

Implement a program—e.g., as given by the following program Problem2.java—that outputs the plaintext produced by encrypting each plaintext message X, then decrypting the resulting ciphertext Y.

```
public class Problem2 {
    public static void main(String[] argv) throws java.io.IOException {
        byte[] x = new byte[16];
        byte[] z = new byte[16];

        System.in.read(z);
        AES aes = new AES(z);

        while (System.in.read(x) != -1)
            System.out.write(aes.decrypt(aes.encrypt(x)));
    }
}
```

- 3 The following ciphertext file Problem3.out contains a stream of 8-bit bytes, shown as hexadecimal numbers. The first 24 bytes constitute a 192-bit secret key Z, and the remaining bytes are partitioned into 16-byte ciphertext messages Y.

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

```

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

```

[...]

```

dc bc 7a f7 b3 2f 15 c3 01 d8 e4 06 ec e4 6b 62 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 55 1a e8 91 e3 50 ef 8f
34 86 9a 50 19 0b d5 88 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 5f b7 ac 0b 9b 16 30 6e 94 58 f1 ea 98 00 b4 f1 09 98 7b 1d 24 d9 73 2c
de 88 bb 1a 86 d7 86 7d 2a 07 a7 e1 67 fc a6 f1 79 09 f5 61 06 20 37 3b 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 35 9a d3 de 5f a3 6c 57 13 b3 3a a5 de 08 eb 03 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
37 72 f2 66 ad 49 cd ad d9 2c b6 21 c5 41 8f 62 5d 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 1e ed e0 5b a9 fa d1 48 17 4c 52 4c 94 28 de 52
ac 0d e1 2e aa 39 60 9b 47 44 73 19 e9 24 85 63 d3 50 31 83 47 ef f8 cf b6 5a 52 1b a9 2f d2 93 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 2d bf fb 9f 12 f1 0c 60 ee a6 cf c5 6e 9a 25 16 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f e3 d2 df 56 f3 ff 29 64 e3 ec 08 9d 44 fd 6a 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
53 d4 bc 34 67 7e e3 05 72 94 78 30 5c 02 94 f1 a6 26 49 8b 1d 08 44 06 39 9d f5 24 ef 68 64 62 a7 5f 60 d3 8d 5a 07 2f
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 14 3c 72 22 4a 52 92 2c a9 2d f6 3b a2 ed b0 60
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
9d 07 e8 99 72 a7 14 24 6d 18 a9 2f e2 f1 e0 18 20 c6 f1 8a 28 8b 5a b7 91 bb 42 3d 84 97 41 f7 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 1e 79 ce 16 2a 64 d9 20
d6 fb 99 29 e3 62 90 21 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 7b b8 04 e0 c2 a4 e9 d5 01 40 51 b9 75 66 b7 88
3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0
f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4 3f 5b 99 e0 c0 1b 28 e0 f5 44 b3 22 93 70 c2 f4
96 9e 4b 0e 0a 4e 12 0b 28 ca 57 d8 0e db 5c 0d

```

Implement a program—e.g., as given by the following program Problem3.java—that outputs the plaintext X produced by decrypting each ciphertext message Y.

```

public class Problem3 {
    public static void main(String[] argv) throws java.io.IOException {
        byte[] y = new byte[16];
        byte[] z = new byte[24];

        System.in.read(z);
        AES aes = new AES(z);

        while (System.in.read(y) != -1)
            System.out.write(aes.decrypt(y));
    }
}

```