Security in IT

Daniel Lobato García – 100277139

Basica optional
a)I have chosen AOLAQUETHLESTAS? and HOLAQUETALESTAS? because just swapping the letters corresponding to the first byte of a block the result must be identical.

Desplazamiento optional
a)
b)Initializing the hash value to 0s is not a good option to increase the security of the hash, because the first block will assign all of its values to the 'first' hash value, making the hash function more vulnerable to a prefix collision attack.
c)If you are using ASCII representation, the values that each of the bytes will take will vary between 0 and 127, so this will not affect the rest of the question.
shift+XOR will be repeated 8 times in order to create the hash using this function. If the initial hash was public, the problem is that it would be easy to find a message that produces that very same initial hash and hence the security of the hashing would be compromised.

Encadenada optional
a)If DES is removed from the compression function, the hashing function is much more likely to produce collisions, as XOR is a fairly simple procedure.

Collisions:

XORBasica - 20 bytes
N�mero total de entradas: 2244709
N�mero total de entradas con colisiones (n�mero de coincidencias > 1): 105509 (4.700342004241975%)
N�mero total de colisiones encontradas: 565998

XORBasica - 255 bytes
N�mero total de entradas: 176055
N�mero total de entradas con colisiones (n�mero de coincidencias > 1): 810 (0.4600834966345745%)
N�mero total de colisiones encontradas: 825

XORDesplazamiento - 20 bytes
N�mero total de entradas: 2244709
N�mero total de entradas con colisiones (n�mero de coincidencias > 1): 104247 (4.644120908322638 5%)
N�mero total de colisiones encontradas: 563868

XORDesplazamiento - 255 bytes
N�mero total de entradas: 176055
N�mero total de entradas con colisiones (n�mero de coincidencias > 1): 810 (0.4600834966345745%)
N�mero total de colisiones encontradas: 825

Encadenada - 20 bytes
N&#65533;mero total de entradas: 2244709
N&#65533;mero total de entradas con colisiones (n&#65533;mero de coincidencias > 1): 103901 (4.6287068836094125%)
N&#65533;mero total de colisiones encontradas: 562971

Encadenada - 255 bytes
The message size is too long. Encadenada has to add the length of the message and since 255 is not a multiple of 8, this would result on a message of more than 256 bytes, unabling the function to hash it.

The figures show a slight improvement from the most basic function to the less basic. Nevertheless, before running the tests I thought that the performance of Encadenada would
be significantly better than the rest, and the figures show that it actually is not that better. A surprising fact was that the collisions are the same for 255 byte blocks in XORBasica
and XORDesplazamiento. However, the latter function improves around 0.06 the results of the number of entries with more than one collision.