1) Crittografia Simmetrica e funzione hash

K = chiave crittografica

M = messaggio diviso in blocchi di ugual lunghezza $(M_1, \dots, M_n)$

H = funzione hash

$$H(M_1) = E(K, M_1)$$

$$H(M_1 M_2 \dots M_i M_{i+1}) = E(K, H(M_1 \dots M_i) \oplus M_{i+1}) \quad \text{per } i = 1, \dots, n-1$$

$$H(A_1 A_2) = E(K, E(K, A_1) \oplus A_2)$$

$$H(B_1 B_2) = E(K, E(K, B_1) \oplus B_2)$$

Quindi è sufficiente trovare un blocco B_2 che:

$$E(K, B_1) \oplus B_2 = E(K, A_1) \oplus A_2$$

$$B_2 = E(K, B_1) \oplus E(K, A_1) \oplus A_2$$

Quindi se $B_2 = E(K, B_1) \oplus E(K, A_1) \oplus A_2$ allora $H(B_1 B_2) = H(A_1 A_2)$ per qualunque valore di A_i, A_2 e B_1, quindi H non è weak collision.

- Crittografia

Si sostituisce ogni lettera dell'alfabeto "m" con "(am+b) mod 26"
dove la chiave è data da K = <a,b> con "a" e "b" interi [0,25]

- Dimostra che se "a" e 26 non sono relativamente primi allora lo schema non è utilizzabile.

Se "a" e "26" hanno divisori in comune
allora lo schema non è utilizzabile:

Se K<2,0> → "a" non è relativamente primo con 26

Un numero si dice relativamente primo se non hanno nessun divisore in comune.

$m_1 = = 0$ coincide con $m_2 = 13$ ciò significa che la funzione di cifratura non è invertibile e quindi non è sempre univocamente possibile risalire al plaintext.

- Grittografia