Krypto 2 - ingara

Task 1)

DES was submitted by IBM to the NBS after they had opened for proposals of an encryption algorithm to be used by the government.
The NBS consulted the NSA, and the algorithm used in the DES standard adopted by the US government had been modified with undisclosed
changes as well as having a reduced key length. This led to much skepticism toward the security of the algorithm and the potential
of backdoors.

In contrast, the election of the AES was an open process that anyone could submit a proposal to and/or participate in the evaluation
of the submitted proposals. Of 15 initial submissions, 5 were picked for further analysis, and and the final choice for the algorithm
landed on Rijndael, developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. People were surprised that this algorithm
was chosen because the creators were unknown in the international community and not members of established academic or industrial
organizations.

Task 2 a)
A:
x1 xor'd with K1:
000000010011001101000101011001111000100110101011110011011110111100000001001000110100
01010110011110001001101010111100110111101111

x2 xor'd with K1
0000000100000001101000101011001111000100110101011110011011110111100000001001000110100
01010110011110001001101010111100110111101111

In regards to diffusion, xor is terrible, as only two bits are different.

B:
Affine encoding for x1:
FEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Affine encoding for x2:
FDFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Affine encoding only changed the digit that was different, meaning it has worse diffusion than xor

C:
1 round of AES on x1:
01fcf41f4c13eaaa96747c97c49b6222

1 round of AES on x2:
19fcf41f4c13eaaa96747c97c49b6222

Only the two left-most digits differ after one round of AES, so the same as xor.

D:
Full AES of x1:
0694267ba398480c6b2b9f649be476cb

Full AES of x2:
282f7b11019800f8a978c6f750827ab5

This time only 3 digits are the same. It's impossible to tell if there is a pattern as to which values are changed from just one sample. This is much much better than the preceding methods.

Task 2 b)
A:
x1 xor K1:
0000000100110011010001010110011110001001101010111100110111101111000000010010001101000
1010110011110001001101010111100110111101111

x1 xor K2:
0001000100110011010001010110011110001001101010111100110111101111000000010010001101000
1010110011110001001101010111100110111101111

1 bit is different

B:
Affine encoding for x1 with K1:
FEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Affine encoding for x1 with K2:
FEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

They are identical

C:
1 round of AES on x1 with K1 as the key:
01fcf41f4c13eaaa96747c97c49b6222

1 round of AES on x1 with K2 as the key:
b8fcf41f5c13eaaa86747c97d49b6222

Two hex digits are different, which means 8 bits are different.

D:
Full AES on x1 with K1 as the key:
0694267ba398480c6b2b9f649be476cb

Full AES on x1 with K2 as the key:

7af49a8defad94fa27cb03ac9f1c149a

29 hex digits are different, which means 116 bits are different.

Task 3)

What is the mathematical term for a one-to-one correspondence?

The term is bijective.

What is the name for the best single-key attack against AES?

biclique

matrix2bytes:

crypto{inmatrix}

add_round_key:

crypto{r0undk3y}

sbox:

crypto{l1n34rly}

diffusion:

crypto{d1ffUs3R}

all_together:

crypto{MYAES128}