

Forum:[Hack Forums](#)

Thread: [AES 256 puzzle](#)

timbermat - May 18, 2018, 4:28 pm

Hi people

I'm working on a challenge and would value your input.

We've been given a base64 encoded message that we believe is the output of AES encryption.

We've been told that the message did not use IVs.

We know that the key is 32 ascii characters long. We have been given a 16 digit number and an 8 digit number. We have to work out the other 8 digits

For the given key length, I'm guessing it's been encoded with AES 256. Given there's no IVs, I think that narrows AES modes to ECB or CTR.

I've written a code in python to cycle through the remaining 8 digits and try the key. I've tested the code and it works. But when using the supplied encoded message, I get no outputs that you can read. I've tried reordering the key to all possible combinations and still get nothing legible.

I've tried doing all this in ECB and CTR mode and still nothing.

Anyone got any ideas? Anything I might have overlooked or just plain got wrong?

Kernel - May 20, 2018, 9:45 am

It's ECB. If it were CTR, you would need to supply a nonce.

Quote:I've written a code in python to cycle through the remaining 8 digits and try the key. I've tested the code and it works.

How do you know it works? Did you get a readable output?

timbermat - May 20, 2018, 10:02 am

(May 20, 2018 09:45 AM)Kernel Wrote: [\[CITE\]](#) It's ECB. If it were CTR, you would need to supply a nonce.

How do you know it works? Did you get a readable output?

Hi. Yes, I tested it with a known message encrypted using AES in ECB mode, with a know numeric keyword. Managed to get a readable output.

so to that end, i'm wondering if I've missed something in he original description of the puzzle.