```
1  using System.Linq;
2  using AES3_EDE_Lib;
3
4  namespace AES3StreamCipher
5  {
6      class ANSIX9_17PRNG
7      {
8          private AES3_EDE aes3;
9
10         private byte[] ULongToBytes(ulong u)
11         {
12             byte[] b = new byte[8];
13
14             b[0] = (byte)((u >> 56) & 0xFFul);
15             b[1] = (byte)((u >> 48) & 0xFFul);
16             b[2] = (byte)((u >> 40) & 0xFFul);
17             b[3] = (byte)((u >> 32) & 0xFFul);
18             b[4] = (byte)((u >> 24) & 0xFFul);
19             b[5] = (byte)((u >> 16) & 0xFFul);
20             b[6] = (byte)((u >> 8) & 0xFFul);
21             b[7] = (byte)(u & 0xFFul);
22
23             return b;
24         }
25
26         private byte[] ULongsToBytes(int count, ulong[] u)
27         {
28             byte[] ba = new byte[8 * count];
29
30             for (int i = 0; i < count; i++)
31             {
32                 byte[] b = ULongToBytes(u[i]);
33
34                 for (int j = 0; j < 8; j++)
35                     ba[8 * i + j] = b[j];
36             }
37
38             return ba;
39         }
40
41         private byte[] XOR(byte[] b1, byte[] b2)
42         {
43             byte[] r = new byte[16];
44
45             for (int i = 0; i < 16; i++)
46                 r[i] = (byte)(b1[i] ^ b2[i]);
47
48             return r;
49         }
50
51         public byte[] Generate(
52             int m,
```

```
53              ulong[] ukey_0,
54              ulong[] ukey_1,
55              ulong[] ukey_2,
56              ulong[] udateI,
57              ulong[] useeds,
58              out int count)
59          {
60              byte[] X = new byte[16 * m];
61              byte[] bkey_0 = ULongsToBytes(4, ukey_0);
62              byte[] bkey_1 = ULongsToBytes(4, ukey_1);
63              byte[] bkey_2 = ULongsToBytes(4, ukey_2);
64              byte[] bdatei = ULongsToBytes(2, udateI);
65              byte[] bseeds = ULongsToBytes(2, useeds);
66
67              aes3 = new AES3_EDE(bkey_0, bkey_1, bkey_2, 8, 14, 8, 14, 8, 14);
68
69              byte[] I = aes3.Cipher(bdatei);
70              byte[] s = bseeds.ToArray();
71              byte[] x = null;
72
73              for (int i = 0; i < m; i++)
74              {
75                  x = aes3.Cipher(XOR(I, s));
76                  s = aes3.Cipher(XOR(x, I));
77
78                  for (int j = 0; j < 16; j++)
79                      X[16 * i + j] = x[j];
80              }
81
82              count = 16 * m;
83              return X;
84          }
85      }
86  }
```