Assignment I: Q3

Friday, 27 June 2025 00:27

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:

$$H(M_1 || M_2 || \ldots || M_N) = H_N$$

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 $M_1 || M_2 || \ldots || M_N$. (Marks 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 + B = B + 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' + B) = A * B

Table 2.21: Properties of algebra

DeMorgan XOR

XOR gets much more interesting. Unlike AND and OR, the truth table for XOR is symmetric.

This means $A \oplus B = A' \oplus B'$

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

The usual symbol: The output is 1 when A OR B is 1, but not both.

Alternate symbol: The output is 1 when A OR B is 0, but not both.

▸ confirm

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

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

$= H_{i-1}' \oplus E(m_i, H_{i-1})'$ (De Morgan law XOR)

$= H_{i-1}' \oplus E(m_i', H_{i-1}')$ $(A \oplus B = A' \oplus B')$

$= H_i$

$\therefore H_i' = H_i$

$\therefore H(m_1 || m_2 || \ldots || m_i)' = H(m_1 || m_2 || \ldots || m_i)$

$\therefore H(m_1' || m_2' || \ldots || m_i')' = H(m_1 || m_2 || \ldots || m_i)$

$\therefore$ for $i = N$ $\therefore$

$H_N' = H_N$

M_i is a message block and H_i is its hash. 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 blocks $M_1, M_2, \cdots, M_N$. (Marks 10)
2. Show that a similar attack succeeds for

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

(Marks 5)

Total marks :15

b) ② . $H_i' = [M_i \oplus E(H_{i-1}, M_i)]'$

$= M_i' \oplus E(H_{i-1}, M_i)'$ (XOR De Morgan law)

$= M_i' \oplus E(H_{i-1}', M_i')$ (DES complementary property)

$= M_i \oplus E(H_{i-1}, M_i)$ (XOR $A \oplus B = A' \oplus B'$)

$\therefore H_i' = H_i$

Thus taking XOR of M still permits collision $H_i' = H_i$