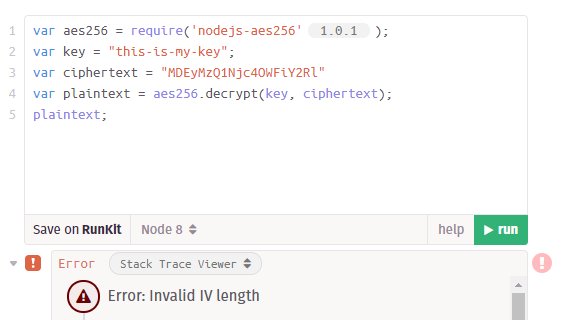
# Elf Web Access--Encryption Gone Wrong Part 4, The Break-in

## Question 1, 2

If we put a string of 15 bytes into ciphertext, it generates an error. (One ASCII character is one byte.)





A string of 17 bytes generates a Unicode character, and different strings generate different characters. Not much help there.





A string of 16 bytes generates an empty string.





Repeated tests show that \*any\* 16-byte string generates an empty string. Now try a different key.



So, any 16-byte string generates a plaintext that is an empty string, “”, no matter what the key. We can use MDEyMzQ1Njc4OWFiY2RlZg== as our ciphertext and leave the plaintext as an empty string.

## Question 3

How can we break into the EWA server? Inject our specially crafted cookie, of course!

## The Break-in

Use the web developer tools in your browser to edit the EWA cookie to match what we’ve just learned. Remember that the name value must be a valid account on the EWA server, in the format the server expects.

## Question

What is the title (or SHA1 hash, if you prefer) of the Great Book Page you find in EWA emails?