3 Hash Functions

Consider the following Hash Function H defined by the recurrence:

 $H_i = H_{i-1} \oplus E(M_i, H_{i-1})$

where M_i is a message block, H_i is its corresponding hash block and H_0 is some initial value (which can be selected arbitrarily by the attacker). The output digest of a message is then defined as:

 $H(M_1||M_2||\dots,||M_N)=H_N$

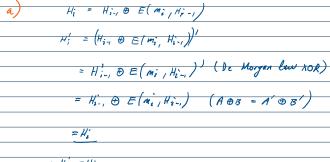
Let E be DES encryption scheme. DES has Complementarity Property, where means that if Y = E(K, X), then Y' = E(K', X'). A' is such that the 0s in A are replaced by 1 and vice versa.

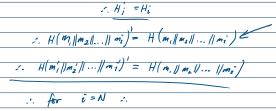
- 1. Use this property to find a collision for message $M_1||M_2||\dots||M_N$. (Marks \longrightarrow 10)
- 2. Show that a similar attack succeeds for the recurrence:

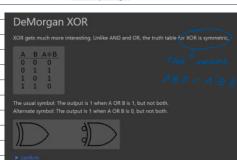
 $H_i = M_i \oplus E(H_{i-1}, M_i)$

(Marks 5) Total marks :15

Property	EXPRESSION 1	EXPRESSION 2
Absorption	A+A*B=A	A * (A + B) = A
Adjacency	A * B + A * B'= A	(A + B) * (A + B') = A
Associative	A+(B+C)+(A+B)+C	A*(B*C)=(A*B)*C
Commutative	A+8=8+A	A * B = B * A
Complement	A+A'=1	A * A' = 0
Consensus	(A * X) + (A' * Y) + (X * Y) = (A * X) + (A' * Y)	(A + X) * (A' + Y) * (X + Y) = (A + X) * (A' + Y)
DeMorgan	(A + B)' = A' * B'	(A * B)' = A' + B'
Distributive	A*(B+C)=A*B+A*C	A+B*C=(A+B)*(A+C)
Idempotency	A+A=A	A*A=A
Identity	A+0=A	A*1=A
Involution	(A')' = A	
Null	A+1=1	A*0=0
Simplification	A+A'B=A+B	A* (A'+8) = A* B







 M_i is a message block and M_i is its hash. Let E be DES encryption scheme. DES has Complementarity Property, where means that if Y = E(K, X), then $Y^i = E(K', X') A'$ is such that the Qs in A are replaced by 1 and vice versa.

1. Use this property to find a collision for blocks M_1, M_2, \cdots, M_N . (Marks 10)

Show that a similar attack succeeds for

 $H_i = M_i \oplus E(H_{i-1}, M_i)$

 $H_N' = H_N$

(Marks 5) Total marks :15

b) ②. $H_{i}^{'} = \begin{bmatrix} M_{i} \oplus E(H_{i-1}, M_{i}) \end{bmatrix}'$ $= M_{i} \oplus E(H_{i-1}, M_{i})' \quad (XOK De Morgan law)$ $= M_{i}^{'} \oplus E(H_{i-1}, M_{i}^{'}) \quad (DES complementary property)$ $= M_{i}^{'} \oplus E(H_{i-1}, M_{i}^{'}) \quad (XOR A B B = A' \oplus B')$ $\vdots \quad H_{i}^{'} = H_{i}^{'}$ Thus taking XOR of M still permits $\underline{Cdleston} \quad H_{i}^{'} = H_{i}^{'}$