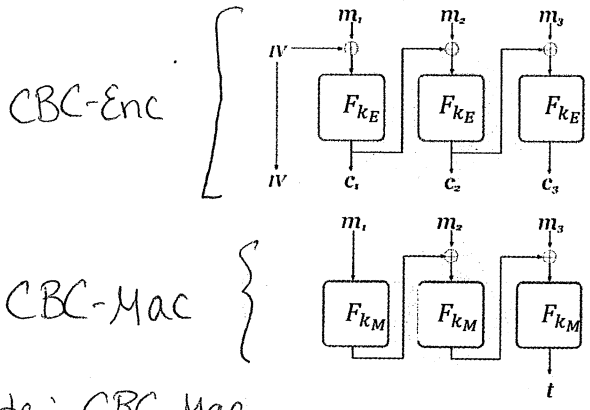
Solutions

Class Exercise—Authenticated Encryption
ENEE 457/CMSC 498E
11/01/17

Consider the following approaches for combining CBC-ENC with CBC-MAC. For each one, explain why the approach is insecure. I.e. each approach will either compromise message privacy or message authentication/integrity. In both cases, assume that we are trying to construct a fixed-length authenticated encryption scheme were it is known that all messages will consist of exactly three blocks.

1. Run CBC-ENC and CBC-MAC in parallel on the message m:

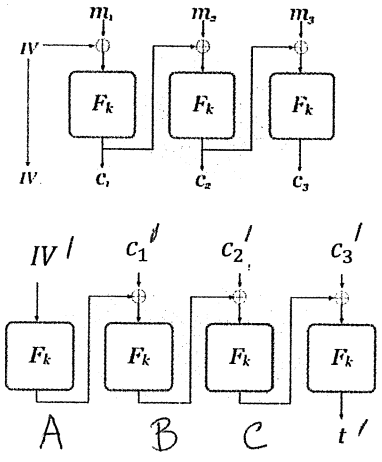


Output: (IV, c_1, c_2, c_3, t)

note: CBC-Mac is deterministic

To break CPA security query m_0, get back (c_0, t_0).
Now submit (m_0, m_1) to the challenger.
Get back (c^*, t^*).
If $t^* = t_0$, output $b' = 0$
o/w output $b' = 1$
The attacker always guesses correctly.

2. First run CBC-ENC, then run CBC-MAC on the ciphertext, but use the *same* key for both.



Output: (IV, c_1, c_2, c_3, t)

To break Unforgeability:
query (m_1, m_2, m_3).
Get back (IV, c_1, c_2, c_3, t).
Now we know the following about F_K:
1. $F_K(IV \oplus m_1) = c_1$
2. $F_K(c_1 \oplus m_2) = c_2$
3. $F_K(c_2 \oplus m_3) = t$

lots of possible variations.

We will choose (IV', c_1', c_2', c_3') such that all values of A, B, C, t' are known.
This means that $(IV', c_1', c_2', c_3', t')$ breaks unforgeability.
1. Set $IV' = IV \oplus m_1$ then $A = c_1$
2. Set $c_1' = c_1 \oplus c_2 \oplus m_3$ $B = c_3$
3. set $c_2' = c_1 \oplus m_2 \oplus c_3$ $C = c_2$
4. set $c_3' = IV \oplus m_1 \oplus c_2$; $t' = c_1$