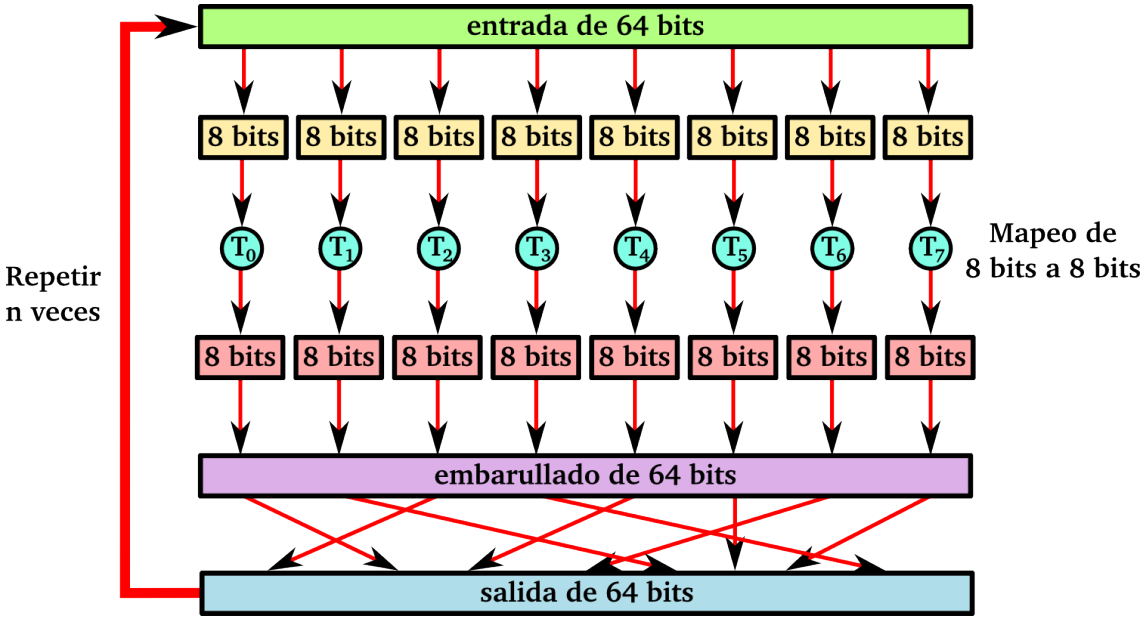
P3 – Considere un sistema de cifrado polialfabético con dos alfabetos distintos. Un ataque con texto en claro seleccionado que es capaz de obtener la codificación del texto en claro del mensaje “Es extraño mojar queso en la cerveza o probar whisky de garrafa”, ¿será suficiente para decodificar todos los mensajes? ¿Por qué?

Every letter in the alphabet appears in the phrase “Es extraño mojar queso en la cerveza o probar whisky de garrafa.” Given this phrase in a chosen plaintext attack (where the attacker has both the plain text, and the ciphertext), the Caesar cipher would be broken - the intruder would know the ciphertext character for every plaintext character. However, the Vigenere cipher does not alway translate a given plaintext character to the same ciphertext character each time, and hence a Vigenere cipher would not be immediately broken by this chosen plaintext attack.

P4 – Considere el cifrado de bloque de la siguiente figura.



Suponga que cada cifrado de bloque Ti simplemente invierte el orden de los 8 bits de la entrada (11110000 → 00001111). Suponga además que el vector de aleatorización no modifica ningún bit.

a) con n=3 y siendo la entrada original 8 bloques iguales 10100000, cuál es el valor de salida?
b) Y si la entrada fuese 7 bloques 10100000 y un bloque 10100001?
c) Repita a) y b), suponiendo que la función de aleatorización invierte el orden de los 64bits.

(a) The output is equal to 00000101 repeated eight times.

(b) The output is equal to 00000101 repeated seven times + 10000101.

(c) We have $(A^R B^R C^R)^R$ = CBA, where A, B, C are strings, and R means inverse operation. Thus:

1. For (a), the output is 10100000 repeated eight times;

2. For (b), the output is 10100001 + 10100000 repeated seven times.

P5)

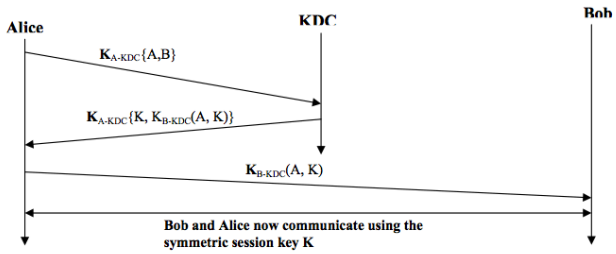
(a) There are 8 tables. Each table has 2^8 entries. Each entry has 8 bits.
number of tables * size of each table * size of each entry = $8*2^{8*}$ $8= 2^{14}$ bits

(b) There are 2^{64} entries. Each entry has 64 bits. 2^{71} bits

P8)

p = 5, q = 11
(a) n = p*q = 55, z = (p-1)(q-1) = 40
(b) e = 3 is less than n and has no common factors with z.
(c) d = 27
(d) m = 8, m^e = 512, Ciphertext c= m^e mod n = 17

P10)



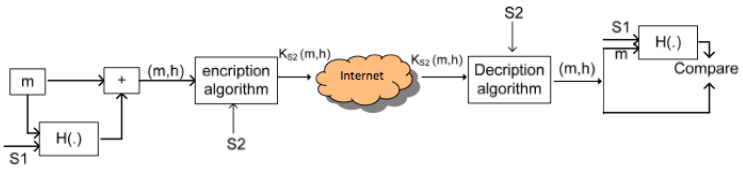
P11)

The message

I	O	U	1
9	0	.	9
0	B	O	B

has the same checksum

P12)



P13)

The file is broken into blocks of equal size. For each block, calculate the hash (for example with MD5 or SHA-1). The hashes for all of the blocks are saved in the .torrent

file. Whenever a peer downloads a block, it calculates the hash of this block and compares it to the hash in the .torrent file. If the two hashes are equal, the block is valid. Otherwise, the block is bogus, and should be discarded.

P14

Digital signatures require an underlying Public Key Infrastructure (PKI) with certification authorities. For OSPF, all routers are in a same domain, so the administrator can easily deploy the symmetric key on each router, without the need of a PKI.