① ciphertext "vealrunwgwwk"
key "DAWN"

process:

D A W N
3 0 22 13

v e a l r u w g w w k
21, 4, 0, 11, 17, 20, 22, 6, 22, 22, 10
− 3, 0, 22, 13, 3, 0, 22, 13, 3, 0, 22
+26 +26 +26 +26
18, 4, 4, 24, 14, 20, 0, 19, 19, 22, 14
s e e y o u a T T w o

See you at two!

(2)

there are 8 bits used for parity bit, so if we change them it won't influence the encryption/decryption. So, as long as we used up all other bits, we can guarantee 2 new keys will encrypt same ciphertext. So after 2^{56} keys. the rest $2^8 \Rightarrow 256$ keys will result into same text.

③. I believe faster, more specifically 2x faster computer will help more for attacker than good guy in theory, since it will cut down more time for key exhaustive search,

but, ~~practt~~ practically, I believe 2x faster won't be enough for attackers to see a difference. AES has security attacks ~~to~~ strength of 2^{128-1} and no successful attack so far, 2^{56} already require more than a thousand years. half the time indeed make it more promising, but not practically realistic for now.

④.

(message ⊕ message) ⊕ key

= (message ⊕ key) ⊕ (message ⊕ key).

the property can be understand in a different way.

$(m_1 \oplus m_2) \oplus key = (m_1 \oplus key) \oplus (m_2 \oplus key)$

$m_1 \oplus m_2$: new text, C_3

$m_1 \oplus key$: encryption with known text 1, C_1

$m_2 \oplus key$: encryption with known text 2, C_2.

now what we have is pairs like

$m_1 - c_1$ (we choose to known them)

$m_2 - c_2$

$m_3 - c_3$

$\vdots$

$m_{128} - c_{128}$.

using the formula, if we form $c_1 \oplus c_2 = c_3$ 2 ciphertext XOR into another ciphertext that we also know, then we can know that the original text for hacking is just $m_1 \oplus m_2$,

To make sure we can garentee to ~~the~~ c_2 ~~we can~~ find a pair of ciphertext 1 & 2 for any given ciphertext 3, considering C_3 is obtained by $c_1 \oplus c_2$.

we let, C_1 be 1, 0, 0, 0, ...

C_2 be 0, 1, 0, 0, ...

C_3 be 0, 0, 1, 0 ....

⋮

C_{128} be 0, 0, 0, ... 0, 0, 1

In this case, any cipher text can be ⊕ by 2 or more cipher texts that we know.

ex. ciphertext : 1, 1, 0, 0, ... 0

$= C_1 \oplus C_2 = 1,0,0,0 \oplus 0,1,0,0 \ldots$

$= 1, 1, 0, 0, \ldots 0.$

so message is just $m_1 \oplus m_2$

ex. cipher text. 1, 1, 1, 0, 0, ... 0.

$= C_1 \oplus C_2 \oplus C_3$

we will focus on $C_1 \oplus C_2$ first, create

$C_m = C_1 \oplus C_2 = 1, 1, 0, 0 \ldots \Leftarrow m_m = m_1 \oplus$

$C_{final} = C_m \oplus C_3 \Leftarrow m_m \oplus m_3 = (m_1 \oplus m_2) \oplus m_3$

1, 1, 0, 0, 0,
0, 0, 1, 0, 0. ⇒ 1, 1, 1, 0, 0, 0