Problem 3. «HAS01»

Bob is a beginner cryptographer. He read an article about the new hash function HAS01 (see a description here). Bob decided to implement the HAS01 function in order to use it for checking the integrity of messages being forwarded. However, he was inattentive and made a mistake during the implementation. In the function f_1, he did not notice the sign «'» in the variable a and used the following set of formulas:

```
for $i = 0$ to $7$ do
    for $j = 0$ to $6$ do
        $a_{(i+1) \bmod 8,j} \leftarrow \mathrm{SBox}(((a_{i,j} \oplus a_{(i+1) \bmod 8,j}) \ll 3) \oplus ((a_{i,j+1} \oplus a_{(i+1) \bmod 8,j+1}) \gg 5))$
    end for
    $a_{(i+1) \bmod 8,7} \leftarrow \mathrm{SBox}(((a_{i,7} \oplus a_{(i+1) \bmod 8,7}) \ll 3) \oplus ((a_{i,0} \oplus a_{(i+1) \bmod 8,0}) \gg 5) \oplus 7)$
end for
```

Q1 Prove that Bob's version of the hash function is cryptographically weak.

Q2 Find a collision to the following message (given in hexadecimal format):
`3165203938203362203236203437203163203738203865 20`.

The test set value for the original HAS01 hash function is given here.
The test set value for Bob's implementation is given here.