**Ozel fragmentation process**

Text to be protected: “Ozel=>Privacy”

AES 256 bit key: 48 0e 05 9f 39 f7 b4 b9 81 68 4b e8 19 f1 8a d1

Encrypted text (SUN JCE): c1 15 cb 66 33 9a 87 8d c3 2d dd 63 8c 14 30 45

A single predefined finite field is always used: The tables for log and exp Galois field GF(28) are shown in hexadecimal.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **exp()** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | 01 | 02 | 04 | 08 | 10 | 20 | 40 | 80 | 1d | 3a | 74 | e8 | cd | 87 | 13 | 26 |
| **1** | 4c | 98 | 2d | 5a | b4 | 75 | ea | c9 | 8f | 03 | 06 | 0c | 18 | 30 | 60 | c0 |
| **2** | 9d | 27 | 4e | 9c | 25 | 4a | 94 | 35 | 6a | d4 | b5 | 77 | ee | c1 | 9f | 23 |
| **3** | 46 | 8c | 05 | 0a | 14 | 28 | 50 | a0 | 5d | ba | 69 | d2 | b9 | 6f | de | a1 |
| **4** | 5f | be | 61 | c2 | 99 | 2f | 5e | bc | 65 | ca | 89 | 0f | 1e | 3c | 78 | f0 |
| **5** | fd | e7 | d3 | bb | 6b | d6 | b1 | 7f | fe | e1 | df | a3 | 5b | b6 | 71 | e2 |
| **6** | d9 | af | 43 | 86 | 11 | 22 | 44 | 88 | d | 1a | 34 | 68 | d0 | bd | 67 | ce |
| **7** | 81 | 1f | 3e | 7c | f8 | ed | c7 | 93 | 3b | 76 | ec | c5 | 97 | 33 | 66 | cc |
| **8** | 85 | 17 | 2e | 5c | b8 | 6d | da | a9 | 4f | 9e | 21 | 42 | 84 | 15 | 2a | 54 |
| **9** | a8 | 4d | 9a | 29 | 52 | a4 | 55 | aa | 49 | 92 | 39 | 72 | e4 | d5 | b7 | 73 |
| **A** | e6 | d1 | bf | 63 | c6 | 91 | 3f | 7e | fc | e5 | d7 | b3 | 7b | f6 | f1 | ff |
| **B** | e3 | db | ab | 4b | 96 | 31 | 62 | c4 | 95 | 37 | 6e | dc | a5 | 57 | ae | 41 |
| **C** | 82 | 19 | 32 | 64 | c8 | 8d | 07 | 0e | 1c | 38 | 70 | e0 | dd | a7 | 53 | a6 |
| **D** | 51 | a2 | 59 | b2 | 79 | f2 | f9 | ef | c3 | 9b | 2b | 56 | ac | 45 | 8a | 09 |
| **E** | 12 | 24 | 48 | 90 | 3d | 7a | f4 | f5 | f7 | f3 | fb | eb | cb | 8b | 0b | 16 |
| **F** | 2c | 58 | b0 | 7d | fa | e9 | cf | 83 | 1b | 36 | 6c | d8 | ad | 47 | 8e | 01 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **log()** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | ff | 00 | 01 | 19 | 02 | 32 | 1a | c6 | 03 | df | 33 | ee | 1b | 68 | c7 | 4b |
| **1** | 04 | 64 | e0 | 0e | 34 | 8d | ef | 81 | 1c | c1 | 69 | f8 | c8 | 08 | 4c | 71 |
| **2** | 05 | 8a | 65 | 2f | e1 | 24 | 0f | 21 | 35 | 93 | 8e | da | f0 | 12 | 82 | 45 |
| **3** | 1d | b5 | c2 | 7d | 6a | 27 | f9 | b9 | c9 | 9a | 09 | 78 | 4d | e4 | 72 | a6 |
| **4** | 06 | bf | 8b | 62 | 66 | dd | 30 | fd | e2 | 98 | 25 | b3 | 10 | 91 | 22 | 88 |
| **5** | 36 | d0 | 94 | ce | 8f | 96 | db | bd | f1 | d2 | 13 | 5c | 83 | 38 | 46 | 40 |
| **6** | 1e | 42 | b6 | a3 | c3 | 48 | 7e | 6e | 6b | 3a | 28 | 54 | fa | 85 | ba | 3d |
| **7** | ca | 5e | 9b | 9f | 0a | 15 | 79 | 2b | 4e | d4 | e5 | ac | 73 | f3 | a7 | 57 |
| **8** | 07 | 70 | c0 | f7 | 8c | 80 | 63 | 0d | 67 | 4a | de | ed | 31 | c5 | fe | 18 |
| **9** | e3 | a5 | 99 | 77 | 26 | b8 | b4 | 7c | 11 | 44 | 92 | d9 | 23 | 20 | 89 | 2e |
| **A** | 37 | 3f | d1 | 5b | 95 | bc | cf | cd | 90 | 87 | 97 | b2 | dc | fc | be | 61 |
| **B** | f2 | 56 | d3 | ab | 14 | 2a | 5d | 9e | 84 | 3c | 39 | 53 | 47 | 6d | 41 | a2 |
| **C** | 1f | 2d | 43 | d8 | b7 | 7b | a4 | 76 | c4 | 17 | 49 | ec | 7f | 0c | 6f | f6 |
| **D** | 6c | a1 | 3b | 52 | 29 | 9d | 55 | aa | fb | 60 | 86 | b1 | bb | cc | 3e | 5a |
| **E** | cb | 59 | 5f | b0 | 9c | a9 | a0 | 51 | 0b | f5 | 16 | eb | 7a | 75 | 2c | d7 |
| **F** | 4f | ae | d5 | e9 | e6 | e7 | ad | e8 | 74 | d6 | f4 | ea | a8 | 50 | 58 | af |

Assuming we want to force a minimum of 4 (M) to be required of a possible (N) 8 fragments the following 4\*8 Vandermonde matrix is generated:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 0 | 0 | 0 |  |
|  | 1 | 1 | 1 | 1 |  |
|  | 1 | 2 | 4 | 8 |  |
|  | 1 | 4 | 10 | 40 |  |
|  | 1 | 8 | 40 | 3a |  |
|  | 1 | 10 | 1d | cd |  |
|  | 1 | 20 | 74 | 26 |  |
|  | 1 | 40 | cd | 2d |  |

Using Forward Error Correction (FEC) the following identity matrix is generated:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 0 | 0 | 0 |  |
|  | 0 | 1 | 0 | 0 |  |
|  | 0 | 0 | 1 | 0 |  |
|  | 0 | 0 | 0 | 1 |  |
|  | 77 | 40 | 38 | 0e |  |
|  | c7 | A7 | 0d | 6c |  |
|  | 53 | 2 | 6f | 3f |  |
|  | f1 | 7b | 83 | 08 |  |

For the example we use a small packet size of 8, it practice a larger block oriented fragment size would be used. The AES key and the encrypted text are then distributed into the following matrix:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 48 | 0e | 05 | 9f | c1 | 15 | cb | 66 |  |
|  | 39 | f7 | b4 | b9 | 33 | 9a | 87 | 8d |  |
|  | 81 | 68 | 4b | e8 | c3 | 2d | dd | 63 |  |
|  | 19 | f1 | 8a | d1 | 8c | 14 | 30 | 45 |  |

Multiplying the FEC identity matrix and the encrypted text matrix results in the following fragmentation matrix, where each row represents a fragment to be distributed.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 48 | 0e | 05 | 9f | c1 | 15 | cb | 66 |  |
|  | 39 | f7 | b4 | b9 | 33 | 9a | 87 | 8d |  |
|  | 81 | 68 | 4b | e8 | c3 | 2d | dd | 63 |  |
|  | 19 | f1 | 8a | d1 | 8c | 14 | 30 | 45 |  |
|  | 02 | 54 | bc | e3 | 06 | 52 | bd | 29 |  |
|  | 8a | eb | 5b | 2a | 3c | 06 | 0a | dd |  |
|  | 52 | 8c | 36 | c2 | bb | a9 | df | 91 |  |
|  | 34 | 3e | 07 | 95 | a6 | cc | 10 | 9f |  |

Note: Using the FEC identity matrix approach for fragmentation combined with the AES key being distributed in the binary data, does by definition mean all fragments could allow deriving 1/Mth of the AES key. This reduces the effective strength of the AES key used. Selecting larger values for M will reduce this impact.