Below there are two problems. Please think about them BEFORE the exam on Feb 4. The problems should focus your attention so that you do some research instead of just browsing the notices...

MK

PROBLEM 1.

Below I attach a description of CCM authenticated encryption mode. We have discussed GCM mode (and its weaknesses). CCM is a much better choice.

Read the description of CCM (or maybe in the web with a more detailed description) and find an answer to the following questions:

question 1: is it possible to extend the ciphertext with a new block? After decryption the last block might be garbage, but we aim just to pass the authentication test.

question 2: would it be ok to replace the definition of C by the following one:

$C := (T \oplus S_0)||(P \oplus \mathrm{MSB}_{Plen}(S))$?

CCM encryption mode, just to avoid patent threats (triggered by request to patent OCB mode - patented in USA, exempt for general public license for non-commertial use)

Prerequisites: block cipher algorithm; key K; counter generation function; formatting function; MAC length $Tlen$

Input: nonce N; payload P of $Plen$ bits; valid associated data A

Computation: Steps:

1. formatting applied to (N, A, P), result: blocks $B_0, ..., B_r$
2. $Y_0 := \mathrm{Enc}_K(B_0)$
3. for $i = 1$ to r: $Y_i := \mathrm{Enc}_K(B_i \oplus Y_{i-1})$
4. $T := \mathrm{MSB}_{Tlen}(Y_r)$
5. generate the counter blocks $\mathrm{Ctr}_0, \mathrm{Ctr}_1, ..., \mathrm{Ctr}_m$ for $m = Plen/128$
6. for $j = 0$ to m: $S_j := \mathrm{Enc}_K(\mathrm{Ctr}_j)$
7. $S := S_1||...||S_m$
8. $C := (P \oplus \mathrm{MSB}_{Plen}(S))||\,(T \oplus S_0)$

Decryption:

1. return INVALID, if $Clen < Tlen$
2. generate the counter blocks $\mathrm{Ctr}_0, \mathrm{Ctr}_1, ..., \mathrm{Ctr}_m$ for $m = Plen/128$
3. for $j = 0$ to m: $S_j := \mathrm{Enc}_K(\mathrm{Ctr}_j)$
4. $S := S_1||...||S_m$
5. $P := \mathrm{MSB}_{Clen}(C) \oplus \mathrm{MSB}_{Plen}(S)$
6. $T := \mathrm{LSB}_{Tlen}(C) \oplus \mathrm{MSB}_{Tlen}(S_0)$
7. If N, A or P invalid, then return INVALID, else reconstruct $B_0, ..., B_r$
8. recompute $Y_0, ..., Y_r$
9. if $T \neq \mathrm{MSB}_{Tlen}(Y_r)$, then return INVALID, else return P.

PROBLEM 2.

In order to deal with the problem of cache attacks against AES (described during the lecture) there is the following proposition:

the lookup table is extended by inserting a random prefix: i.e. instead of a lookup table T we have $R||T$, where R is a random string of a random length k. A look up operation is as usual, but we have to add an offset k to the standard address.

question: is this countermeasure effective against cache attack?