MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Advent Challenge – Part 3

Author: Anna Lena Rotthaler

December 2017

Challenge (1/3)

Lisa doesn't get along very well with her stepmother Maud. She constantly gets the impression that Maud is trying to get between her and her father.
When the two of them do a Diffie-Hellman key exchange in order to communicate only encrypted from now on, Lisa is suspicious and tape-records the messages.

Moreover, she knows that her father uses only the digits 4 and 7 in all of his passwords.
She also knows that the message that follows the key exchange is encrypted with AES in ECB mode and PKCS7 padding. The MD5 hash of the shared Diffie-Hellman key is used as the key for AES.

Challenge (2/3)

Stepmother to father: p = 151303, g = 86813

Father to stepmother: 48507

Stepmother to father: 23919

Stepmother to father: 86 B8 31 2D 26 F4 9E A7 2A 92 85 DE EA 1C 93 8E 8F A8 2A 00 6F E1 D8 19 52 25 E7 F6 A5 6C 7D 06 85 7B 9C D6 36 46 6D D5 03 CB 05 14 71 00 BB 11 D4 F6 39 5D FB 8F C7 8C EB CC 0C 6C 94 67 61 CC 3E 6B FF 6F 76 66 6E C2 14 27 5D 6E 5B 6A 84 9A 50 8E 6E 3B B4 CC 37 7C AF 82 A1 37 1F 6B C7 14 4C 19 D8 7C 48 28 9D 84 1E 43 E3 95 56 99 A5 C4

Challenge (3/3)

Unfortunately, Lisa is a lame duck at maths. Can you help her to compute the shared key of her father and her stepmother and to decrypt the message?

Hint: Her stepmother is not stupid, too, and put it deliberately mystical in her message. What shall be Lisa's present for Christmas?

Please enter the solution (one word) in capital letters.