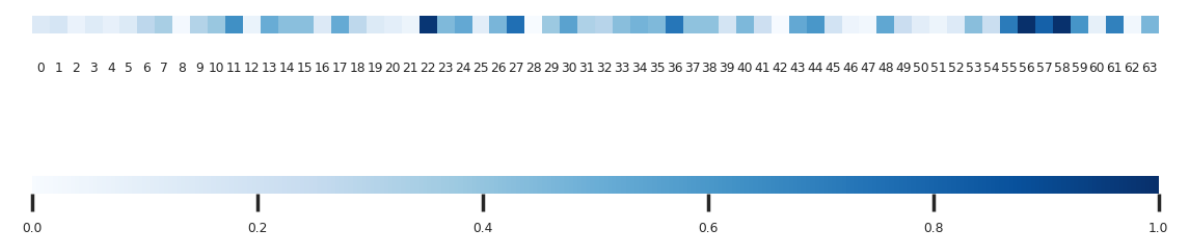
Source code snippet:

```

D_ENCRYPT(l, r, 16);     /* 9 */
D_ENCRYPT(r, l, 18);     /* 10 */
D_ENCRYPT(l, r, 20);     /* 11 */
D_ENCRYPT(r, l, 22);     /* 12 */
D_ENCRYPT(l, r, 24);     /* 13 */
D_ENCRYPT(r, l, 26);     /* 14 */

```

Key bit dependencies (estimated):

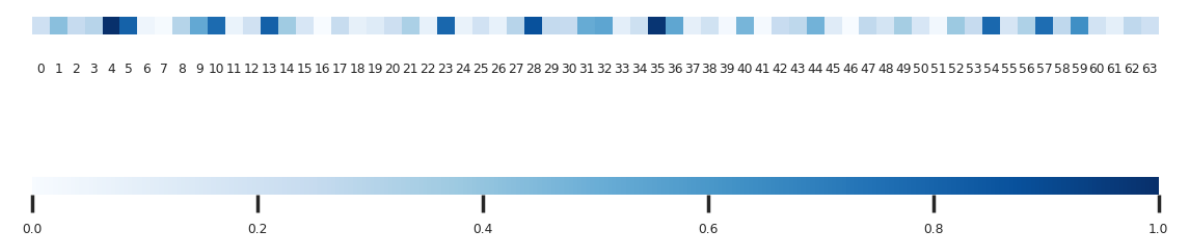


offset	MI score	Leakage model	Function
0x108686	1.13167	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108a92	1.13157	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x108737	1.12919	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x108a3a	1.12864	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63

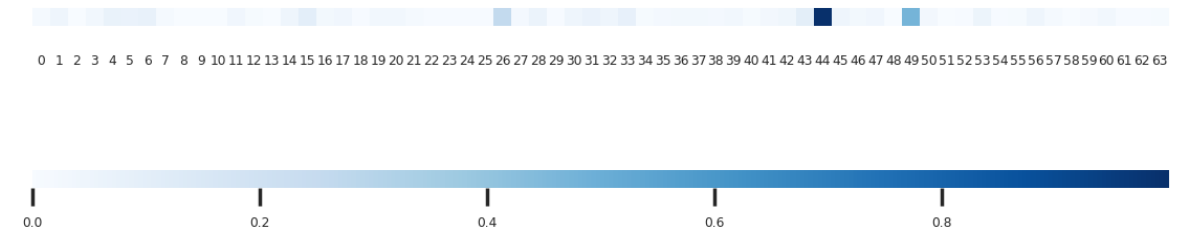


offset	MI score	Leakage model	Function
0x10834c	1.12751	neural-learnt	DES_encrypt1

Source code snippet:

```
    */
    if (enc) {
        D_ENCRYPT(l, r, 0);    /* 1 */
        D_ENCRYPT(r, l, 2);    /* 2 */
        D_ENCRYPT(l, r, 4);    /* 3 */
        D_ENCRYPT(r, l, 6);    /* 4 */
    }
```

Key bit dependencies (estimated):

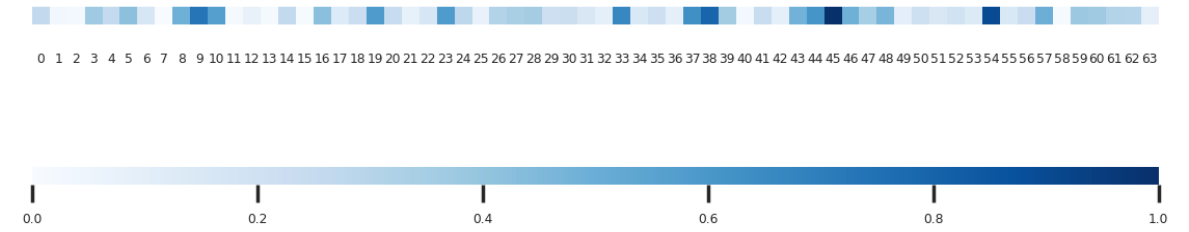


offset	MI score	Leakage model	Function
0x108bd7	1.12734	neural-learnt	DES_encrypt1

Source code snippet:

```
        D_ENCRYPT(l, r, 12);    /* 7 */
        D_ENCRYPT(r, l, 14);    /* 8 */
        D_ENCRYPT(l, r, 16);    /* 9 */
        D_ENCRYPT(r, l, 18);    /* 10 */
        D_ENCRYPT(l, r, 20);    /* 11 */
        D_ENCRYPT(r, l, 22);    /* 12 */
    }
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108368	1.12592	neural-learnt	DES_encrypt1

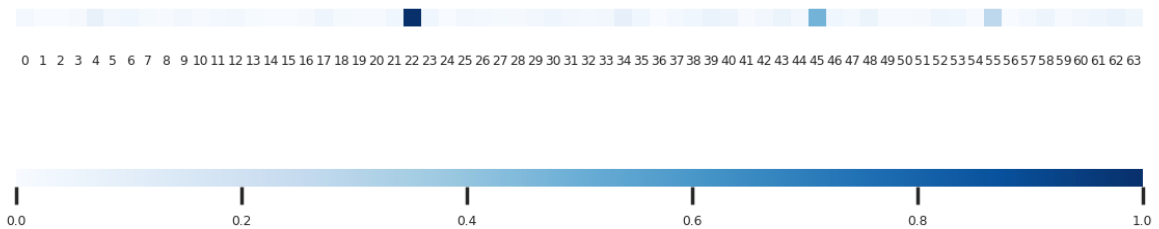
Source code snippet:

```

    */
    if (enc) {
        D_ENCRYPT(l, r, 0);    /* 1 */
        D_ENCRYPT(r, l, 2);    /* 2 */
        D_ENCRYPT(l, r, 4);    /* 3 */
        D_ENCRYPT(r, l, 6);    /* 4 */
    }

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x10894b	1.12317	neural-learnt	DES_encrypt1

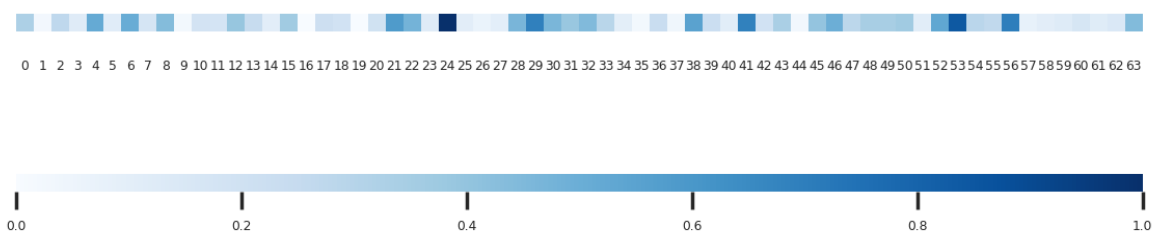
Source code snippet:

```

    D_ENCRYPT(l, r, 8);    /* 5 */
    D_ENCRYPT(r, l, 10);   /* 6 */
    D_ENCRYPT(l, r, 12);   /* 7 */
    D_ENCRYPT(r, l, 14);   /* 8 */
    D_ENCRYPT(l, r, 16);   /* 9 */
    D_ENCRYPT(r, l, 18);   /* 10 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1089e2	1.12292	neural-learnt	DES_encrypt1

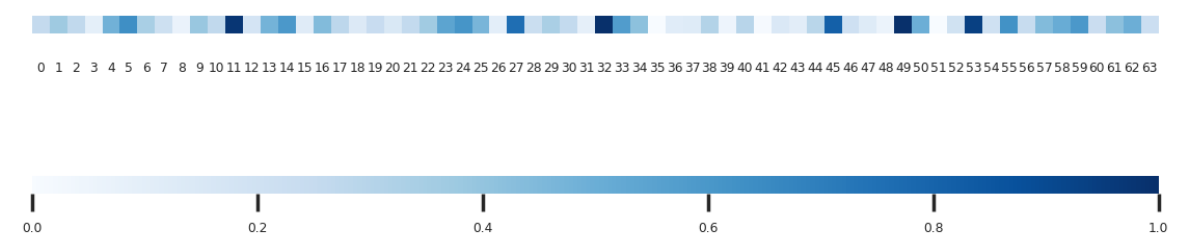
Source code snippet:

```

    D_ENCRYPT(l, r, 8);    /* 5 */
    D_ENCRYPT(r, l, 10);   /* 6 */
    D_ENCRYPT(l, r, 12);   /* 7 */
    D_ENCRYPT(r, l, 14);   /* 8 */
    D_ENCRYPT(l, r, 16);   /* 9 */
    D_ENCRYPT(r, l, 18);   /* 10 */

```

Key bit dependencies (estimated):

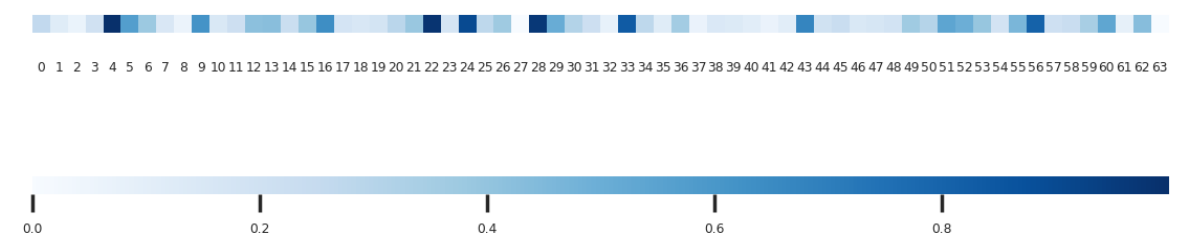


offset	MI score	Leakage model	Function
0x1085ba	1.11768	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):

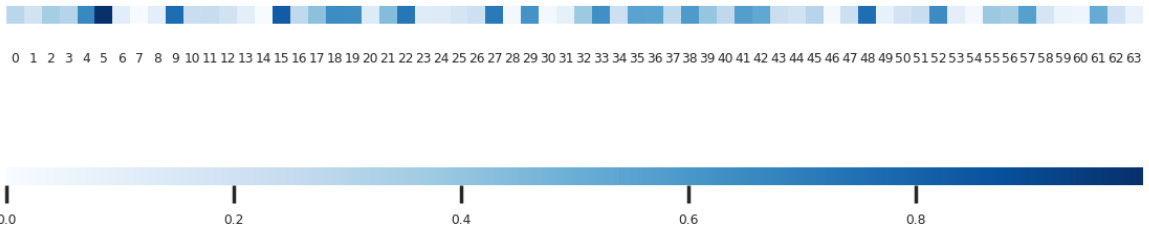


offset	MI score	Leakage model	Function
0x108545	1.1164	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):

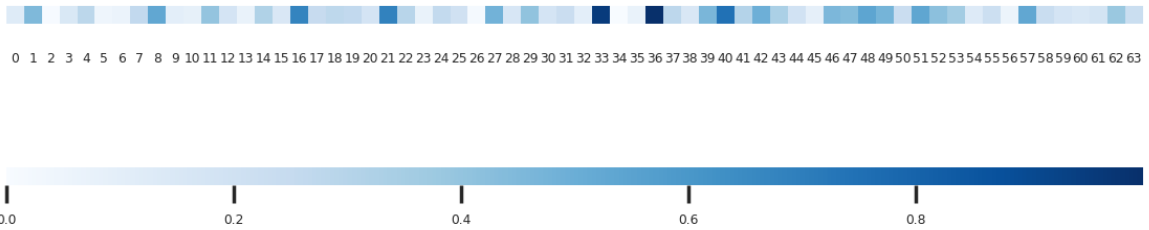


offset	MI score	Leakage model	Function
0x10896d	1.1135	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
```

Key bit dependencies (estimated):

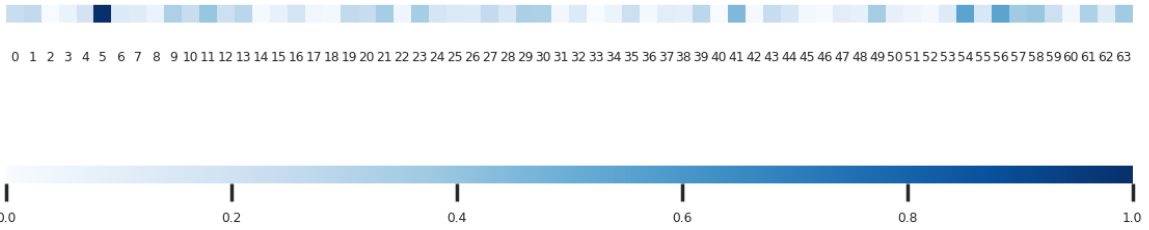


offset	MI score	Leakage model	Function
0x108b81	1.11229	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):



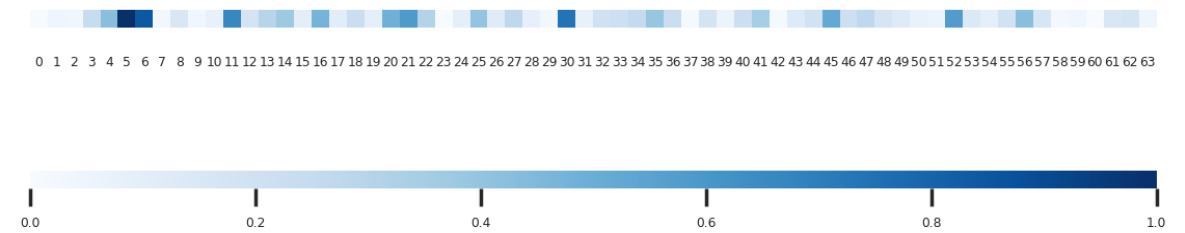


offset	MI score	Leakage model	Function
0x108e7d	1.11072	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
```

Key bit dependencies (estimated):

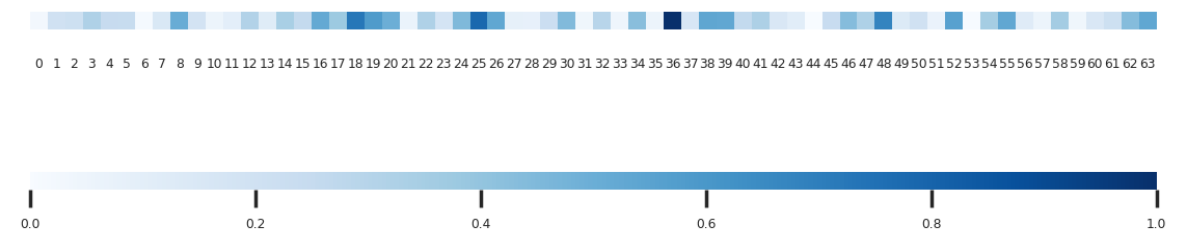


offset	MI score	Leakage model	Function
0x108c8b	1.10467	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108deb	1.10231	neural-learnt	DES_encrypt1

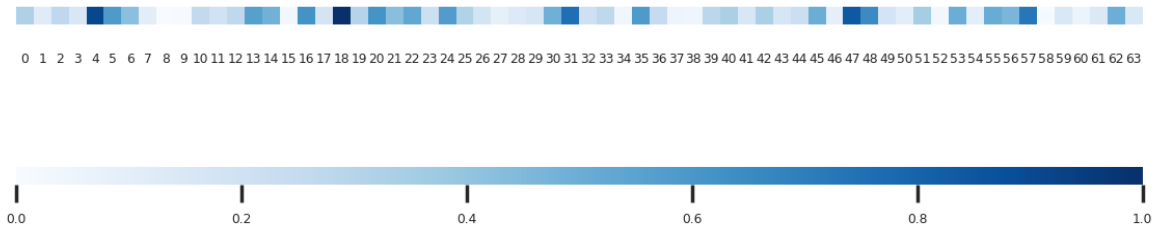
Source code snippet:

```

D_ENCRYPT(1, r, 16);    /* 9 */
D_ENCRYPT(r, 1, 18);    /* 10 */
D_ENCRYPT(1, r, 20);    /* 11 */
D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */
D_ENCRYPT(r, 1, 26);    /* 14 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108491	1.10055	neural-learnt	DES_encrypt1

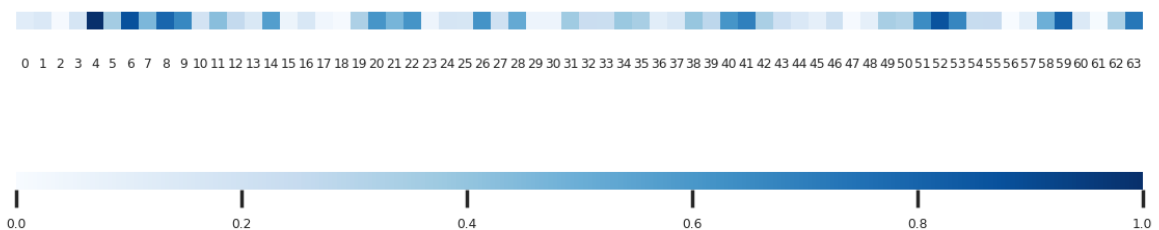
Source code snippet:

```

if (enc) {
    D_ENCRYPT(1, r, 0);    /* 1 */
    D_ENCRYPT(r, 1, 2);    /* 2 */
    D_ENCRYPT(1, r, 4);    /* 3 */
    D_ENCRYPT(r, 1, 6);    /* 4 */
    D_ENCRYPT(1, r, 8);    /* 5 */
}

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1090ea	1.09956	neural-learnt	DES_encrypt1

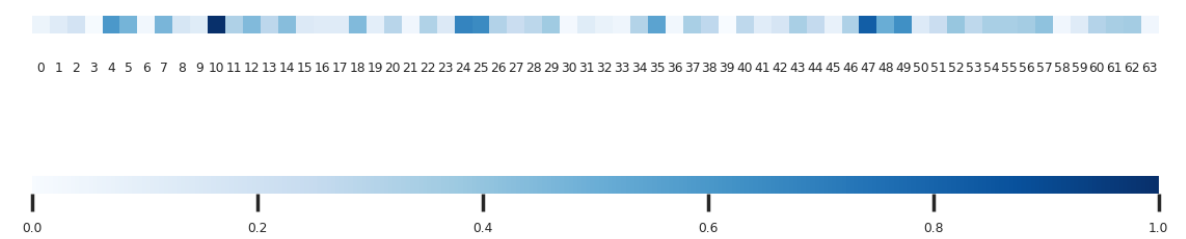
Source code snippet:

```

D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */
D_ENCRYPT(r, 1, 26);    /* 14 */
D_ENCRYPT(1, r, 28);    /* 15 */
D_ENCRYPT(r, 1, 30);    /* 16 */
} else {

```

Key bit dependencies (estimated):

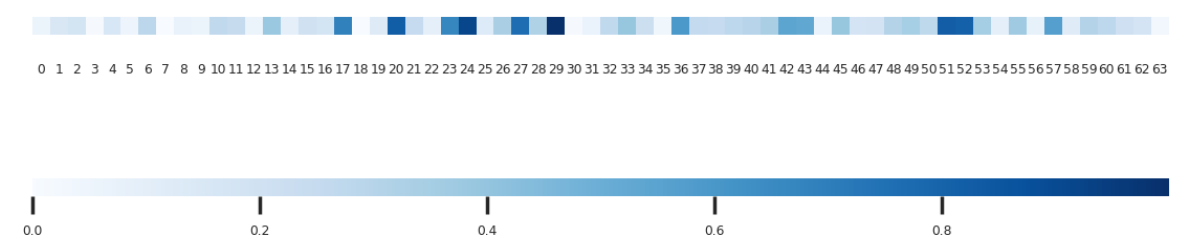


offset	MI score	Leakage model	Function
0x1087e8	1.09706	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):

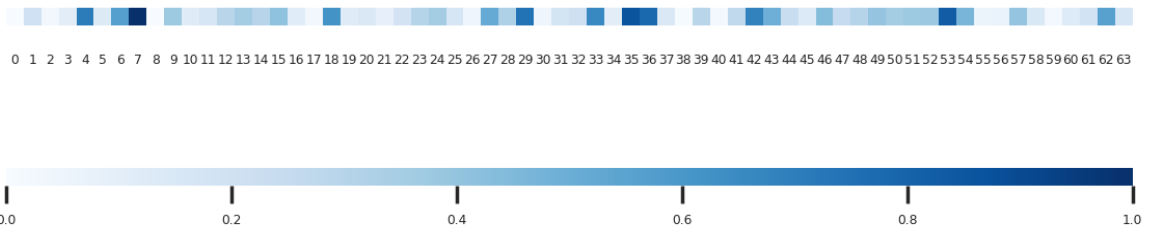


offset	MI score	Leakage model	Function
0x10866a	1.09565	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):

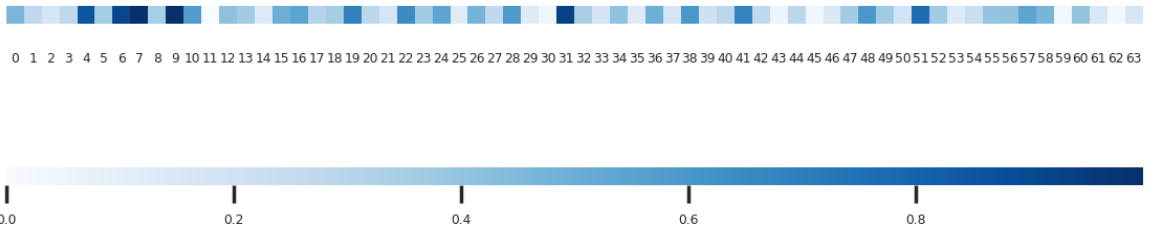


offset	MI score	Leakage model	Function
0x1092e2	1.09487	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
  D_ENCRYPT(l, r, 30); /* 16 */
  D_ENCRYPT(r, l, 28); /* 15 */
}
```

Key bit dependencies (estimated):

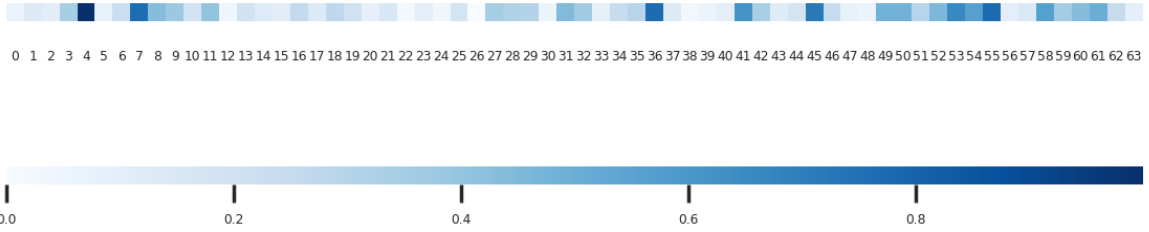


offset	MI score	Leakage model	Function
0x1088d8	1.09397	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):

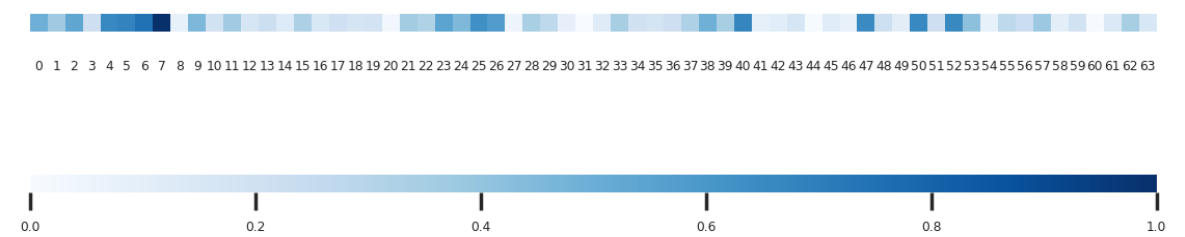


offset	MI score	Leakage model	Function
0x109213	1.09341	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):

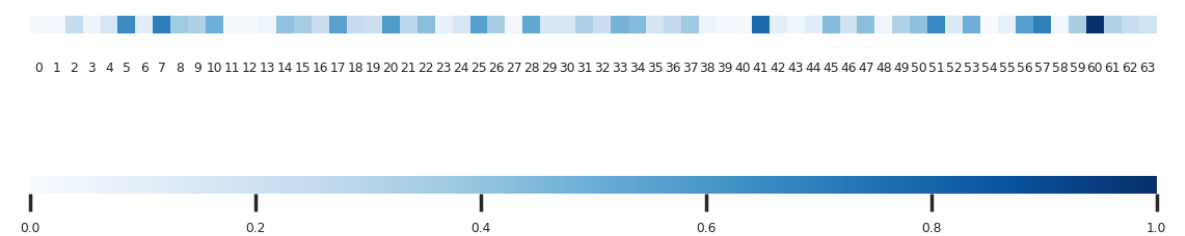


offset	MI score	Leakage model	Function
0x10830f	1.09251	neural-learnt	DES_encrypt1

Source code snippet:

```
*/
if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1087af	1.09102	neural-learnt	DES_encrypt1

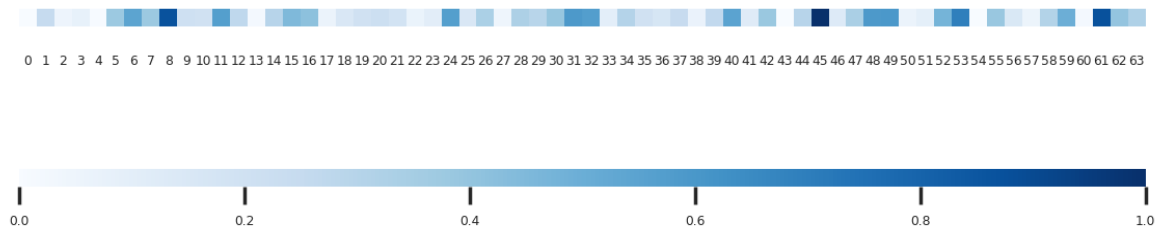
Source code snippet:

```

D_ENCRYPT(l, r, 4);      /* 3 */
D_ENCRYPT(r, l, 6);      /* 4 */
D_ENCRYPT(l, r, 8);      /* 5 */
D_ENCRYPT(r, l, 10);     /* 6 */
D_ENCRYPT(l, r, 12);     /* 7 */
D_ENCRYPT(r, l, 14);     /* 8 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x10843b	1.09024	neural-learnt	DES_encrypt1

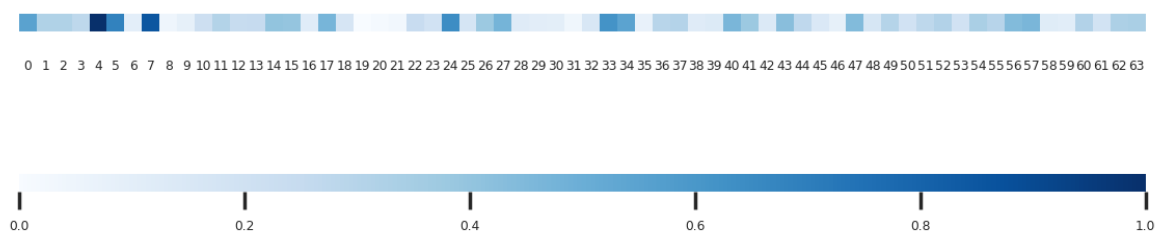
Source code snippet:

```

if (enc) {
    D_ENCRYPT(l, r, 0);      /* 1 */
    D_ENCRYPT(r, l, 2);      /* 2 */
    D_ENCRYPT(l, r, 4);      /* 3 */
    D_ENCRYPT(r, l, 6);      /* 4 */
    D_ENCRYPT(l, r, 8);      /* 5 */
}

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1091f4	1.08576	neural-learnt	DES_encrypt1

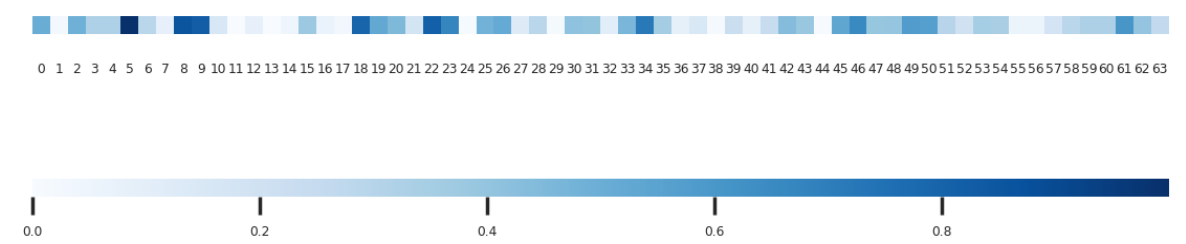
Source code snippet:

```

D_ENCRYPT(l, r, 24);      /* 13 */
D_ENCRYPT(r, l, 26);      /* 14 */
D_ENCRYPT(l, r, 28);      /* 15 */
D_ENCRYPT(r, l, 30);      /* 16 */
} else {
    D_ENCRYPT(l, r, 30);    /* 16 */
}

```

Key bit dependencies (estimated):

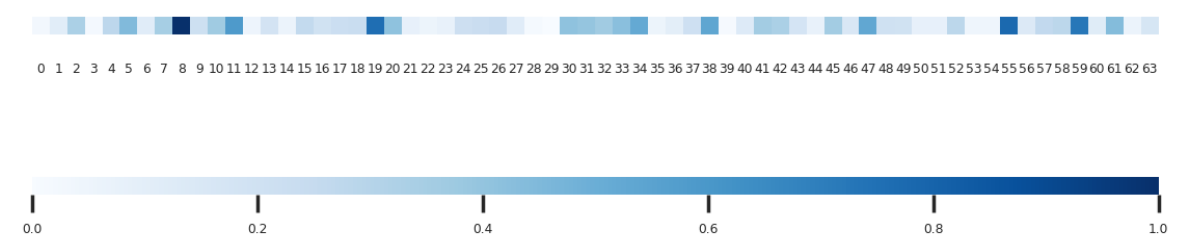


offset	MI score	Leakage model	Function
0x1086c4	1.08493	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):

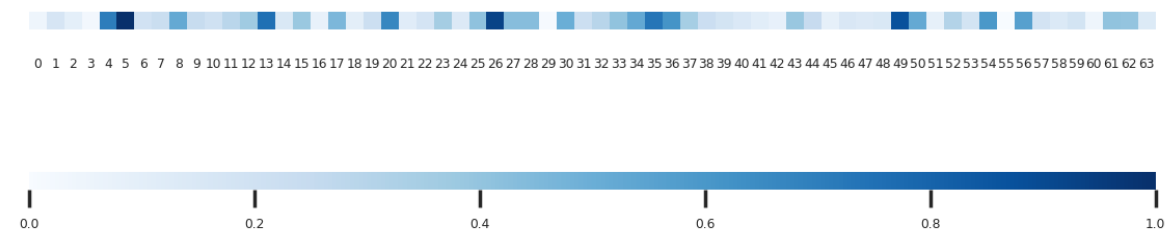


offset	MI score	Leakage model	Function
0x1086a5	1.08455	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):

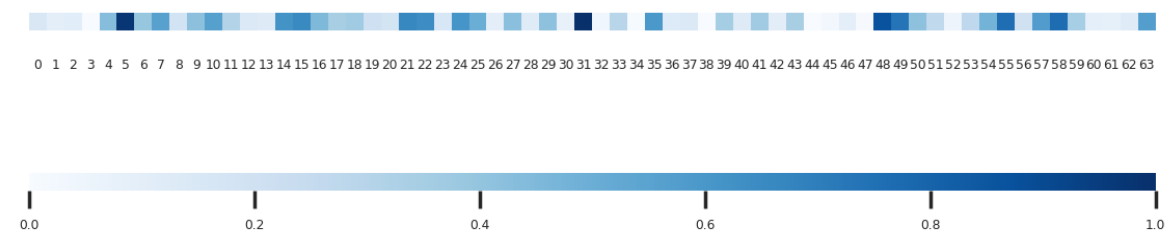


offset	MI score	Leakage model	Function
0x108774	1.08076	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):

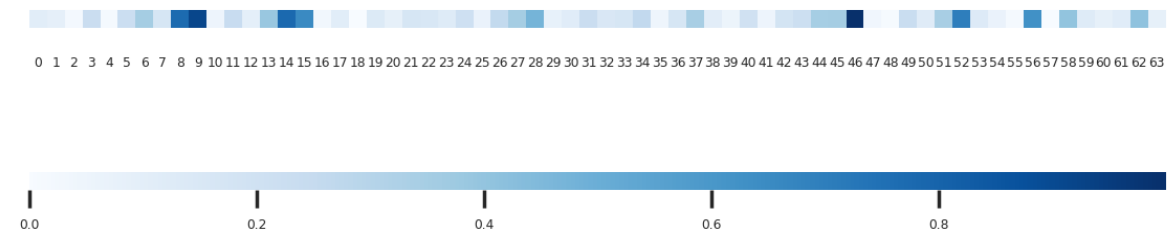


offset	MI score	Leakage model	Function
0x108419	1.0799	neural-learnt	DES_encrypt1

Source code snippet:

```
if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
    D_ENCRYPT(l, r, 8); /* 5 */
}
```

Key bit dependencies (estimated):



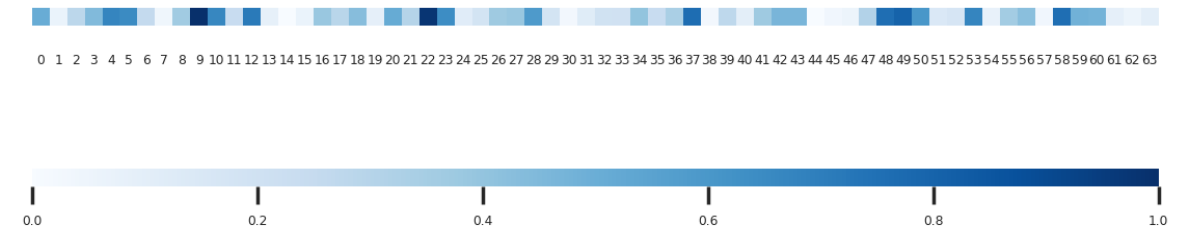


offset	MI score	Leakage model	Function
0x108d1a	1.07272	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
```

Key bit dependencies (estimated):

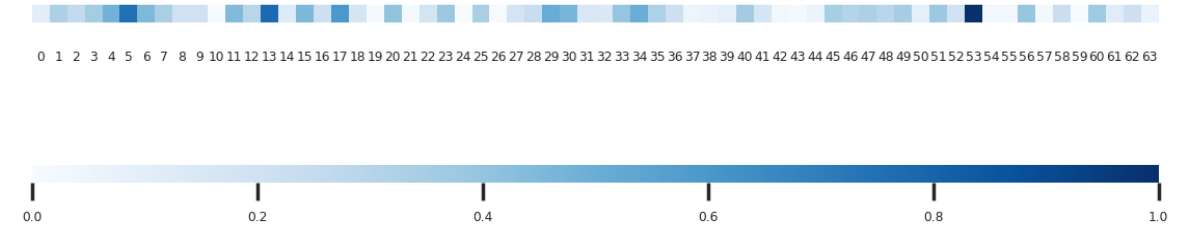


offset	MI score	Leakage model	Function
0x108472	1.06632	neural-learnt	DES_encrypt1

Source code snippet:

```
if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
    D_ENCRYPT(l, r, 8); /* 5 */
}
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108b5f	1.06573	neural-learnt	DES_encrypt1

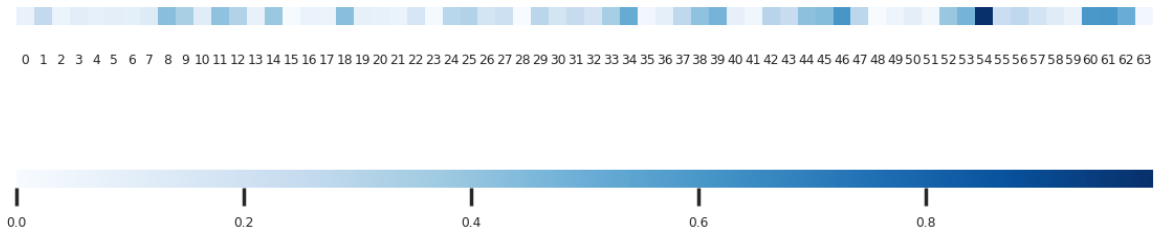
Source code snippet:

```

D_ENCRYPT(l, r, 12);    /* 7 */
D_ENCRYPT(r, l, 14);    /* 8 */
D_ENCRYPT(l, r, 16);    /* 9 */
D_ENCRYPT(r, l, 18);    /* 10 */
D_ENCRYPT(l, r, 20);    /* 11 */
D_ENCRYPT(r, l, 22);    /* 12 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108826	1.06303	neural-learnt	DES_encrypt1

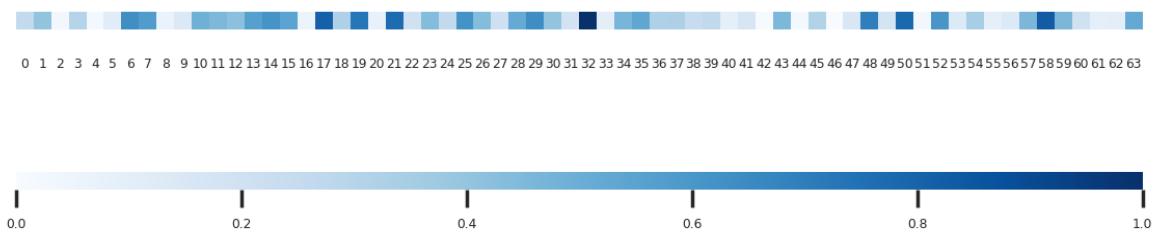
Source code snippet:

```

D_ENCRYPT(r, l, 6);     /* 4 */
D_ENCRYPT(l, r, 8);     /* 5 */
D_ENCRYPT(r, l, 10);    /* 6 */
D_ENCRYPT(l, r, 12);    /* 7 */
D_ENCRYPT(r, l, 14);    /* 8 */
D_ENCRYPT(l, r, 16);    /* 9 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108988	1.05855	neural-learnt	DES_encrypt1

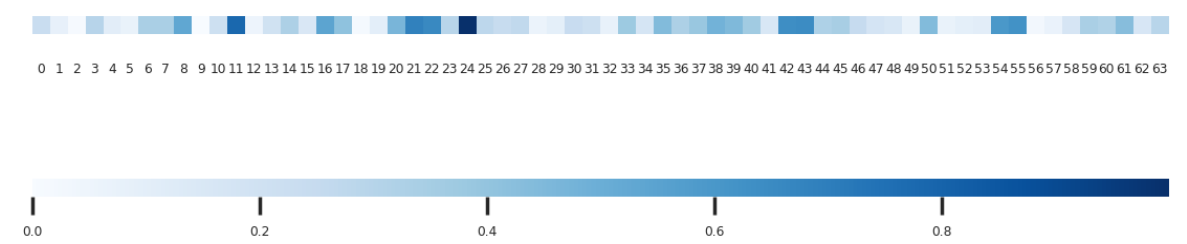
Source code snippet:

```

D_ENCRYPT(l, r, 8);     /* 5 */
D_ENCRYPT(r, l, 10);    /* 6 */
D_ENCRYPT(l, r, 12);    /* 7 */
D_ENCRYPT(r, l, 14);    /* 8 */
D_ENCRYPT(l, r, 16);    /* 9 */
D_ENCRYPT(r, l, 18);    /* 10 */

```

Key bit dependencies (estimated):

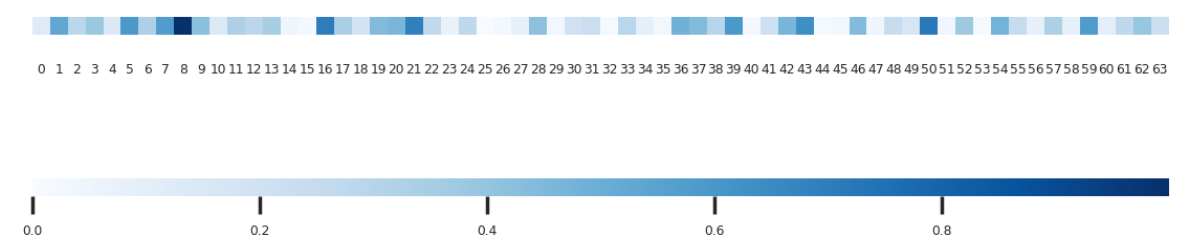


offset	MI score	Leakage model	Function
0x10901e	1.05565	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
```

Key bit dependencies (estimated):

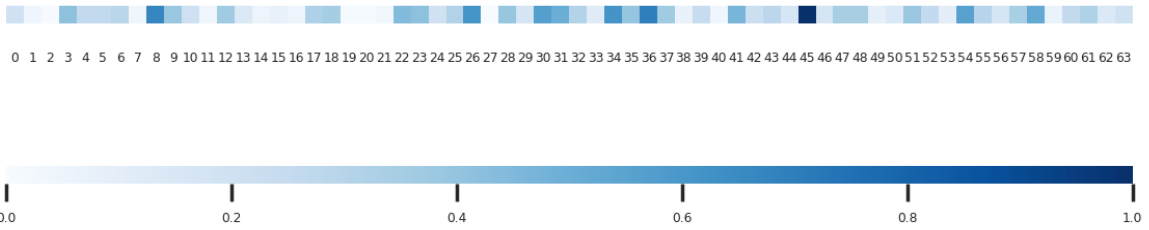


offset	MI score	Leakage model	Function
0x108508	1.05323	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):

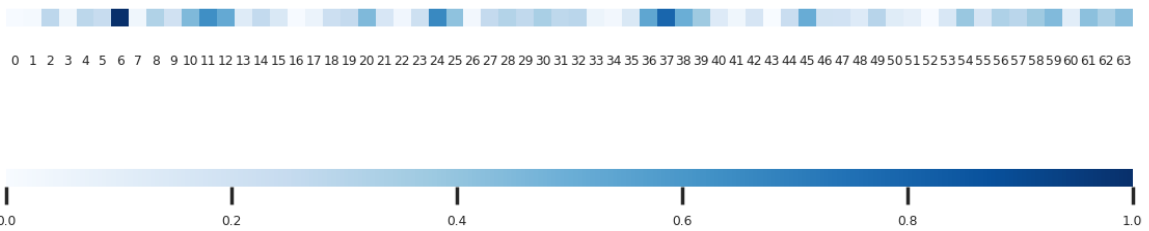


offset	MI score	Leakage model	Function
0x108fff	1.05262	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
```

Key bit dependencies (estimated):

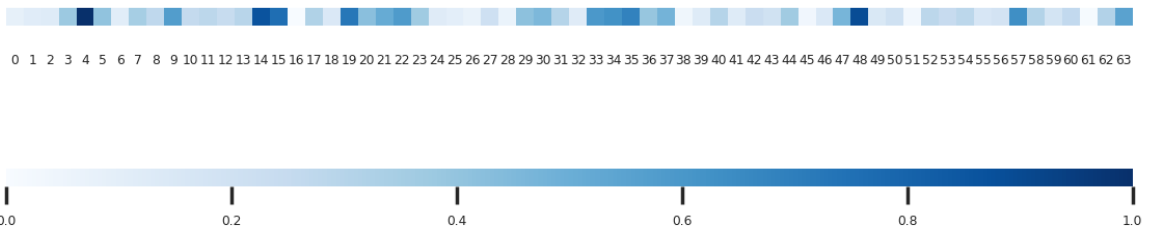


offset	MI score	Leakage model	Function
0x108e24	1.04896	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
```

Key bit dependencies (estimated):

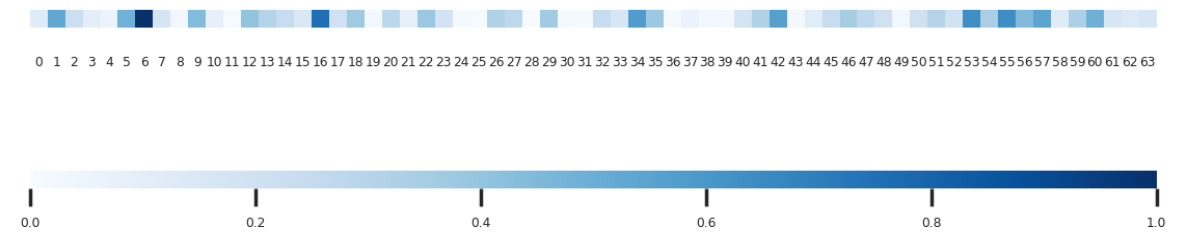


offset	MI score	Leakage model	Function
0x108bb8	1.04861	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):

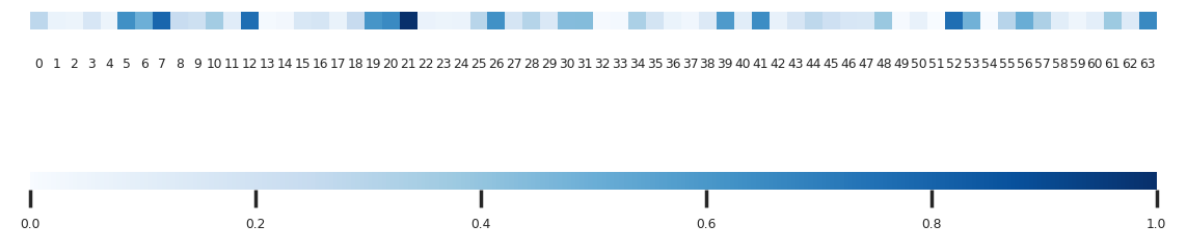


offset	MI score	Leakage model	Function
0x108acd	1.04648	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1090b3	1.04566	neural-learnt	DES_encrypt1

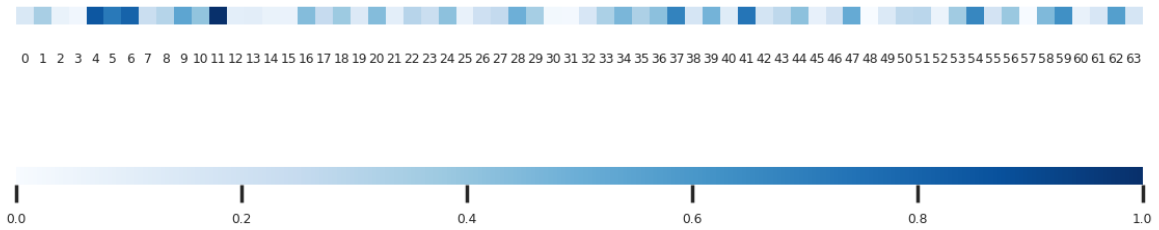
Source code snippet:

```

D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108c69	1.04527	neural-learnt	DES_encrypt1

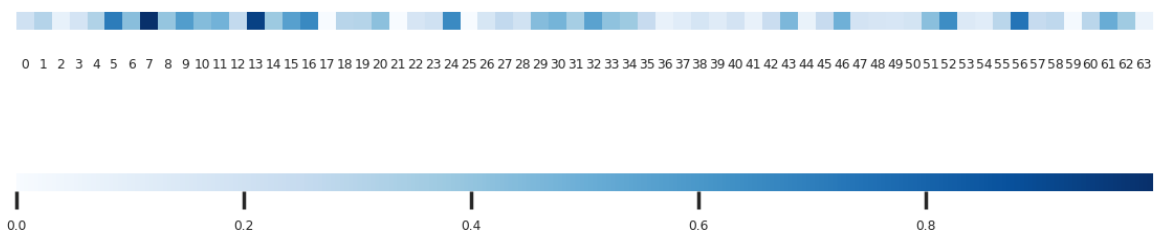
Source code snippet:

```

D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x109038	1.04331	neural-learnt	DES_encrypt1

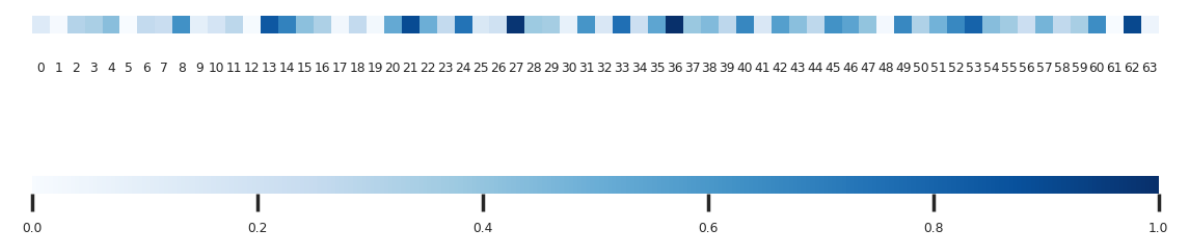
Source code snippet:

```

D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */

```

Key bit dependencies (estimated):

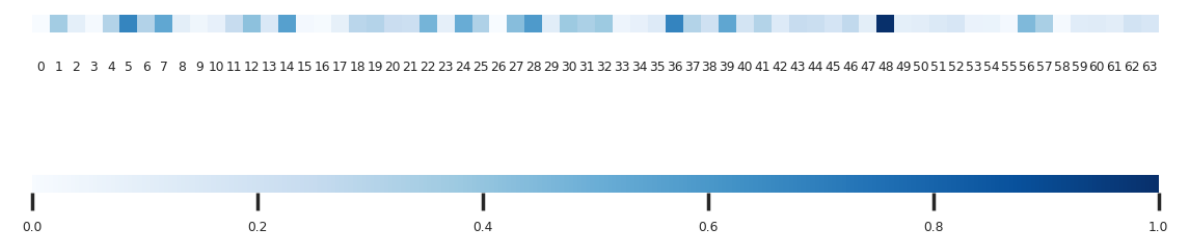


offset	MI score	Leakage model	Function
0x108f87	1.04312	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
```

Key bit dependencies (estimated):

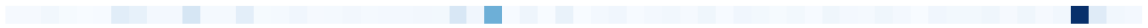


offset	MI score	Leakage model	Function
0x108331	1.04251	neural-learnt	DES_encrypt1

Source code snippet:

```
*/
if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
}
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x10864f	1.04022	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x109356	1.03899	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
D_ENCRYPT(l, r, 30); /* 16 */
D_ENCRYPT(r, l, 28); /* 15 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



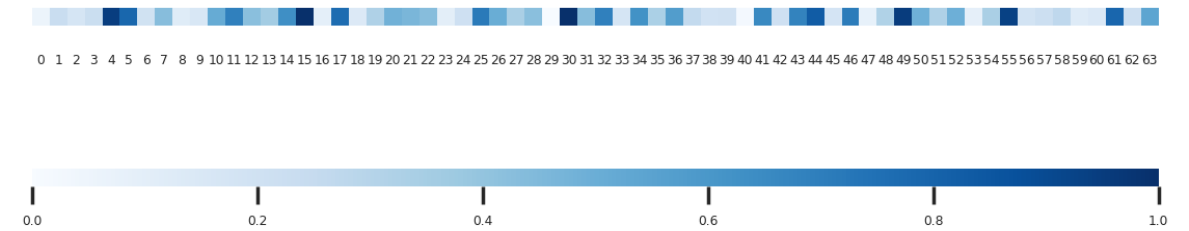


offset	MI score	Leakage model	Function
0x1092c7	1.03781	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
D_ENCRYPT(l, r, 30); /* 16 */
D_ENCRYPT(r, l, 28); /* 15 */
```

Key bit dependencies (estimated):

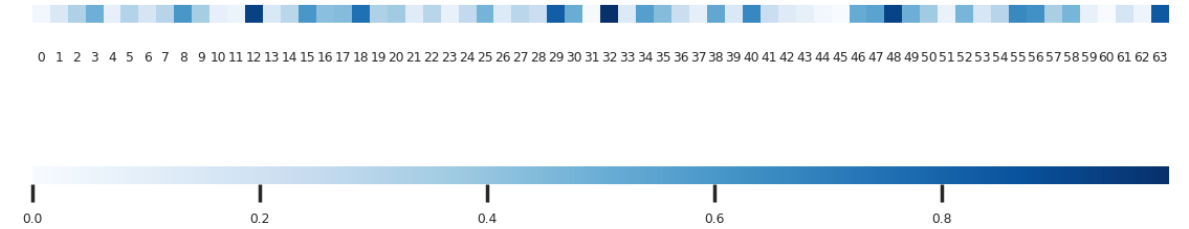


offset	MI score	Leakage model	Function
0x108bf6	1.03771	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):

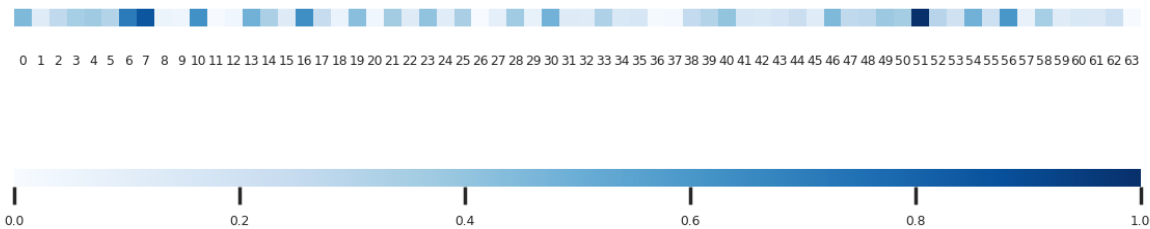


offset	MI score	Leakage model	Function
0x108c10	1.03554	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
```

Key bit dependencies (estimated):

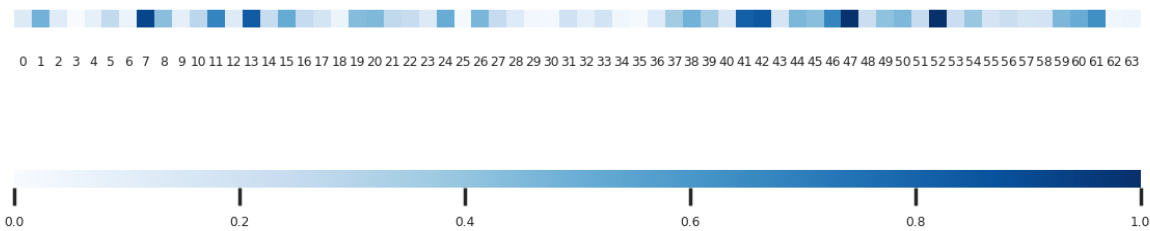


offset	MI score	Leakage model	Function
0x108b06	1.03353	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):

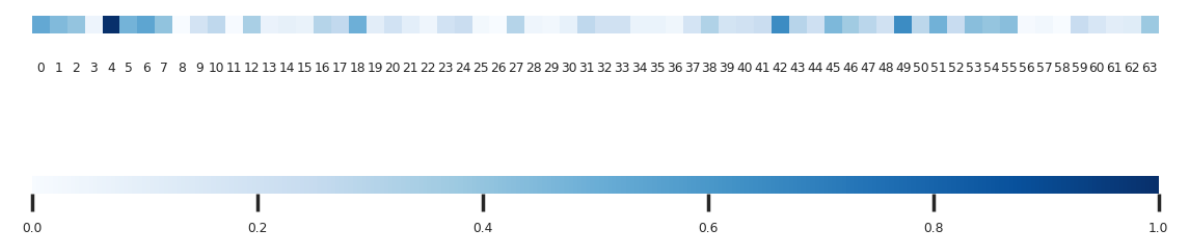


offset	MI score	Leakage model	Function
0x10924c	1.03324	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):

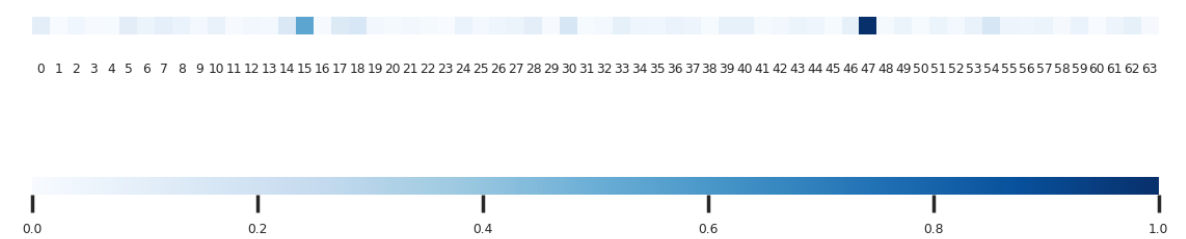


offset	MI score	Leakage model	Function
0x1082f4	1.03275	neural-learnt	DES_encrypt1

Source code snippet:

```
    */
    if (enc) {
        D_ENCRYPT(l, r, 0);    /* 1 */
        D_ENCRYPT(r, l, 2);    /* 2 */
        D_ENCRYPT(l, r, 4);    /* 3 */
        D_ENCRYPT(r, l, 6);    /* 4 */
    }
```

Key bit dependencies (estimated):

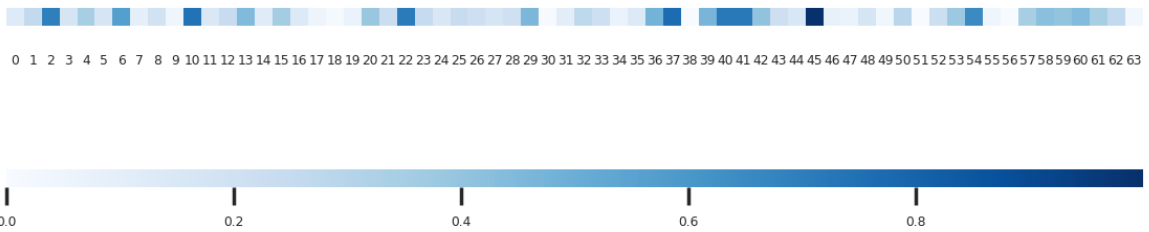


offset	MI score	Leakage model	Function
0x109128	1.02989	neural-learnt	DES_encrypt1

Source code snippet:

```
        D_ENCRYPT(r, l, 22);    /* 12 */
        D_ENCRYPT(l, r, 24);    /* 13 */
        D_ENCRYPT(r, l, 26);    /* 14 */
        D_ENCRYPT(l, r, 28);    /* 15 */
        D_ENCRYPT(r, l, 30);    /* 16 */
    } else {
```

Key bit dependencies (estimated):

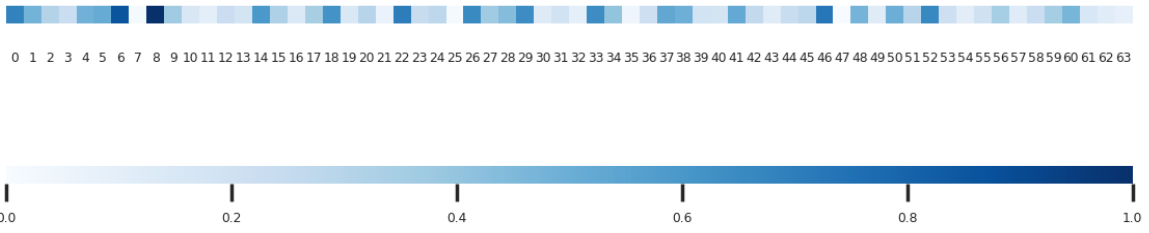


offset	MI score	Leakage model	Function
0x10857c	1.02714	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):

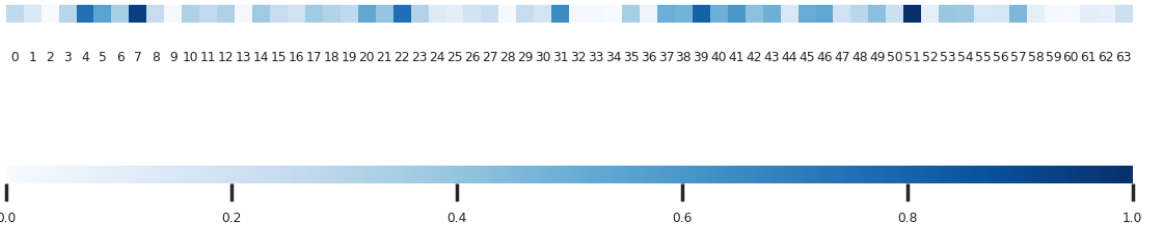


offset	MI score	Leakage model	Function
0x10933c	1.0253	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
D_ENCRYPT(l, r, 30); /* 16 */
D_ENCRYPT(r, l, 28); /* 15 */
```

Key bit dependencies (estimated):



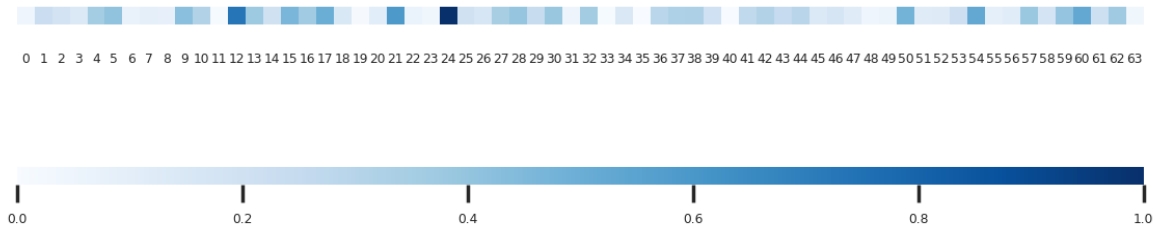


```

D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108f14	1.02027	neural-learnt	DES_encrypt1

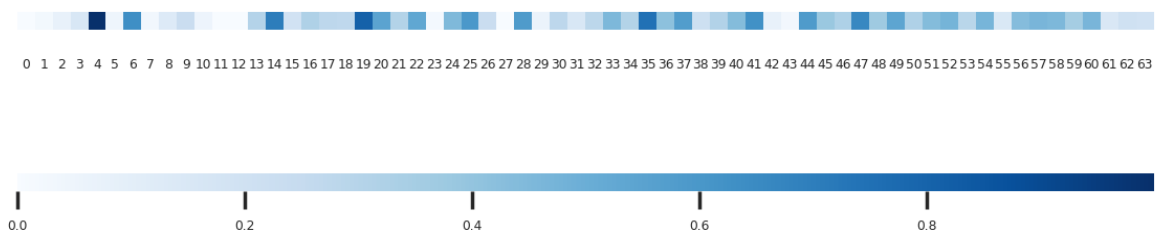
Source code snippet:

```

D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108456	1.01943	neural-learnt	DES_encrypt1

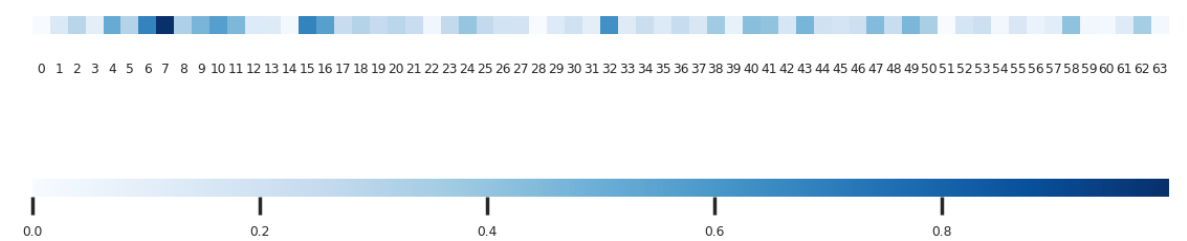
Source code snippet:

```

if (enc) {
    D_ENCRYPT(l, r, 0); /* 1 */
    D_ENCRYPT(r, l, 2); /* 2 */
    D_ENCRYPT(l, r, 4); /* 3 */
    D_ENCRYPT(r, l, 6); /* 4 */
    D_ENCRYPT(l, r, 8); /* 5 */
}

```

Key bit dependencies (estimated):

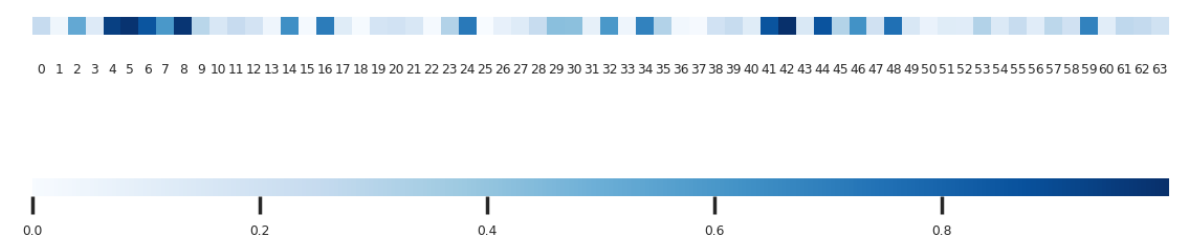


offset	MI score	Leakage model	Function
0x10931d	1.01786	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
  D_ENCRYPT(l, r, 30); /* 16 */
  D_ENCRYPT(r, l, 28); /* 15 */
}
```

Key bit dependencies (estimated):

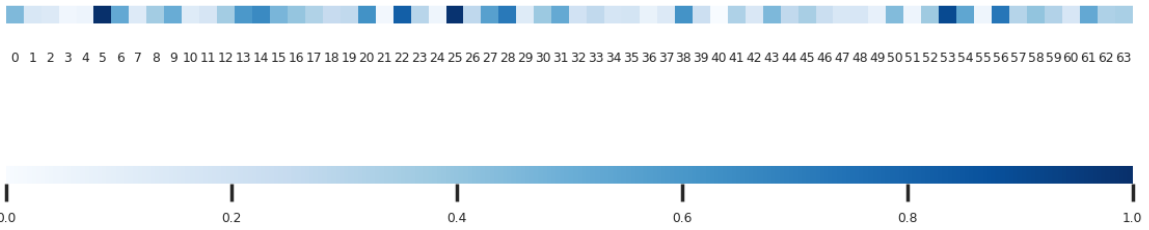


offset	MI score	Leakage model	Function
0x10887e	1.01701	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):

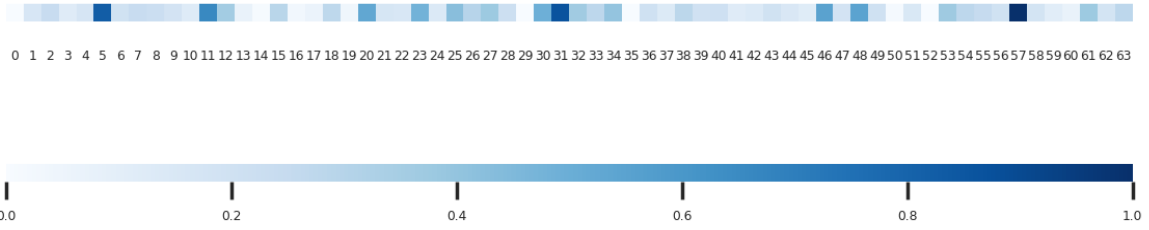


offset	MI score	Leakage model	Function
0x108863	1.01384	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):

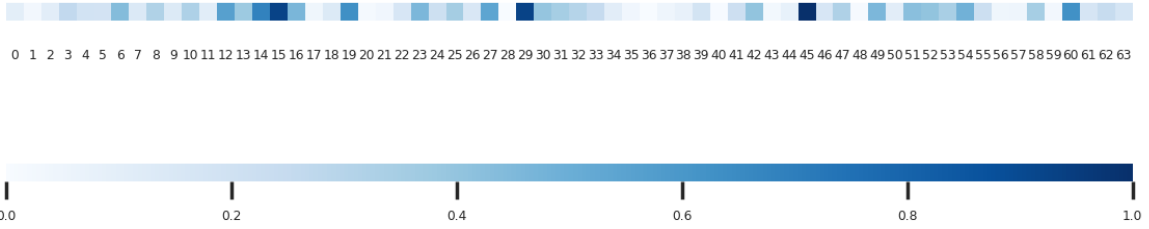


offset	MI score	Leakage model	Function
0x10871c	1.009	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):



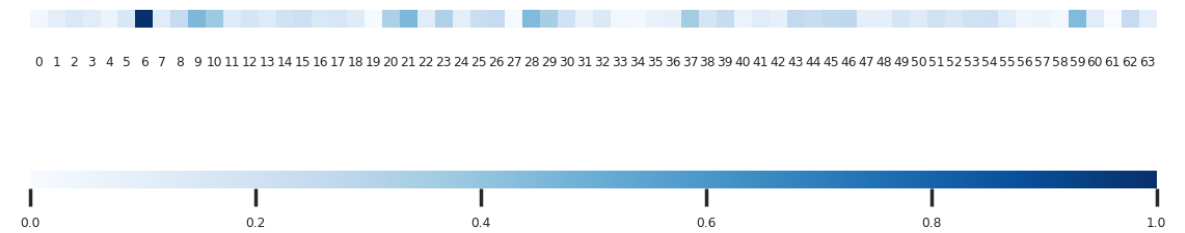


offset	MI score	Leakage model	Function
0x108612	1.00841	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
```

Key bit dependencies (estimated):

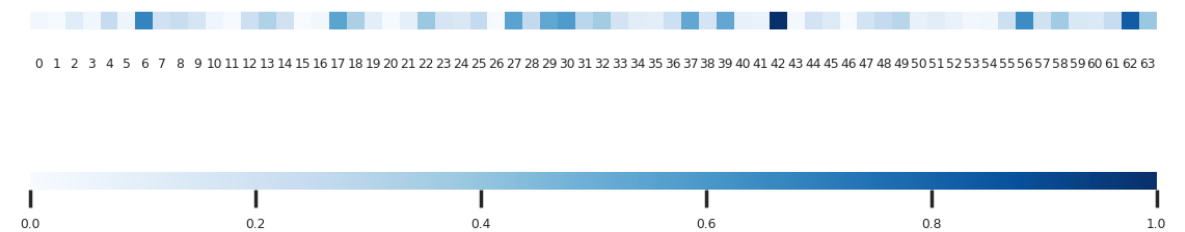


offset	MI score	Leakage model	Function
0x1091d8	1.00642	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1085d4	1.00583	neural-learnt	DES_encrypt1

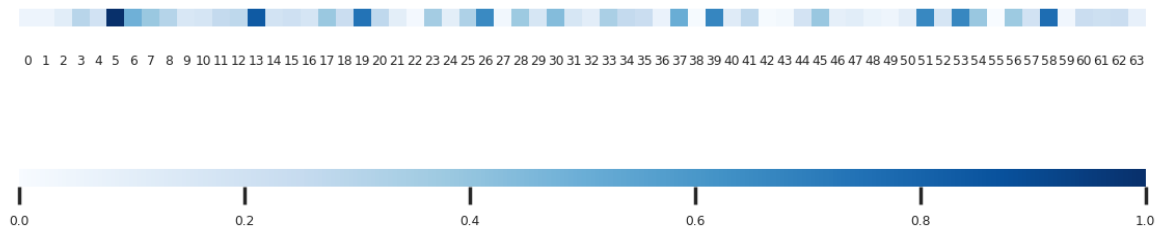
Source code snippet:

```

D_ENCRYPT(1, r, 0);    /* 1 */
D_ENCRYPT(r, 1, 2);    /* 2 */
D_ENCRYPT(1, r, 4);    /* 3 */
D_ENCRYPT(r, 1, 6);    /* 4 */
D_ENCRYPT(1, r, 8);    /* 5 */
D_ENCRYPT(r, 1, 10);   /* 6 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x1084ca	1.00201	neural-learnt	DES_encrypt1

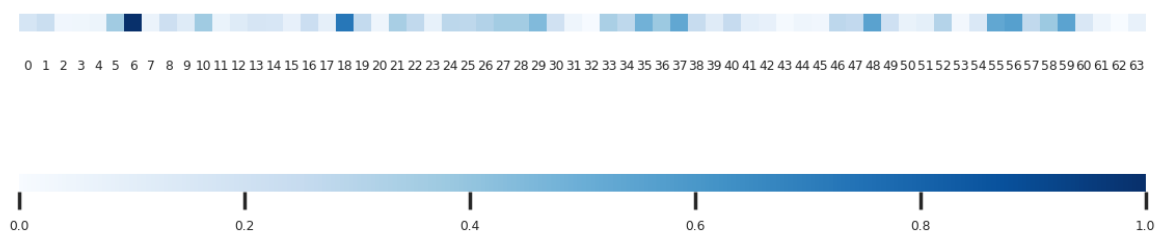
Source code snippet:

```

if (enc) {
    D_ENCRYPT(1, r, 0);    /* 1 */
    D_ENCRYPT(r, 1, 2);    /* 2 */
    D_ENCRYPT(1, r, 4);    /* 3 */
    D_ENCRYPT(r, 1, 6);    /* 4 */
    D_ENCRYPT(1, r, 8);    /* 5 */
}

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108ed6	1.00194	neural-learnt	DES_encrypt1

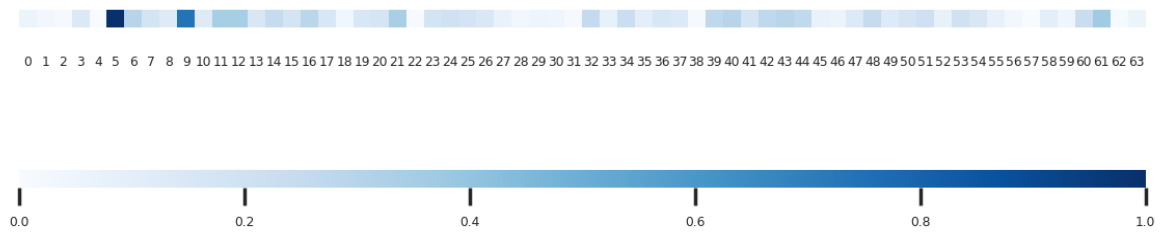
Source code snippet:

```

D_ENCRYPT(r, 1, 18);    /* 10 */
D_ENCRYPT(1, r, 20);    /* 11 */
D_ENCRYPT(r, 1, 22);    /* 12 */
D_ENCRYPT(1, r, 24);    /* 13 */
D_ENCRYPT(r, 1, 26);    /* 14 */
D_ENCRYPT(1, r, 28);    /* 15 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x109091	0.999219	neural-learnt	DES_encrypt1

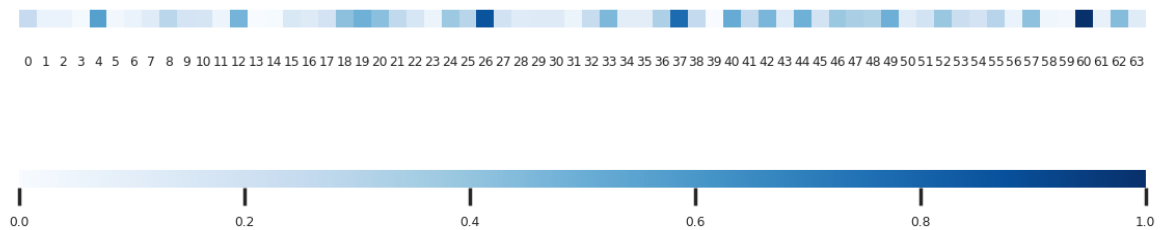
Source code snippet:

```

    D_ENCRYPT(r, l, 22);      /* 12 */
    D_ENCRYPT(l, r, 24);      /* 13 */
    D_ENCRYPT(r, l, 26);      /* 14 */
    D_ENCRYPT(l, r, 28);      /* 15 */
    D_ENCRYPT(r, l, 30);      /* 16 */
} else {

```

Key bit dependencies (estimated):

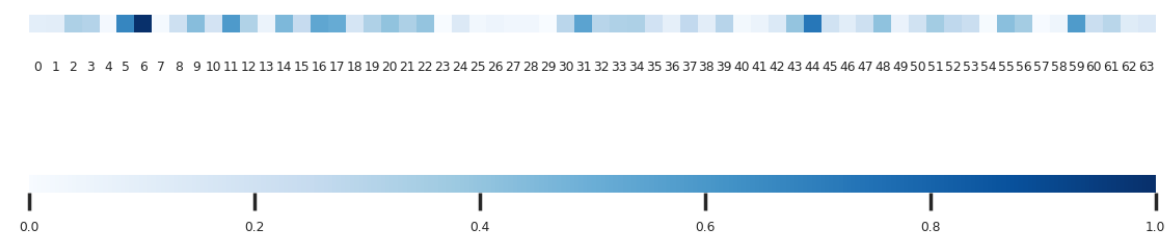


offset	MI score	Leakage model	Function
0x1089fc	0.997644	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(1, r, 8); /* 5 */
D_ENCRYPT(r, 1, 10); /* 6 */
D_ENCRYPT(1, r, 12); /* 7 */
D_ENCRYPT(r, 1, 14); /* 8 */
D_ENCRYPT(1, r, 16); /* 9 */
D_ENCRYPT(r, 1, 18); /* 10 */
```

Key bit dependencies (estimated):

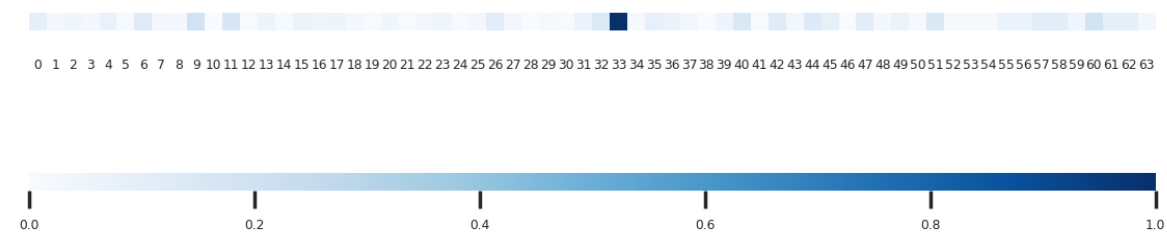


offset	MI score	Leakage model	Function
0x1083c0	0.997488	neural-learnt	DES_encrypt1

Source code snippet:

```
*/  
if (enc) {  
    D_ENCRYPT(l, r, 0);    /* 1 */  
    D_ENCRYPT(r, l, 2);    /* 2 */  
    D_ENCRYPT(l, r, 4);    /* 3 */  
    D_ENCRYPT(r, l, 6);    /* 4 */  
}
```

Key bit dependencies (estimated):

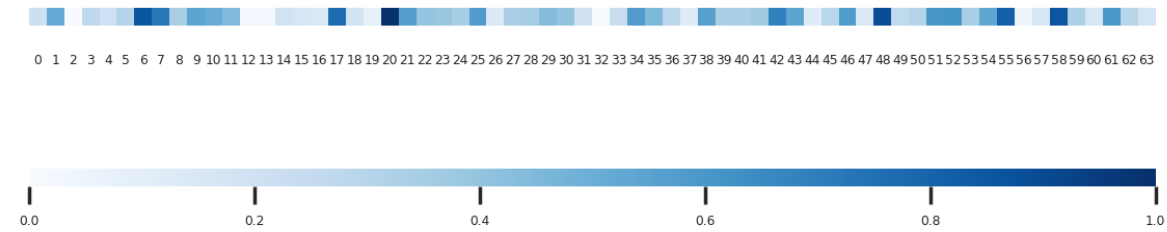


offset	MI score	Leakage model	Function
0x108a55	0.995844	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10);    /* 6 */  
D_ENCRYPT(l, r, 12);    /* 7 */  
D_ENCRYPT(r, l, 14);    /* 8 */  
D_ENCRYPT(l, r, 16);    /* 9 */  
D_ENCRYPT(r, l, 18);    /* 10 */  
D_ENCRYPT(l, r, 20);    /* 11 */
```

Key bit dependencies (estimated):

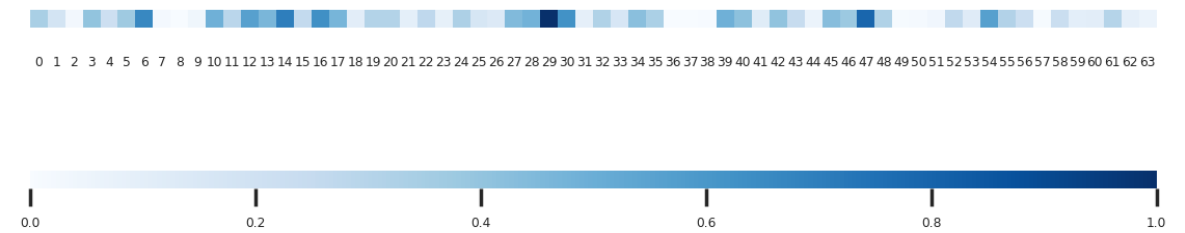


offset	MI score	Leakage model	Function
0x108523	0.992062	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):

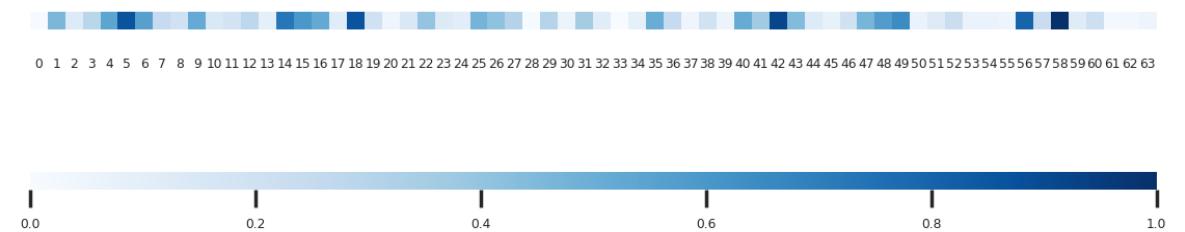


offset	MI score	Leakage model	Function
0x108560	0.987648	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 0); /* 1 */
D_ENCRYPT(r, l, 2); /* 2 */
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108d00	0.984008	neural-learnt	DES_encrypt1

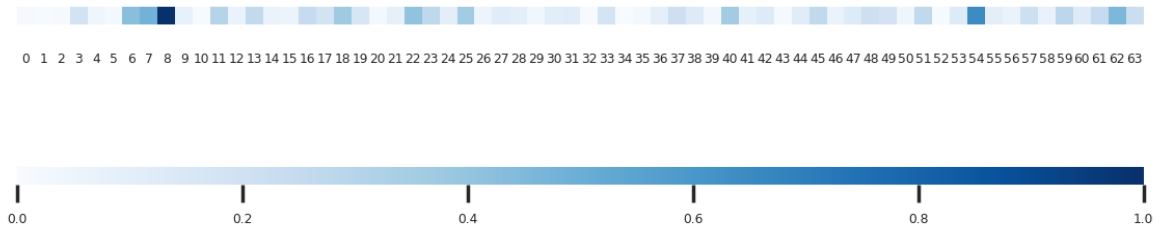
Source code snippet:

```

D_ENCRYPT(r, l, 14);    /* 8 */
D_ENCRYPT(l, r, 16);    /* 9 */
D_ENCRYPT(r, l, 18);    /* 10 */
D_ENCRYPT(l, r, 20);    /* 11 */
D_ENCRYPT(r, l, 22);    /* 12 */
D_ENCRYPT(l, r, 24);    /* 13 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108fe0	0.977914	neural-learnt	DES_encrypt1

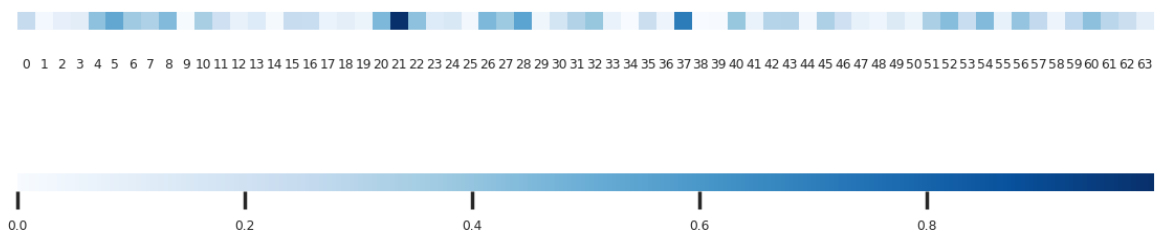
Source code snippet:

```

D_ENCRYPT(l, r, 20);    /* 11 */
D_ENCRYPT(r, l, 22);    /* 12 */
D_ENCRYPT(l, r, 24);    /* 13 */
D_ENCRYPT(r, l, 26);    /* 14 */
D_ENCRYPT(l, r, 28);    /* 15 */
D_ENCRYPT(r, l, 30);    /* 16 */

```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x108e62	0.972554	neural-learnt	DES_encrypt1

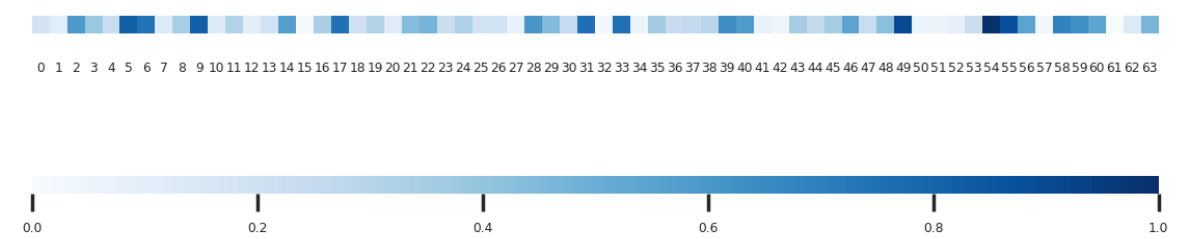
Source code snippet:

```

D_ENCRYPT(r, l, 18);    /* 10 */
D_ENCRYPT(l, r, 20);    /* 11 */
D_ENCRYPT(r, l, 22);    /* 12 */
D_ENCRYPT(l, r, 24);    /* 13 */
D_ENCRYPT(r, l, 26);    /* 14 */
D_ENCRYPT(l, r, 28);    /* 15 */

```

Key bit dependencies (estimated):

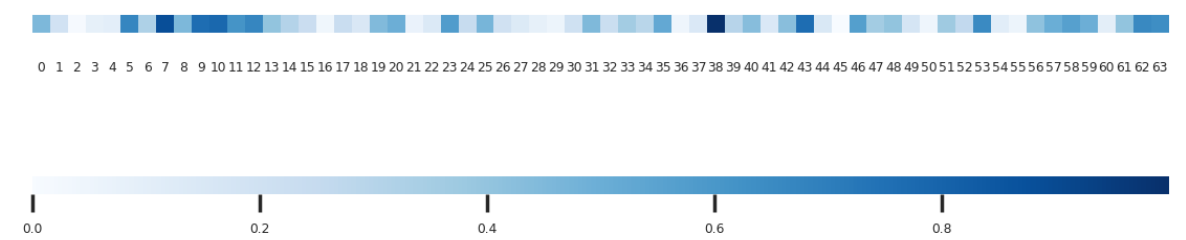


offset	MI score	Leakage model	Function
0x109232	0.972179	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):

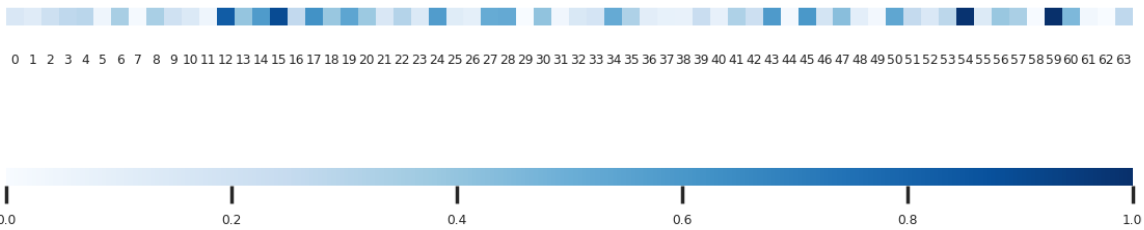


offset	MI score	Leakage model	Function
0x108a77	0.968667	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
```

Key bit dependencies (estimated):

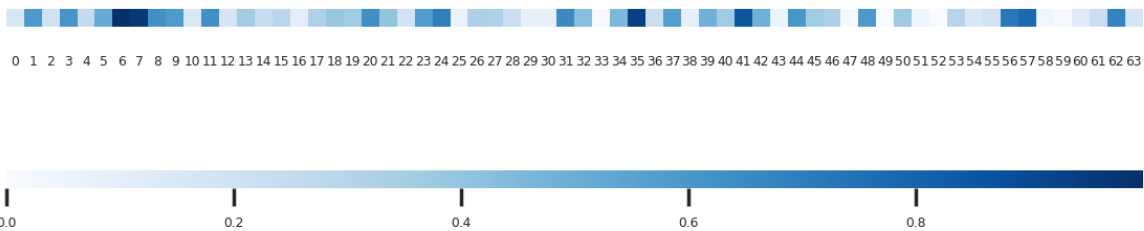


offset	MI score	Leakage model	Function
0x10889a	0.968433	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
```

Key bit dependencies (estimated):

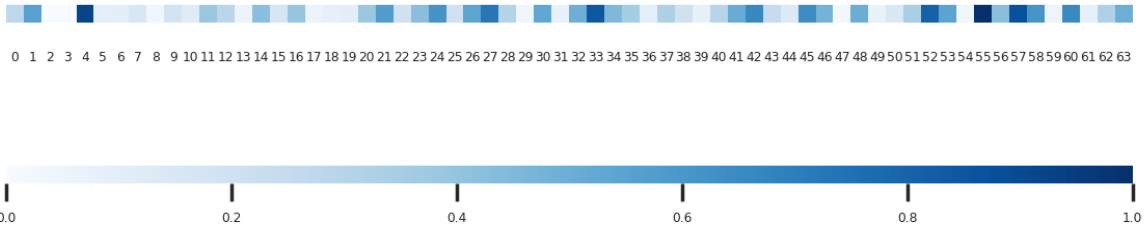


offset	MI score	Leakage model	Function
0x108eba	0.966414	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
```

Key bit dependencies (estimated):



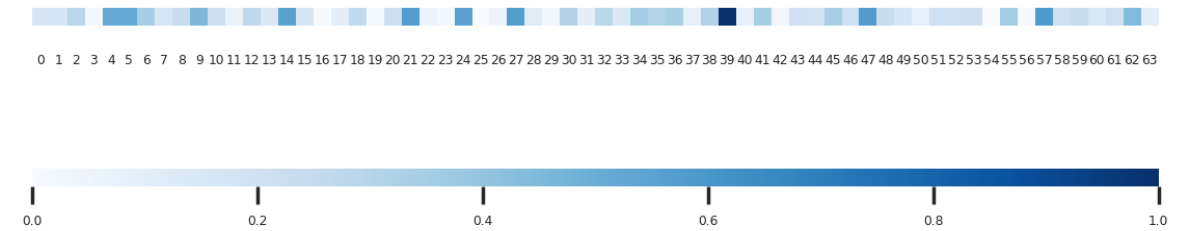


offset	MI score	Leakage model	Function
0x108cc2	0.955767	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
```

Key bit dependencies (estimated):

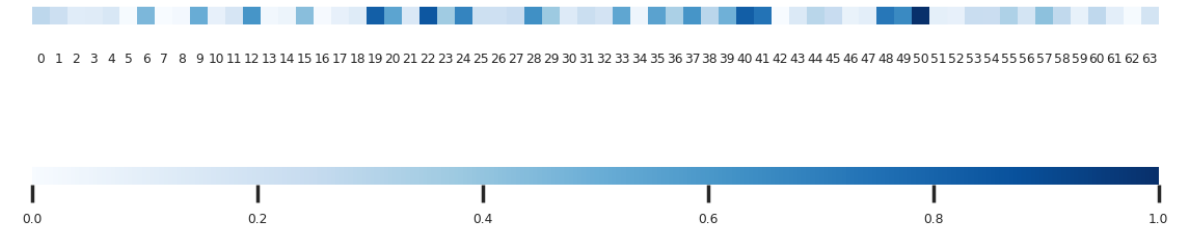


offset	MI score	Leakage model	Function
0x1091bd	0.951374	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):

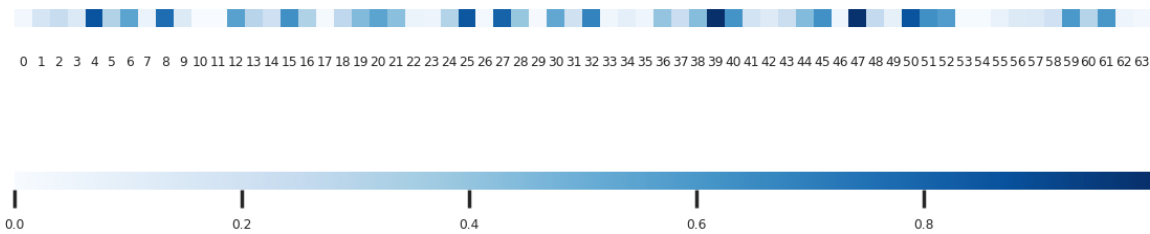


offset	MI score	Leakage model	Function
0x1089c3	0.950901	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(1, r, 8);      /* 5 */
D_ENCRYPT(r, 1, 10);     /* 6 */
D_ENCRYPT(1, r, 12);     /* 7 */
D_ENCRYPT(r, 1, 14);     /* 8 */
D_ENCRYPT(1, r, 16);     /* 9 */
D_ENCRYPT(r, 1, 18);     /* 10 */
```

Key bit dependencies (estimated):

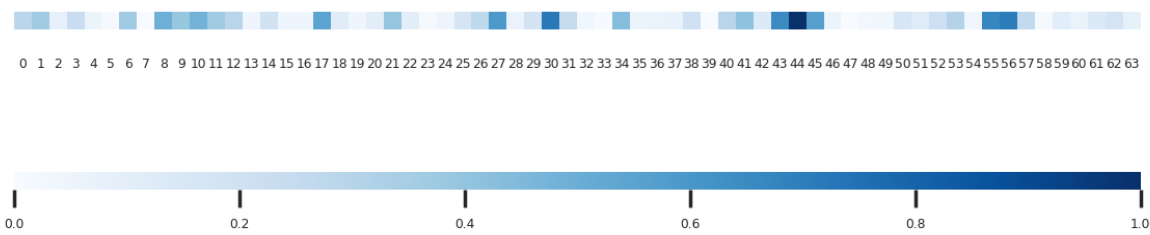


offset	MI score	Leakage model	Function
0x10859b	0.933349	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(1, r, 0);      /* 1 */
D_ENCRYPT(r, 1, 2);     /* 2 */
D_ENCRYPT(1, r, 4);     /* 3 */
D_ENCRYPT(r, 1, 6);     /* 4 */
D_ENCRYPT(1, r, 8);     /* 5 */
D_ENCRYPT(r, 1, 10);    /* 6 */
```

Key bit dependencies (estimated):

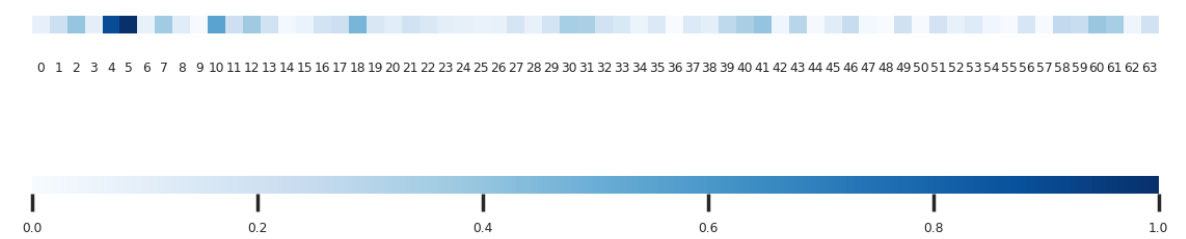


offset	MI score	Leakage model	Function
0x108aec	0.927673	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, 1, 10);     /* 6 */
D_ENCRYPT(1, r, 12);     /* 7 */
D_ENCRYPT(r, 1, 14);     /* 8 */
D_ENCRYPT(1, r, 16);     /* 9 */
D_ENCRYPT(r, 1, 18);     /* 10 */
D_ENCRYPT(1, r, 20);     /* 11 */
```

Key bit dependencies (estimated):

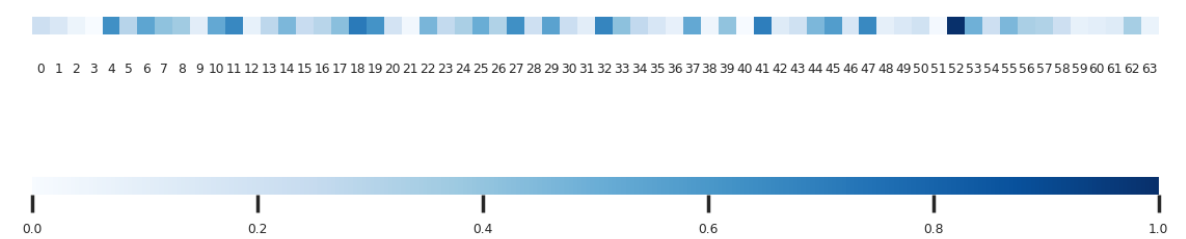


offset	MI score	Leakage model	Function
0x108790	0.890148	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):



offset	MI score	Leakage model	Function
0x109180	0.882786	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
} else {
    D_ENCRYPT(l, r, 30); /* 16 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x108c4e	0.876941	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63



offset	MI score	Leakage model	Function
0x108ce1	0.86898	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 14); /* 8 */
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
```

Key bit dependencies (estimated):



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63

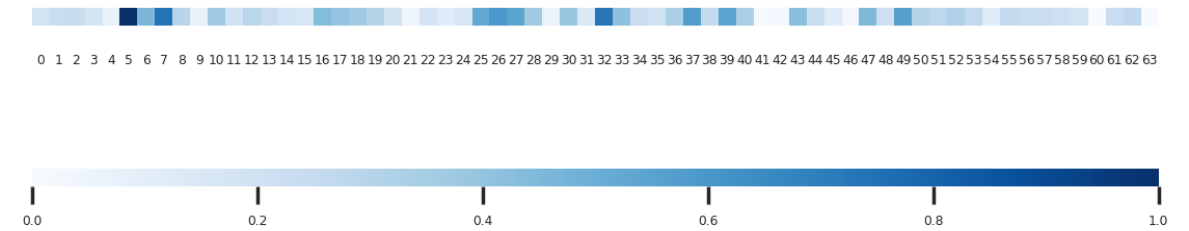


offset	MI score	Leakage model	Function
0x108fc4	0.826585	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
D_ENCRYPT(r, l, 30); /* 16 */
```

Key bit dependencies (estimated):

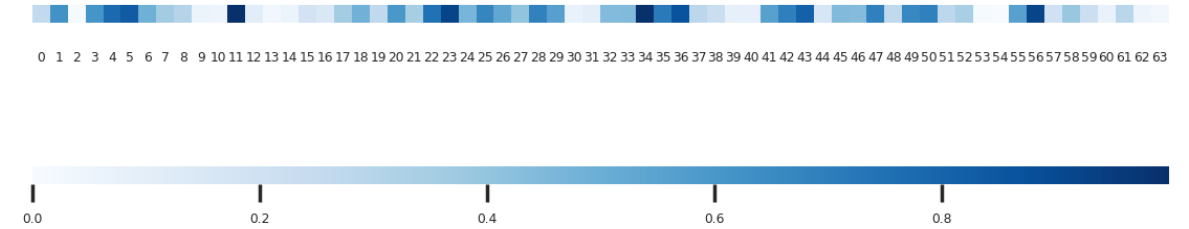


offset	MI score	Leakage model	Function
0x108dcc	0.81737	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 16); /* 9 */
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
```

Key bit dependencies (estimated):

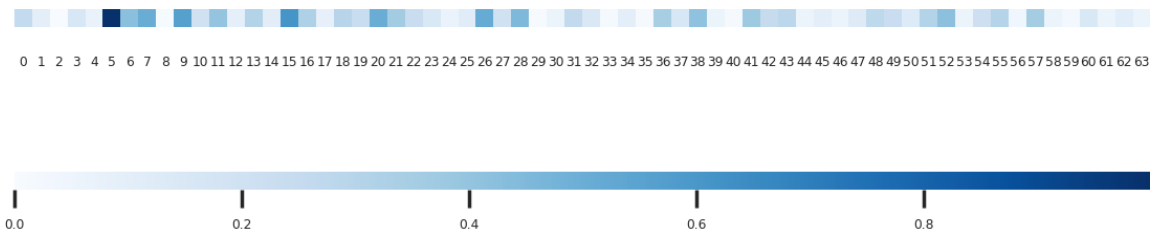


offset	MI score	Leakage model	Function
0x108e9f	0.808461	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(r, l, 18); /* 10 */
D_ENCRYPT(l, r, 20); /* 11 */
D_ENCRYPT(r, l, 22); /* 12 */
D_ENCRYPT(l, r, 24); /* 13 */
D_ENCRYPT(r, l, 26); /* 14 */
D_ENCRYPT(l, r, 28); /* 15 */
```

Key bit dependencies (estimated):

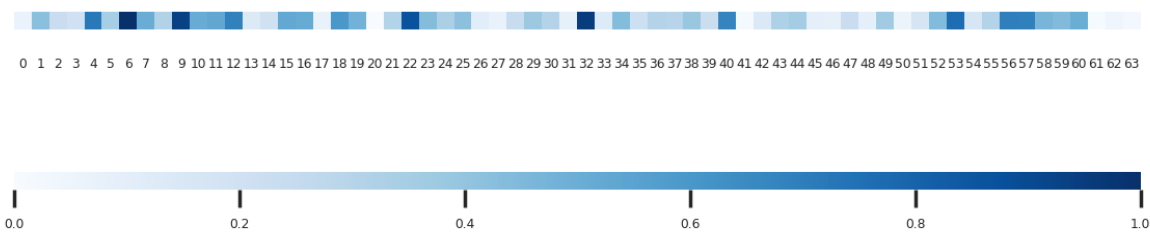


offset	MI score	Leakage model	Function
0x108759	0.74434	neural-learnt	DES_encrypt1

Source code snippet:

```
D_ENCRYPT(l, r, 4); /* 3 */
D_ENCRYPT(r, l, 6); /* 4 */
D_ENCRYPT(l, r, 8); /* 5 */
D_ENCRYPT(r, l, 10); /* 6 */
D_ENCRYPT(l, r, 12); /* 7 */
D_ENCRYPT(r, l, 14); /* 8 */
```

Key bit dependencies (estimated):



Grouped by function name

Function	Leak Count
DES_encrypt1	128
DES_set_key_unchecked	8
OPENSSL_hexchar2int	1
set_hex	1

## All Leaks (summary), sorted by MI

offset	MI score	Leakage model	Function
0x111155	1.48753	neural-learnt	DES_set_key_unchecked
0x111266	1.47854	neural-learnt	DES_set_key_unchecked
0x111181	1.44628	neural-learnt	DES_set_key_unchecked
0x1111eb	1.44279	neural-learnt	DES_set_key_unchecked
0x108387	1.41744	neural-learnt	DES_encrypt1
0x111298	1.33979	neural-learnt	DES_set_key_unchecked
0x1083a6	1.3205	neural-learnt	DES_encrypt1
0x108e0a	1.28946	neural-learnt	DES_encrypt1
0x108fa9	1.28552	neural-learnt	DES_encrypt1
0x1a9af0	1.26796	neural-learnt	OPENSSL_hexchar2int
0x11123f	1.23345	neural-learnt	DES_set_key_unchecked
0x1092a5	1.22984	neural-learnt	DES_encrypt1
0x1083fe	1.22978	neural-learnt	DES_encrypt1
0x1090ce	1.22908	neural-learnt	DES_encrypt1
0x108930	1.21887	neural-learnt	DES_encrypt1
0x1084b0	1.21441	neural-learnt	DES_encrypt1
0x11120f	1.2141	neural-learnt	DES_set_key_unchecked
0x108aae	1.21079	neural-learnt	DES_encrypt1
0x108d73	1.20173	neural-learnt	DES_encrypt1
0x108d58	1.19477	neural-learnt	DES_encrypt1
0x109076	1.18844	neural-learnt	DES_encrypt1
0x108ca6	1.18824	neural-learnt	DES_encrypt1
0x108ef5	1.18057	neural-learnt	DES_encrypt1
0x108b44	1.17905	neural-learnt	DES_encrypt1
0x108b9c	1.17222	neural-learnt	DES_encrypt1
0x10928a	1.17207	neural-learnt	DES_encrypt1
0x10919b	1.17093	neural-learnt	DES_encrypt1
0x108841	1.16688	neural-learnt	DES_encrypt1
0x10862d	1.16432	neural-learnt	DES_encrypt1
0x035720	1.16133	neural-learnt	set_hex



offset	MI score	Leakage model	Function
0x1111b1	1.15831	neural-learnt	DES_set_key_unchecked
0x1088f2	1.15831	neural-learnt	DES_encrypt1
0x1087ce	1.14497	neural-learnt	DES_encrypt1
0x1092fe	1.13991	neural-learnt	DES_encrypt1
0x108f2e	1.13856	neural-learnt	DES_encrypt1
0x109109	1.13848	neural-learnt	DES_encrypt1
0x1086de	1.13462	neural-learnt	DES_encrypt1
0x1088b9	1.13447	neural-learnt	DES_encrypt1
0x1089a4	1.13308	neural-learnt	DES_encrypt1
0x108d95	1.13199	neural-learnt	DES_encrypt1
0x108686	1.13167	neural-learnt	DES_encrypt1
0x108a92	1.13157	neural-learnt	DES_encrypt1
0x108737	1.12919	neural-learnt	DES_encrypt1
0x108a3a	1.12864	neural-learnt	DES_encrypt1
0x10834c	1.12751	neural-learnt	DES_encrypt1
0x108bd7	1.12734	neural-learnt	DES_encrypt1
0x108368	1.12592	neural-learnt	DES_encrypt1
0x10894b	1.12317	neural-learnt	DES_encrypt1
0x1089e2	1.12292	neural-learnt	DES_encrypt1
0x1085ba	1.11768	neural-learnt	DES_encrypt1
0x108545	1.1164	neural-learnt	DES_encrypt1
0x10896d	1.1135	neural-learnt	DES_encrypt1
0x108b81	1.11229	neural-learnt	DES_encrypt1
0x108e7d	1.11072	neural-learnt	DES_encrypt1
0x108c8b	1.10467	neural-learnt	DES_encrypt1
0x108deb	1.10231	neural-learnt	DES_encrypt1
0x108491	1.10055	neural-learnt	DES_encrypt1
0x1090ea	1.09956	neural-learnt	DES_encrypt1
0x1087e8	1.09706	neural-learnt	DES_encrypt1
0x10866a	1.09565	neural-learnt	DES_encrypt1

offset	MI score	Leakage model	Function
0x1092e2	1.09487	neural-learnt	DES_encrypt1
0x1088d8	1.09397	neural-learnt	DES_encrypt1
0x109213	1.09341	neural-learnt	DES_encrypt1
0x10830f	1.09251	neural-learnt	DES_encrypt1
0x1087af	1.09102	neural-learnt	DES_encrypt1
0x10843b	1.09024	neural-learnt	DES_encrypt1
0x1091f4	1.08576	neural-learnt	DES_encrypt1
0x1086c4	1.08493	neural-learnt	DES_encrypt1
0x1086a5	1.08455	neural-learnt	DES_encrypt1
0x108774	1.08076	neural-learnt	DES_encrypt1
0x108419	1.0799	neural-learnt	DES_encrypt1
0x108d1a	1.07272	neural-learnt	DES_encrypt1
0x108472	1.06632	neural-learnt	DES_encrypt1
0x108b5f	1.06573	neural-learnt	DES_encrypt1
0x108826	1.06303	neural-learnt	DES_encrypt1
0x108988	1.05855	neural-learnt	DES_encrypt1
0x10901e	1.05565	neural-learnt	DES_encrypt1
0x108508	1.05323	neural-learnt	DES_encrypt1
0x108fff	1.05262	neural-learnt	DES_encrypt1
0x108e24	1.04896	neural-learnt	DES_encrypt1
0x108bb8	1.04861	neural-learnt	DES_encrypt1
0x108acd	1.04648	neural-learnt	DES_encrypt1
0x1090b3	1.04566	neural-learnt	DES_encrypt1
0x108c69	1.04527	neural-learnt	DES_encrypt1
0x109038	1.04331	neural-learnt	DES_encrypt1
0x108f87	1.04312	neural-learnt	DES_encrypt1
0x108331	1.04251	neural-learnt	DES_encrypt1
0x10864f	1.04022	neural-learnt	DES_encrypt1
0x109356	1.03899	neural-learnt	DES_encrypt1
0x1092c7	1.03781	neural-learnt	DES_encrypt1

offset	MI score	Leakage model	Function
0x108bf6	1.03771	neural-learnt	DES_encrypt1
0x108c10	1.03554	neural-learnt	DES_encrypt1
0x108b06	1.03353	neural-learnt	DES_encrypt1
0x10924c	1.03324	neural-learnt	DES_encrypt1
0x1082f4	1.03275	neural-learnt	DES_encrypt1
0x109128	1.02989	neural-learnt	DES_encrypt1
0x10857c	1.02714	neural-learnt	DES_encrypt1
0x10933c	1.0253	neural-learnt	DES_encrypt1
0x109142	1.02291	neural-learnt	DES_encrypt1
0x108db0	1.02153	neural-learnt	DES_encrypt1
0x108f6c	1.02048	neural-learnt	DES_encrypt1
0x108f14	1.02027	neural-learnt	DES_encrypt1
0x108456	1.01943	neural-learnt	DES_encrypt1
0x10931d	1.01786	neural-learnt	DES_encrypt1
0x10887e	1.01701	neural-learnt	DES_encrypt1
0x108863	1.01384	neural-learnt	DES_encrypt1
0x10871c	1.009	neural-learnt	DES_encrypt1
0x108612	1.00841	neural-learnt	DES_encrypt1
0x1091d8	1.00642	neural-learnt	DES_encrypt1
0x1085d4	1.00583	neural-learnt	DES_encrypt1
0x1084ca	1.00201	neural-learnt	DES_encrypt1
0x108ed6	1.00194	neural-learnt	DES_encrypt1
0x109091	0.999219	neural-learnt	DES_encrypt1
0x1089fc	0.997644	neural-learnt	DES_encrypt1
0x1083c0	0.997488	neural-learnt	DES_encrypt1
0x108a55	0.995844	neural-learnt	DES_encrypt1
0x108523	0.992062	neural-learnt	DES_encrypt1
0x108560	0.987648	neural-learnt	DES_encrypt1
0x108d00	0.984008	neural-learnt	DES_encrypt1
0x108fe0	0.977914	neural-learnt	DES_encrypt1

offset	MI score	Leakage model	Function
0x108e62	0.972554	neural-learnt	DES_encrypt1
0x109232	0.972179	neural-learnt	DES_encrypt1
0x108a77	0.968667	neural-learnt	DES_encrypt1
0x10889a	0.968433	neural-learnt	DES_encrypt1
0x108eba	0.966414	neural-learnt	DES_encrypt1
0x108cc2	0.955767	neural-learnt	DES_encrypt1
0x1091bd	0.951374	neural-learnt	DES_encrypt1
0x1089c3	0.950901	neural-learnt	DES_encrypt1
0x10859b	0.933349	neural-learnt	DES_encrypt1
0x108aec	0.927673	neural-learnt	DES_encrypt1
0x108790	0.890148	neural-learnt	DES_encrypt1
0x109180	0.882786	neural-learnt	DES_encrypt1
0x108c4e	0.876941	neural-learnt	DES_encrypt1
0x108ce1	0.86898	neural-learnt	DES_encrypt1
0x108fc4	0.826585	neural-learnt	DES_encrypt1
0x108dcc	0.81737	neural-learnt	DES_encrypt1
0x108e9f	0.808461	neural-learnt	DES_encrypt1
0x108759	0.74434	neural-learnt	DES_encrypt1